آشنایی با رمزگشایی

به روش ریاضی

آبراهام سینکوف

ترجمهٔ رؤیا درودی، عبادالله محمودیان

(ریاضیات پیش‌دانشگاهی- ۲۲)

آشنایی با رمزگشایی

به روش ریاضی

(ریاضیات پیش‌دانشگاهی- ۲۲)

آبراهام سینکوف

ترجمهٔ رؤیا درودی، عبادالله محمودیان

مرکز نشردانشگاهی، تهران

Elementary Cryptanalysis –a Mathematical Approach
New Mathematical Library (22)
Abraham Sinkov
The Mathematical Association of America, 1980

آشنایی با رمزگشایی به روش ریاضی
تألیف آبراهام سینکوف
ترجمهٔ رؤیا درودی، دکتر عبادالله محمودیان
ویراستهٔ عبدالحسین مصحفی، همایون معین
نسخه‌پرداز: حسن طلوع
مرکز نشر دانشگاهی، تهران
چاپ اول ۱۳۷۴
تعداد ۵۰۰۰
حروفچینی: TEX-پارسی مرکز نشر دانشگاهی
لیتوگرافی: ۱۱۰
چاپ و صحافی: نوبهار

فهرستنویسی پیش از انتشار کتابخانهٔ ملی جمهوری اسلامی ایران

سینکوف، آبراهام، ۱۹۰۷-
Sinkov, Abraham
آشنایی با رمزگشایی به روش ریاضی / آبراهام سینکوف؛ ترجمهٔ رؤیا درودی، عبادالله محمودیان.- تهران: مرکز نشر دانشگاهی، ۱۳۷۴.
پنج، ۲۳۷ ص.- (مرکز نشر دانشگاهی؛ ۷۵۹. ریاضی، آمار و کامپیوتر؛ ۹۸)
ISBN: 964-01-0759-10
عنوان اصلی:
Elementary cryptanalysis -a mathematical approach
«ریاضیات پیش دانشگاهی- ۲۲»
واژه‌نامه:
۱. رمزنگاری. ۲. رمز. الف. درودی، رؤیا، ۱۳۴۳- ، مترجم. ب. محمودیان، عبادالله، ۱۳۲۲- ، مترجم. ج. مرکز نشر دانشگاهی. د. عنوان.
۵ آ ۹ س/ Z ۱۰۴
۶۵۲/۸
۱۳۷۴
کتابخانهٔ ملی ایران
۷۴-۱۴۷۸م

بسم الله الرحمن الرحیم

فهرست

عنوان	صفحه
مقدمه	۱
۱. رمزهای تک‌الفبایی حاصل از الفبای متعارف مستقیم	۵
۱.۱ رمز سزاری	۵
۲.۱ حساب همنهشتی	۷
۳.۱ الفبای متعارف مستقیم	۱۱
۴.۱ گشودن الفباهای متعارف مستقیم از راه تکمیل دنبالهٔ صریح	۱۴
۵.۱ گشودن الفباهای متعارف مستقیم با استفاده از فراوانی حرفها	۱۷
۶.۱ الفباهای مبتنی بر طرحهای چند درمیان دنبالهٔ معمولی	۲۳
۷.۱ گشودن الفباهای متعارفِ با طرح چند در میان	۳۱
۸.۱ رمزهای تک‌الفبایی مبتنی بر تبدیلهای خطی	۳۵
۲. جایگذاری تک‌الفبایی کلی	۴۱
۱.۲ الفبای درهم‌ریخته	۴۱
۲.۲ گشودن الفباهای درهم‌ریخته	۴۵
۳.۲ گشودن رمزهای تک‌الفبایی که در دسته‌های پنج‌حرفی نوشته شده‌اند	۵۲
۴.۲ رمزهای تک‌الفبایی با معادلهای رمزی نمادین	۶۱

عنوان	صفحه
۳. جایگذاری چندالفبایی	۶۴
۱.۳ رمزهای چندالفبایی	۶۴
۲.۳ تشخیص رمزهای چندالفبایی	۶۸
۳.۳ تعیین تعداد الفباها	۷۷
۴.۳ گشودن الفباهای پیام چندالفبایی، در صورتی که متعارف باشند	۸۱
۵.۳ رمزهای چندالفبایی با دنبالهٔ صریح درهم‌ریخته	۸۶
۶.۳ تطبیق الفباها	۹۰
۷.۳ تبدیل رمز چندالفبایی به رمز تک‌الفبایی	۱۰۲
۸.۳ رمز چندالفبایی با دنبالهٔ رمزی درهم‌ریخته	۱۰۴
۹.۳ تذکرات کلی دربارهٔ رمزهای چندالفبایی	۱۲۰
۴. سیستمهای چندحرفی	۱۲۴
۱.۴ رمزهای دوحرفی مبتنی بر تبدیلهای خطی یا ماتریسها	۱۲۴
۲.۴ ضرب ماتریسها و وارون آنها	۱۳۳
۳.۴ تبدیل برگشتی	۱۴۰
۴.۴ شناسایی رمزهای دوحرفی	۱۴۲
۵.۴ گشودن تبدیل خطی	۱۴۵
۶.۴ چگونه می‌توان ایمنی سیستم هیل را بیشتر کرد	۱۵۳
۵. انتقال	۱۵۵
۱.۵ انتقال ستونی	۱۵۵
۲.۵ گشودن رمزهای انتقالی دارای مستطیل کاملاً پر	۱۶۲
۳.۵ مستطیلهای ناکامل	۱۶۶
۴.۵ گشودن مستطیلهای ناکامل به روش کلمهٔ احتمالی	۱۶۸
۵.۵ مستطیلهای ناکامل در حالت کلی	۱۷۴
۶.۵ عبارات تکراری در پیامهای متفاوت؛ پیامهای هم‌طول	۱۸۳
ضمیمهٔ الف جدول فراوانیهای دوحرفیها	۱۸۹

عنوان	صفحه
ضمیمهٔ ب وزنهای لگاریتمی	۱۹۰
ضمیمهٔ ج فراوانی حروف الفبا	۱۹۱
ضمیمهٔ د فراوانی حروف اول کلمات	۱۹۲
ضمیمهٔ ه فراوانی حروف آخر کلمات	۱۹۳
پاسخ تمرینها	۱۹۴
منابعی برای مطالعهٔ بیشتر	۱۹۸
فهرست راهنما	۲۰۱
پیوست ــ برنامه‌های کامپیوتری از پال اروین	۲۰۵
مقدمه	۲۰۷
۱. توزیع فراوانی سه‌حرفی	۲۰۹
۲. شاخص انطباق	۲۱۵
۳. تطبیق الفباها	۲۱۸
۴. توزیع فراوانی سه‌حرفی به ازای هریک از الفباهای یک رمز چندالفبایی تناوبی	۲۲۲
۵. توزیع فراوانی دوحرفی	۲۳۰
واژه‌نامهٔ پیوست	۲۳۷

مقدمه

پیشرفت بشر تا اندازهٔ بسیار زیادی مرهون قابلیت وی در برقراری ارتباط است، و یک جنبهٔ اساسی این قابلیت، توانایی برقراری ارتباط ازطریق نوشتن است. از همان نخستین روزهای نوشتن، موقعیتهایی پیش می‌آمد که کسانی می‌خواستند اطلاعات خود را منحصراً به عدهٔ محدودی برسانند. آنان اسراری داشتند که می‌خواستند فاش نشود. برای این کار، طرحهایی یافتند که از آن راه می‌توانستند برای کسانی که به اطلاعات بخصوصِ مورد نیاز برای از رمز درآوردن دسترسی نداشتند، مکاتبه‌های خود را نامفهوم سازند. تکنیکهای کلی به‌انجام رساندن چنین مقصودی، یعنی پنهان داشتن مفهوم پیامها، مبحثی را تشکیل می‌دهد که آن را تحت‌عنوان رمزنگاری می‌شناسیم.

پیش از پیدایش پست به مفهوم امروزی آن و ارسال الکتریکی اطلاعات، شیوهٔ معمول فرستادن پیام، استفاده از قاصد خصوصی بود. باوجود این، باز هم غالباً صلاح در این بود که از روشهای پنهان‌سازی رمزنگاری استفاده شود، زیرا امکان دستگیرشدن قاصد یا خیانت وی وجود داشت. در روزگارکنونی هم، از پیامی که با بی‌سیم انتقال یابد، هرکسی که ابزار مناسب را دارا باشد و از آن در زمان مناسب با انتخاب فرکانس صحیح استفاده کند، می‌تواند رونوشت بردارد. در چنین موردی نیز، اگر پنهان کردن محتوای پیام موردنظر فرستنده باشد، باید از نوعی شیوهٔ پنهان‌سازی رمزنگاری استفاده کند.

اما همان‌طور که فرستندهٔ پیام تلاش می‌کند اطلاعات خود را از هرکس مگر گیرندهٔ موردنظر پنهان دارد، کسانی هم هستند که به کشف محتوای پیام بسیار علاقه‌مندند، و چه‌بسا این افراد از همان کسانی باشند که فرستنده تلاش دارد اطلاعات خود را از ایشان

پنهان دارد. اگر چنین کسانی به‌طریقی رونوشتی از پیام رمزی را به‌دست آورند، در آشکار کردن رازی که پیام حاوی آن است خواهند کوشید. البته تلاش آنها بدون داشتن اطلاعاتی دربارهٔ جزئیات عمل رمزنگاری، که برای پنهان ساختن مضمون پیام به‌کار رفته است، انجام خواهد پذیرفت. تلاشی که از این راه و با هدف خواندن پیامهای سرّی انجام می‌پذیرد تحت‌عنوان مبحثی قرار می‌گیرد که رمزگشایی نامیده می‌شود.

در تاریخ از موارد فراوانی می‌توان یاد کرد که رمزگشایی موفقیت‌آمیز، عامل خیلی مهمی در به‌دست آوردن موفقیتهای سیاسی، کسب پیروزیهای نظامی، دستگیری جنایتکاران و فعالیتهای ضدجاسوسی بوده است. در ترجمهٔ اسناد تاریخی که از بایگانیهای رسمی به‌دست آمده‌اند و تشخیص داده شده که به زبان سرّی نوشته شده‌اند، همچنین در بازسازی زبانهایی که مدتها پیش از بین رفته‌اند و کسی دربارهٔ آنها چیزی نمی‌داند و در حقیقت زبانهای سرّی محسوب می‌شوند نیز رمزگشایی سهیم بوده است. این جنبه‌های تاریخی و مهیج رمزگشایی به‌قدر کافی در بسیاری از منابع دیگر موردبحث قرار گرفته‌اند و در این کتاب از آنها گفتگویی به‌میان نمی‌آید.

هدف این کتاب آشنا کردن خواننده با بعضی از شیوه‌های بنیادی رمزگشایی است. روش کار عبارت است از شرح یک فرایند رمزنگاری، و سپس بررسی راهی که ممکن است با استفاده از آن بتوان رمز را بدون داشتن اطلاعی دربارهٔ آن بازسازی کرد. آنگاه با درک نحوهٔ تحلیل در رمزگشایی می‌توان روشهایی برای بهبود رمزنگاری پیدا کرد، یعنی روشهایی برای رفع آن نواقص رمزنگاری که در رمزگشایی مورد استفاده قرارگرفته‌اند. چنین بهبودی مسألهٔ جدیدی را برای رمزگشا به‌دنبال می‌آورد. این بهبودِ گام‌به‌گام، در حقیقت، تاریخ پیشرفت رمزشناسی بوده است ـ رمزشناسی عنوانی است که برای نشان دادن هردو مفهوم رمزنگاری و رمزگشایی به‌کار می‌رود.

فرایندهای تحلیلی که در رمزگشایی به‌کار می‌روند با استفاده از تکنیکهایی صورت می‌گیرند که بعضی ریاضی‌اند، بعضی مربوط به زبان‌اند، بعضی ماهیت مهندسی دارند، و بعضی هم به‌راحتی قابل توصیف نیستند، مانند شانس، فراست، حس ششم، و غیره. از آنجا که این کتاب در اصل برای دانش‌آموزان ریاضی نگاشته شده، توجه ما در ارائهٔ مطالب به جنبه‌های ریاضی رمزگشایی معطوف بوده است. طبیعتاً بعضی از جنبه‌های دیگر در بحث کلی وارد شده‌اند، اما در بیشتر قسمتها، توجه ما معطوف به جنبه‌های ریاضی بوده است، و چون بیشتر مفهومهای ریاضی که مطرح شده‌اند به شاخه‌هایی از ریاضیات

مربوط‌اند که در دبیرستان مطالعه نمی‌شوند، هرجا که این مفهومها مطرح شده‌اند، نسبتاً به تفصیل دربارهٔ آنها بحث شده است.

باید اذعان کرد که توجه به فرایندهای ریاضی به حذف بعضی از مباحث دیگر منجر شده است. برای مثال، دربارهٔ کدهایی که به‌شیوهٔ کتابهای لغت برای تبدیل بیان صریح به بیان سرّی به‌کار می‌روند، سخنی به‌میان نیامده است.

تشریح روشهای گشودن رمز با استفاده از کاربرد آنها در مثالهایی خاص، انجام گرفته است. این مثالها به‌طریقی انتخاب شده‌اند که بیان مطلب را ساده‌تر سازند. تقریباً همهٔ متنها از مقاله‌های روزنامه‌ها گرفته شده‌اند. طول این متنها آن‌قدر هست که مشکل گشودن رمز بیش از حد نباشد. هیچ تلاشی برای دخل و تصرف در زبان، یا در فراوانیهای حروف، انجام نگرفته است.

همان‌طور که از عنوان کتاب برمی‌آید، سیستمهای رمزنگاری که در این کتاب بررسی شده‌اند مقدماتی‌اند. این سیستمها کاملاً شناخته‌شده هستند و در طی مدت مدیدی به‌کار رفته‌اند. شیوه‌های به‌کار رفته برای رمزگشایی نیز شیوه‌های شناخته شده‌ای هستند، اگرچه این شیوه‌ها معمولاً به بیان ریاضی ارائه نمی‌شده‌اند. خواننده متوجه خواهد شد که می‌توان سیستمهای رمزنگاری را که در اینجا بررسی شده‌اند پیچیده‌ترکرد. برای بهترکردن سیستمهای شرح داده شده، قطعاً طرحهایی به فکر او خواهند رسید. مهمترین نوع پیشرفتهای جدید با متداول شدن ماشینهای الکترومکانیکی و الکترونیکی حاصل شده‌اند و به سیستمهای رمزنگاری ماهیت پیچیده‌تری بخشیده‌اند. بنابراین شیوه‌های گشودن رمز چنین سیستمهایی نیز باید به همان نسبت پیشرفته باشند. از این کتاب بیش از این نمی‌توان انتظار داشت که تکنیکهای بنیادی را که در تلاش برای رمزگشایی اساس کارند به خواننده عرضه کند.

اگر خواننده بخواهد به آن درجه از تسلط برسد که برای بررسی مستقل مسأله‌های رمزگشایی لازم است، باید هر مرحله از استدلالهای ارائه شده را درک کند، و آنچه را در متن انجام گرفته است جزءبه‌جزء بررسی کند تا صحت آنها برایش مسجل شود.

در اینجا لازم می‌دانم از خانم انلی لکس[1]، ویراستار این مجموعه کتب پیش‌دانشگاهی، به‌خاطر توصیه‌های سودمندش در طی نوشتن این کتاب، و از دکتر سالمن کولبک[2] به‌خاطر همکاریش در بعضی از جنبه‌های آمار ریاضی این کتاب سپاسگزاری کنم. بیش از همه

1. Anneli Lax 2. Solomon Kullback

نیز همسرم، که خود یک رمزگشای خوب است، به‌خاطر تشویقهایش و به‌خاطر حل‌وفصل بسیاری از نکاتی که باید در نظر گرفته می‌شد، به گردن من حق دارد.

در ۱۹۷۹ پرفسور پال اروین[1] مجموعه‌ای از برنامه‌هایی به‌زبان بیسیک را که خود و دانشجویانش برای ساده‌تر کردن بخش خسته‌کنندهٔ به‌دست آوردن توزیعهای فراوانی و انجام‌دادن محاسبات آماری به‌کار برده بودند برای ضمیمه‌کردن به کتاب مدون کرد. خوشوقتم که در چاپ کنونی کتاب (سال ۱۹۸۰) این ضمیمه را به آن اضافه می‌کنم.

1. Paul L. Irwin

۱

رمزهای تک‌الفبایی حاصل از الفبای متعارف مستقیم

۱.۱ رمز سزاری

یکی از قدیمیترین سیستمهای رمزنگاری که می‌شناسیم سیستمی است که ژول سزار به‌کار می‌برده است و لذا به رمزنگاری سزاری موسوم است. در این روش رمزنگاری، به‌جای هر حرف از پیام، حرف سومِ بعد از آن از حروف الفبای معمولی قرار داده می‌شد. البته سزار الفبای رومی را به‌کار می‌برد، ولی ما شیوهٔ او را با الفبای امروزی [انگلیسی] شرح خواهیم‌داد.

فرض کنید بخواهیم پیام زیر را به رمز درآوریم*:

I CAME I SAW I CONQUERED

زیر هر حرف از پیام، حرفی را می‌نویسیم که در حرفهای الفبا، به‌ترتیب معمول، سه حرف پس از آن قرار گرفته است؛ یعنی به‌جای I حرف L قرار می‌گیرد، به‌جای C حرف F، به‌جای A حرف D، و غیره. نتیجهٔ کار چنین است:

I CAME I SAW I CONQUERED

L FDPH L VDZ L FRQTXHUHG

* فرایند تبدیل پیام از زبان صریح به زبان رمزی را، به‌وسیلهٔ عملیاتی اسلوبمند روی حرفهای آن، به رمز درآوردن می‌نامند؛ فرایند معکوس را، یعنی بازسازی پیام اصلی از روی متنِ به رمز درآمده و از راه عملیات عکس به رمز درآوردن و با اطلاع کامل از جزئیات عملیات به رمز درآوردن را، از رمز درآوردن می‌نامند.

و پیام رمزی عبارت است از:

L FDPH L VDZ L FRQTXHUHG

نتیجه کاملاً نامفهوم به‌نظر می‌رسد. برای فردی که آن را بررسی می‌کند و از چگونگی تهیهٔ آن اطلاعی ندارد، ممکن است تلاش برای کشف آن کاملاً بی‌ثمر باشد. از طرف دیگر برای کسی که رمز را می‌داند، معنی پیام به‌سرعت معلوم می‌شود. فقط کافی است به‌جای هر حرف از پیام رمزی حرفی را که در حرفهای الفبا، به‌ترتیب معمولی، سه‌تا پیش از آن قرار گرفته است قرار دهد تا مطلب اصلی فاش شود.

این مثالی از نوعی رمز به‌نام رمز جایگذاری است که در آن به‌جای هر حرف از پیام اصلی حرف دیگری گذاشته می‌شود. راهی مناسب برای نمایش دادن این جایگذاری استفاده از الفبای جایگذاری است که نشان می‌دهد چه حرفی به‌جای چه حرفی قرار می‌گیرد. روش ساختن الفبای جایگذاری در رمز سزاری، عبارت از نوشتن دنبالهٔ الفبای معمولی در یک سطر، و سپس بازنویسی آن در سطر دوم، منتها با شروع از D به‌جای A است. وقتی که در سطر دوم به حرف آخر الفبا رسیدیم، بعد از حرف Z به‌ترتیب حرفهای A و B و C را می‌نویسیم، در واقع دنبالهٔ الفبا را به‌صورت چرخه‌ای در نظر می‌گیریم که متوالیاً تکرار می‌شود،

صریح **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**

رمزی **D E F G H I J K L M N O P Q R S T U V W X Y Z A B C**

سطر بالایی الفبای جایگذاری را دنبالهٔ صریح و سطر پایینی را دنبالهٔ رمزی می‌خوانیم.

به این ترتیب، عمل به رمز درآوردن را می‌توانیم بدین‌صورت انجام دهیم که به‌جای هر حرف از پیام صریح، حرف زیرین آن در الفبای جایگذاری را قرار دهیم؛ برای از رمز درآوردن می‌توانیم به‌جای هر حرف از پیام رمزی، حرف بالایی آن در الفبای جایگذاری را بگذاریم. (به زبان ریاضی، می‌گوییم عمل از رمز درآوردن معکوس عمل به رمز درآوردن است.)

فرایند رمزنگاری در رمز سزاری را می‌توان به‌صورت عددی نیز انجام داد. فرض کنید به هر حرف، عددی نسبت دهیم که مکان آن را در دنبالهٔ معمولی الفبا نشان دهد. در این صورت تناظر زیر را خواهیم داشت:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

حال برای به رمز درآوردن پیام **I CAME I SAW I CONQUERED** به‌طریق زیر مرحله‌به‌مرحله عمل می‌کنیم:

(۱) به‌جای هر حرف عدد متناظر با آن را قرار می‌دهیم.

(۲) به هر کدام از این اعداد ۳ واحد اضافه می‌کنیم.

(۳) به‌جای اعداد حاصل، حروف متناظرشان را می‌گذاریم.

	I	C	A	M	E	I	S	A	W	I	C	O	N	Q	U	E	R	E	D
(۱) :	9	3	1	13	5	9	19	1	23	9	3	15	14	17	21	5	18	5	4
(۲) :	12	6	4	16	8	12	22	4	26	12	6	18	17	20	24	8	21	8	7
(۳) :	L	F	D	P	H	L	V	D	Z	L	F	R	Q	T	X	H	U	H	G

همان‌طور که انتظار داشتیم، نتیجه همان پیام رمزی است که قبلاً به‌دست آمده بود.

تمرین

پیامهای زیر را که با رمز سزاری به رمز درآمده‌اند از رمز درآورید:

۱. **FRZDUGV GLH PDQB WLPHV EHIRUH WKHLU GHDWKV**

۲. **WKH HYLO WKDW PHQ GR OLYHV DIWHU WKHP**

۲.۱ حساب همنهشتی

در عملِ به رمز درآوردن عددی، ممکن است مسأله‌ای پیش آید. فرض کنید می‌خواهیم X، Y یا Z را که معادلهای عددی آنها به‌ترتیب ۲۴، ۲۵، ۲۶ هستند، به رمز درآوریم. با افزودن عدد ۳ به این اعداد، عددهای ۲۷، ۲۸، ۲۹ حاصل می‌شوند، که هیچ‌کدام از آنها در تناظر سابق‌الذکر بین حروف و اعداد نیامده‌اند. اگر دوباره به الفبای جایگذاری بنگریم، خواهیم دید که X و Y و Z که به رمز درآیند به‌ترتیب به A و B و C تبدیل می‌شوند، بنابراین اعداد ۲۷ و ۲۸ و ۲۹ متناظر همان حروفی هستند که با ۱و۲و۳ متناظرند. چون دنبالهٔ رمزی را به‌صورت چرخه‌ای از حروف الفبا در نظر گرفته‌ایم که متوالیاً تکرار می‌شود، در حقیقت به‌جای اعداد بزرگتر از ۲۶ عددهایی را می‌گذاریم که با کم کردن ۲۶ از آنها

به‌دست می‌آیند. لذا ابهامی پیش نخواهد آمد، زیرا حروف A، B و C در دنبالهٔ رمزی تنها در زیر حروف X، Y و Z واقع می‌شوند، بنابراین حالت یک‌به‌یک تناظر در نمایشهای عددی نیز حفظ خواهد شد.

از این ایدهٔ معادل [یا هم‌ارز] گرفتن اعداد، شیوه‌ای کلی برای محاسبات رمزنگاری به‌دست می‌آوریم. به‌عنوان مثال می‌توانیم قرارداد کنیم که صرفاً با اعداد از ۱ تا ۲۶ کار کنیم، و باتوجه به اینکه هر عدد صحیح مثبت aی خارج از مجموعهٔ $\{۱, ۲, ۳, \ldots, ۲۶\}$ قابل‌تبدیل به یک عدد صحیح bی هم‌ارز آن در داخل این مجموعه است، روشن است که این کار همیشه ممکن است. a را بر ۲۶ تقسیم کنید، باقیمانده (یا مانده) عدد b است. اگر باقیمانده صفر باشد، یعنی اگر a مضربی از ۲۶ باشد، آنگاه b را برابر ۲۶ می‌گیریم.

مثال: اگر a عدد ۷۳ باشد، چون بر ۲۶ تقسیم شود خارج‌قسمت ۲ و باقیماندهٔ ۲۱ به‌دست می‌آید. بنابراین، در این مورد، $b = ۲۱$. اگر a عدد ۱۳۰ باشد، بر ۲۶ که تقسیم شود، خارج‌قسمت ۵ و باقیماندهٔ صفر به‌دست خواهد آمد؛ در این مورد $b = ۲۶$.

به‌طور کلی، اگر عدد صحیح a بزرگتر از ۲۶ باشد، آن را بر ۲۶ تقسیم کرده به‌صورت زیر می‌نویسیم:

$$a = k(۲۶) + b,$$

که باقیماندهٔ تقسیم، یعنی b در مجموعهٔ $\{۱, ۲, \ldots, ۲۶\}$ قرار دارد. در مثالهای بالا داریم:

$$۱۳۰ = ۵(۲۶) = ۴(۲۶) + ۲۶ \quad \text{و} \quad ۷۳ = ۲(۲۶) + ۲۱$$

a و b را به‌عنوان دوعدد هم‌ارز در نظر می‌گیریم و می‌گوییم a با b همنهشت است. شیوهٔ دیگر بیان این مطلب به این صورت است: دو عدد a و b همنهشت‌اند اگر تفاضل آنها، $a - b$، مضربی از ۲۶ باشد. با این تعریف، ۰ با ۲۶ همنهشت است؛ در واقع می‌توانیم، و گاهی وقتها چنین می‌کنیم، که حساب خود را به‌جای عددهای از ۱ تا ۲۶ شامل اعداد ۰ تا ۲۵ فرض کنیم. به‌طور کلی، هر مجموعهٔ ۲۶ عددی از اعداد همنهشت با عددهای ۱ تا ۲۶ می‌تواند به‌عنوان مجموعهٔ موردنظر به‌کار رود. چنین مجموعه‌ای از اعداد مجموعهٔ کامل مانده‌ها نامیده می‌شود. مواردی وجود دارند که در آنها یک مجموعهٔ کامل مانده‌ها، به‌غیر از مجموعهٔ ۲۶ عدد نخستین، مفید واقع می‌شود. اما برای رمزنگاری، تقریباً همیشه با مجموعهٔ کامل مانده‌های از ۱ تا ۲۶ کار خواهیم کرد.

حتی اگر a منفی باشد می‌توانیم به‌راحتی یک عدد مثبت b را در مجموعهٔ $\{۱, \ldots, ۲۶\}$ بیابیم که با a همنهشت باشد: با تقسیم عدد مثبت $-a$ بر ۲۶ خواهیم داشت:

$$-a = q(۲۶) + r = (q+۱)۲۶ - (۲۶ - r), q \geq ۰, ۰ \leq r < ۲۶$$

حال b را برابر $۲۶-r$ می‌گیریم، در نتیجه:

$$a = -(q+۱)۲۶ + b$$

واضح است که، بنابر تعریف، b با a همنهشت است، زیرا:

$$a - b = -(q+۱)۲۶$$

یعنی $a-b$ مضربی از ۲۶ است؛ علاوه براین، از آنجا که $b = ۲۶ - r$، $۰ \leq r < ۲۶$، پس b در مجموعهٔ $\{۱, ۲, \ldots, ۲۶\}$ قرار دارد. بنابراین، به‌ازای عدد منفی a، b را عدد $۲۶-r$ می‌گیریم که r باقیمانده‌ای است که از تقسیم $-a$ بر ۲۶ حاصل می‌شود.

مثال:

۱. $b = ۲۶ - ۶ = ۲۰; \quad -a = ۲(۲۶) + ۶, \quad a = -۵۸,$

پس ۵۸- با ۲۰ همنهشت است.

۲. $b = ۲۶ - ۳ = ۲۳; \quad -a = ۰(۲۶) + ۳, \quad a = -۳,$

پس ۳- با ۲۳ همنهشت است.

به‌طور خلاصه، هر عدد صحیح a اعم از مثبت، صفر یا منفی را می‌توان به‌صورت زیر نوشت:

$$a = \pm k(۲۶) + b,$$

که b متعلق به مجموعهٔ $\{۱, ۲, \ldots, ۲۶\}$ و a همنهشت با b است.

مشاهده می‌کنیم که در این حساب رمزنگاری، انجام دادن هر کدام از اعمال جمع، تفریق، یا ضرب روی اعداد صحیح و تحویل جواب به یکی از عددهای مجموعهٔ کامل مانده‌ها امکان‌پذیر است. (تقسیم پیچیده‌تر است، در آینده در مورد آن بحث خواهد شد.)

در اینجا باید خاطرنشان شود که این نوع حساب، در بسیاری از شاخه‌های ریاضیات که در آنها اعداد صحیح به‌کار می‌روند کاربرد زیادی دارد و حساب همنهشتی خوانده

می‌شود. در حساب همنهشتی هر عدد صحیح مثبت می‌تواند به‌عنوان پیمانه انتخاب شود، یعنی همان نقشی را داشته باشد که ۲۶ در بحث فوق داشت. به‌عنوان مثال اگر پیمانه عدد n باشد، می‌توانیم حساب خود را تنها شامل n عدد بدانیم. این اعداد ممکن است هر n عدد صحیح متوالی باشند، به‌عنوان مثال از ۰ تا $n-1$، یا از ۱ تا n. با انتخاب چنین مجموعه‌ای، می‌توانیم هر عدد صحیح را، چه مثبت باشد، چه منفی و چه صفر، به یک عدد در مجموعهٔ انتخاب‌شده تحویل کنیم. اگر a با این عمل به b قابل‌تحویل باشد، می‌گوییم a به پیمانهٔ n با b همنهشت است، و این عبارت را به‌صورت نمادی چنین می‌نویسیم:

$$a \equiv b \ (\text{پیمانهٔ } n)$$

و مقصود ما این است که

$$a - b = k.n$$

که در آن k عددی صحیح است. این رابطه نوعی تساوی است. در مورد جمع و تفریق، نماد همنهشتی ($\equiv$) مانند تساوی عمل می‌کند.

اگر

$$a \equiv b \ (\text{پیمانهٔ } n), \qquad c \equiv d \ (\text{پیمانهٔ } n)$$

آنگاه

$$a + c \equiv b + d \ (\text{پیمانهٔ } n), \qquad a - c \equiv b - d \ (\text{پیمانهٔ } n).$$

برای اثبات کافی است که این نمادگذاری را به‌طریق زیر ترجمه کنیم: اگر

$$a - b = kn,$$
$$c - d = ln,$$

آنگاه

$$(a + c) - (b + d) = (k + l)n,$$
$$(a - c) - (b - d) = (k - l)n.$$

اگر یک معادلهٔ همنهشتی به‌صورت زیر داشته باشیم

$$x + a \equiv b \ (\text{پیمانهٔ } n),$$

جواب آن

$$x \equiv b - a \ (n \text{ پیمانهٔ})$$

است، زیرا بنابر رابطهٔ اول، $x + a - b = x - (b - a)$ مضربی از n است، یعنی x با $b - a$ همنهشت است. بنابراین هر معادلهٔ همنهشتی به‌صورت $x \pm k \equiv a \ (n \text{ پیمانهٔ})$ با اعداد صحیح ثابت a و k و n، جواب منحصر به‌فردی دارد، که $x \equiv a \pm k$ است.

از آنجا که الفبای ما [انگلیسی] شامل ۲۶ حرف است، غالباً پیمانهٔ ۲۶ را در رمزنگاری به‌کار خواهیم برد.

تمرین

۳. الف) اگر اولین روز یک ماه دوشنبه باشد، در طی آن ماه چه روزی از هفته دارای تاریخهایی است که به پیمانهٔ ۷ با ۳ همنهشت‌اند؟

ب) اگر وزن وزنه‌ای برحسب اونس همنهشت با ۲۰ به پیمانهٔ ۱۶ باشد، قسمت کسری وزن وزنه برحسب پوند چیست؟ [هر پوند ۱۶ اونس است.]

۴. معادلهٔ (پیمانهٔ ۵) $x + ۱۲ \equiv ۳$ را حل کنید.

۵. معادلهٔ (پیمانهٔ ۶) $y - ۱ \equiv ۱۳$ را حل کنید.

۳.۱ الفبای متعارف مستقیم

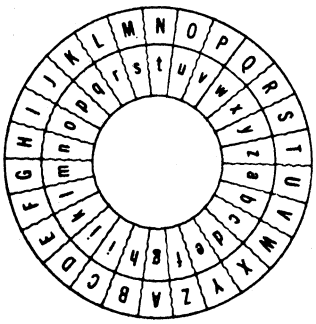
نمی‌دانیم چرا سزار عدد ۳ را به‌عنوان میزان انتقال دنبالهٔ رمزی نسبت به دنبالهٔ صریح انتخاب کرد. او می‌توانست هر عددی را برای این منظور به‌کار ببرد، فقط کافی بود که قبلاً با طرف مکاتبه خود دربارهٔ چگونگی به رمز درآوردن قراری گذاشته باشد. در واقع، به‌فرض یک قرارداد مناسب، میزان انتقال می‌تواند در هر پیام با پیام دیگر فرق داشته باشد. برای مثال می‌توان قرار گذاشت که طبق طرحی، به هر پیام یک عدد نسبت داده شود و باقیماندهٔ این عدد به پیمانهٔ ۲۶، میزان انتقال یعنی مقدار تغییرمکان گرفته شود ـ من‌باب مثال چنین عددی ممکن است عبارت باشد از: تعداد کلمات هر پیام، یا شمارهٔ پیام، یا تاریخ ماهی که پیغام فرستاده می‌شود، یا عددی که از فرایندی به دست می‌آید که اصلاً ربطی به آن مکاتبه ندارد. با داشتن این عدد، الفبای جایگذاری می‌تواند ساخته شود و هم در به رمز درآوردن و هم در از رمز درآوردن به‌کار رود. یک الفبای جایگذاری که در آن

هم دنبالهٔ صریح و هم دنبالهٔ رمزی از الفبای معمولی گرفته شده باشند (به‌این ترتیب که دنبالهٔ رمزی پس از مقدار مشخصی تغییرمکان به‌دست آمده باشد) الفبای متعارف مستقیم خوانده می‌شود. در فرایند عددیِ معادل می‌توان گفت: $C = P + K$ که در آن K، مقدار تغییرمکان، عددی است که باید به P، معادل عددی هر حرف زبان صریح، اضافه شود تا C، جانشین رمزی آن، به‌دست آید. اگر مقدار تغییرمکان K باشد، آنگاه حرف A از دنبالهٔ صریح مقابل حرفی از دنبالهٔ رمزی واقع است که متناظر با $K + ۱$ است.

با ابزاری ساده به‌سرعت می‌توان الفبای متعارف مستقیم را تشکیل داد. این ابزار از دو دایرهٔ هم‌مرکز ساخته می‌شود که در پیرامون هر یک از آنها، حرفهای الفبا به‌ترتیب نوشته شده‌اند (شکل ۱). حلقهٔ بیرونی دنبالهٔ صریح و حلقهٔ درونی، که قابل چرخیدن است، دنبالهٔ رمزی است. اگر مقابل A از حلقهٔ بیرونی، حرف متناظر $K + ۱$ از حلقهٔ درونی را قرار دهیم، الفبای جایگذاری را که میزان انتقال آن K باشد خواهیم داشت (شکل ۱ به‌ازای $K = ۶$ رسم شده است.)

جالب توجه است که سالها پیش، ارتش آمریکا ابزار مشابهی را به‌کار می‌برد. الفبایی که این ابزار تولید می‌کرد، با الفبای متعارف مستقیم این فرق را داشت که دنبالهٔ رمزی در آن با ترتیب وارونه نوشته شده بود. چنین دنباله‌ای دنبالهٔ متعارف وارونه، و الفبایی که این دنباله با قرارگرفتن در مقابل دنبالهٔ صریح معمولی تولید می‌کند الفبای متعارف وارونه نامیده می‌شود.

اگر از دایره برای ساختن الفبای متعارف مستقیم استفاده کنیم، آنگاه انتخاب هر کدام از ۲۶ الفبای متعارف مستقیم با قراردادن دایرهٔ درونی به وضع مناسب امکانپذیر می‌گردد.



شکل۱

چنین امکانی را ویژنر[1]، رمزنگار فرانسوی، به‌طریقی دیگر فراهم آورد. او در یک مربع حرفهای الفبا را نوشت، به این طریق که در بالاترین سطر، دنبالهٔ معمولی الفبا را نوشت و در هر سطر متعاقب آن دنباله‌ای را نوشت که از انتقال دنبالهٔ قبلی به‌اندازهٔ یک حرف به سمت چپ به‌دست می‌آمد. با قراردادن الفبای معمولی به‌عنوان دنبالهٔ صریح در بالای مربع، هر الفبای متعارف مستقیم، از ترکیب دنبالهٔ صریح با یک سطر مناسب در مربع، قابل حصول بود. هریک از این الفباها به‌راحتی با اولین حرف دنبالهٔ رمزیش معین می‌شد.

مربع ویژنر در زیر نشان داده شده است (شکل ۲). این مربع اساس سیستمهایی است که در فصل ۳ مطالعه خواهیم کرد.

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

شکل۲

1. Vigenère

دربارهٔ قراری که برای تعیین میزان انتقال گذاشته می‌شود، نکته‌ای جزئی را باید متذکر شویم. واضح است که اگر طبق قرار ما عدد تعیین‌کنندهٔ کلید رمز پیام بتواند مضربی از ۲۶ باشد، مرتکب اشتباه شده‌ایم؛ چون چنین عددی در تحویل به پیمانهٔ ۲۶، صفر خواهد شد، و در نتیجه پیام باید به زبان معمولی نوشته شود. بنابراین، قرار ما باید چنان باشد که طبق آن نتوان عدد ۲۶ (یا هر مضربی از آن) را به‌عنوان میزان انتقال به‌کار برد؛ اگر از فرایندی که قرار است طبق آن میزان انتقال محاسبه شود چنین عددی به‌دست آید، باید در این قرار مشخص شده باشد که چه عددی جانشین آن شود.

هر سیستم رمزنگاری دو رکن اساسی دارد: فرایند کلی مورد استفاده، و جزئیات نحوهٔ استفاده از آن. فرایند کلی را سیستم کلی و مشخص‌کنندهٔ جزئیات نحوهٔ استفاده از این فرایند را کلید ویژه می‌نامند. مثلاً در رمزنگاری سزاری از یک الفبای متعارف مستقیم با کلید ویژهٔ ۳ استفاده می‌شود. از آنجا که در این سیستم تنها یک الفبای جایگذاری به‌کار می‌رود، نتیجه را رمز تک الفبایی می‌نامند.

تمرین

۶. الف) یک الفبای متعارف مستقیم با میزان انتقال ۷ بسازید، و پیام زیر را به رمز درآورید:

THE FAULT DEAR BRUTUS IS NOT IN OUR STARS BUT IN OURSELVES

ب) پیام رمزی زیر را با دانستن آنکه الفبای متعارف مستقیم آن با میزان انتقال ۱۱ است، از رمز درآورید:

ESPCP TD L ETOP TY ESP LQQLTCD ZQ XPY HSTNS ELVPY LE ESP QWZZO WPLOD ZY EZ QZCEFYP

۴.۱ گشودن الفباهای متعارف مستقیم از راه تکمیل دنبالهٔ صریح

اکنون که می‌دانیم چگونه می‌توان پیامی را با استفاده از یک الفبای متعارف مستقیم به رمز در آورد، گشایش رمز پیامی را که از این راه به رمز درآمده است بررسی می‌کنیم. مثلاً پیام زیر را درنظر می‌گیریم:

BPM VMOWBQIBQWVA NWZ I AMBBTMUMVB WN BPM ABZQSM IZM IB IV QUXIAAM ZMKWUUMVL EM QVKZMIAM WCZ WNNMZ

و خود را در موقعیت یک رمزگشا قرار می‌دهیم که نسخه‌ای از این پیام رمزی را به‌دست آورده است و می‌خواهد آن را بگشاید. به‌علاوه فرض می‌کنیم که رمزگشا به‌طریقی ـشاید با حدسی اتفاقی، یا به‌علت آشنایی با روشهای رمزنگاری فرستندهٔ پیامـ سیستم کلی را می‌داند، امّا از کلید ویژه بی‌اطلاع است. در چنین موقعیتی، تنها کاری که او باید انجام دهد یافتن عددی است که وی را به خواندن پیام قادر سازد، عددی که نشاندهندهٔ میزان انتقال دنبالهٔ رمزی نسبت به دنبالهٔ صریح باشد.

از این نظر، مسأله زیاد مشکل به‌نظر نمی‌رسد. روی هم‌رفته، تنها ۲۵ عدد ممکن وجود دارند، و هر کدام را می‌توان به نوبت امتحان کرد تا عددی به‌دست آید که پیام را فاش سازد. در واقع، ممکن است کارکردن با یک کلمه برای یافتن کلید ویژه کافی باشد.

بنابراین، فرض کنید که BPM، یعنی کلمهٔ اول پیام را در نظر بگیریم. معادلهای عددی حرفهای این کلمه عبارت‌اند از ۲، ۱۶ و ۱۳. اگر عدد ۱ را از هر کدام از این اعداد کم کنیم، داریم:

$$\begin{array}{ccccc} ۱ & & ۱۵ & ۱۲ & = \mathrm{A} \quad \mathrm{O} \quad \mathrm{L} \end{array}$$

اگر ۲ را از هر کدام از عددهای اولیه کم کنیم، داریم:

$$\begin{array}{ccccc} ۲۶ & & ۱۴ & ۱۱ & = \mathrm{Z} \quad \mathrm{N} \quad \mathrm{K} \end{array}$$

این فرایند را ادامه می‌دهیم، و نتیجه را به‌صورت یک جدول منظم می‌کنیم. از ۲، ۱۶ و ۳ شروع می‌کنیم و اطلاعاتی را که به‌دست می‌آوریم به‌ترتیب زیر جدولبندی می‌کنیم:

مقدار کم شده	اعداد حاصل	متناظر حرفی
1	1 15 12	A O L
2	26 14 11	Z N K
3	25 13 10	Y M J
4	24 12 9	X L I
5	23 11 8	W K H
6	22 10 7	V J G
7	21 9 6	U I F
8	20 8 5	T H E

وقتی به عدد ۸ می‌رسیم، کلمهٔ THE را که مناسب به‌نظر می‌رسد مشاهده می‌کنیم؛ و در واقع، اگر اکنون کلید ۸ را برای تمام پیام به‌کار ببریم، قادر خواهیم بود تمام پیام را بخوانیم.

(خواننده باید روی جزئیات از رمز درآوردن کار کند تا بر فرایند رمزگشایی مسلط شود.)

توجه کنید که اگر عمل کم‌کردن را با ظهور کلمهٔ THE متوقف نکرده بودیم، بلکه کار را تا آخرین عدد، یعنی ۲۵ ادامه می‌دادیم، هر یک از سه ستون سمت راست جدول، یک الفبای کامل اما با ترتیب معکوس می‌بود. در صورت تمایل می‌توان این عددهای کلیدی را به‌ترتیب معکوس امتحان کرد. یعنی اول ۲۵، بعد ۲۴، تا به آخر، تا در هر ستون الفباها به‌ترتیب مستقیم قرار گیرند. چنین وضعی روشی را که اندکی با روش فوق تفاوت دارد برای جستجوی کلید به‌دست می‌دهد.

این موضوع را با انتخاب کلمهٔ دیگری از پیام رمزی، مثلاً A B Z Q S M، روشن می‌سازیم. زیر هریک از این حروف بقیهٔ حروف الفبا را به‌ترتیب می‌نویسیم:

A	B	Z	Q	S	M
B	C	A	R	T	N
C	D	B	S	U	O
D	E	C	T	V	P
E	F	D	U	W	Q
F	G	E	V	X	R
G	H	F	W	Y	S
H	I	G	X	Z	T
I	J	H	Y	A	U
J	K	I	Z	B	V
K	L	J	A	C	W
L	M	K	B	D	X
M	N	L	C	E	Y
N	O	M	D	F	Z
O	P	N	E	G	A
P	Q	O	F	H	B
Q	R	P	G	I	C
R	S	Q	H	J	D
S	T	R	I	K	E
T	U	S	J	L	F
U	V	T	K	M	G
V	W	U	L	N	H
W	X	V	M	O	I
X	Y	W	N	P	J
Y	Z	X	O	Q	K
Z	A	Y	P	R	L

سپس دنبال سطری بامعنی می‌گردیم وکلمهٔ STRIKE را می‌یابیم. سپس بررسی می‌کنیم که این سطر متناظر با چه عدد کلیدی است. از آنجا که حرف A از رمز با S از پیام صریح متناظر است و A هم‌ارز ۱ و S هم‌ارز ۱۹ است، K، یعنی عدد کلیدی باید چنان باشد که (پیمانهٔ ۲۶) $K + ۱۹ \equiv ۱$. به‌عبارت دیگر:

$$K \equiv ۱ - ۱۹ \equiv -۱۸ \equiv ۸ \text{ (پیمانهٔ ۲۶)}$$

فرایندِ یافتن کلید پیام رمزی از راه نوشتن تمام الفبا برای هر دسته از حروف رمزی تکمیل دنبالهٔ صریح خوانده می‌شود.

درگشایش پیام بالا، فرض شده بود که سیستم کلی به رمز درآوردن، الفبای متعارف مستقیم است. به‌بیان دیگر، سیستم کلی رمزنگاری مورد استفاده در به رمز درآوردن دانسته فرض شده بود. پس کار گشایش عبارت می‌شد از یافتن تنها یک مقدار مجهول، یعنی همان کلید ویژه، یعنی عددی که مقدار تغییرمکان را در انتقال دنبالهٔ رمزی نسبت به دنبالهٔ صریح به‌دست می‌دهد. مناسب بودن فرض فوق از آنجا معلوم می‌شود که این فرض امکان بازسازی پیام اصلی را فراهم ساخته است؛ و واضح است که همین موضوع، یعنی خواندن پیام، معیار نهایی موفقیت در رمزگشایی است.

تمرین

پیامهای زیر را بگشایید:

۷. **VXMDUJA JARCQVNCRL LXDUM KN LXWBRMNANM ANVJRWMNA JARCQVNCRL**

۸. **MZVYDIB DN OJ OCZ HDIY RCVO ZSZMXDNZ DN OJ OCZ WJYT**

۵.۱ گشودن الفباهای متعارف مستقیم با استفاده از فراوانی حرفها

حال امکان استفاده از روشی متفاوت را بررسی می‌کنیم، روشی که در آن فرض نمی‌شود، بلکه ثابت می‌شود که سیستم رمزنگاری مبتنی بر انتقال الفبای معمولی بوده است. این روش بر یک ویژگی اساسی زبان استوار است: فراوانی نسبی به‌کار رفتن حرفهای مختلف‌الفبا.

یک نمونه از متنی به زبان صریح را انتخاب می‌کنیم، مثلاً صفحه‌ای از یک کتاب یا چند پاراگراف از یک روزنامه، و فراوانی هر حرف را می‌شماریم، یعنی معلوم می‌کنیم که هر

حرف چندبار به‌کار رفته است. مثلاً از نمونه‌ای که به‌طول ۱۰۰۰ حرف انتخاب کرده‌ایم، پس از شمارش، نتیجهٔ زیر به‌دست آمده است:

A	73	J	2	S	63
B	9	K	3	T	93
C	30	L	35	U	27
D	44	M	25	V	13
E	130	N	78	W	16
F	28	O	74	X	5
G	16	P	27	Y	19
H	35	Q	3	Z	1
I	74	R	77		

فراوانی نسبی هر حرف، که موردنظر ماست، درصد تعداد دفعات ظاهرشدن آن حرف، یعنی درصد تعداد دفعات به‌کار رفتن آن حرف است. از آنجا که تعداد کل حروف در این نمونه ۱۰۰۰ است، فراوانی نسبی هر حرف از تقسیم فراوانی واقعی آن بر ۱۰ به‌دست می‌آید. همان‌طور که انتظار می‌رود، فراوانی نسبی حروف مختلف فرق دارد. تعداد Eها ۱۳٪ از کل حرفهاست، تعداد Tها تقریباً ۹٪، تعداد هر یک از حروف صدادار A، I، O حدود ۷٪ است؛ بعضی حروف مانند G، V، W، Y به‌ندرت به‌کار رفته‌اند (تعداد آنها بین ۱ تا ۲ درصد بوده است) و حرفهای J، K، Q و Z تقریباً اصلاً به‌کار نرفته‌اند.

بیان اینکه فراوانی نسبی E برابر ۱۳٪ است، به‌این معنی است که در یک انتخاب تصادفی از کل هزار حرف، احتمال به‌دست آمدن یک E به نسبت ۱۳ به ۱۰۰ است. از این رو، اصطلاح احتمال را، که تعریف دقیق ریاضی آن مبتنی بر مفهوم فراوانی نسبی است، به‌کار می‌بریم و از نماد زیر استفاده می‌کنیم

$$P_{\mathrm{E}} = ۰٫۱۳$$

تا نشان دهیم که احتمال به‌دست آوردن یک E برابر ۱۳٪ است. با این نمادگذاری، $P_{\mathrm{T}} = ۰٫۰۹$ و $P_{\mathrm{A}} = ۰٫۰۷$، و غیره. از آنجا که مجموع همهٔ فراوانیها مساوی تعداد همهٔ حرفها در نمونه است، نتیجه می‌شود که مجموع فراوانیهای نسبی ۱۰۰ درصد، یعنی ۱، است و بنابراین مجموع احتمالها برای همهٔ ۲۶ حرف مساوی ۱ است:

$$P_{\mathrm{A}} + P_{\mathrm{B}} + P_{\mathrm{C}} + \cdots + P_{\mathrm{Z}} = ۱$$

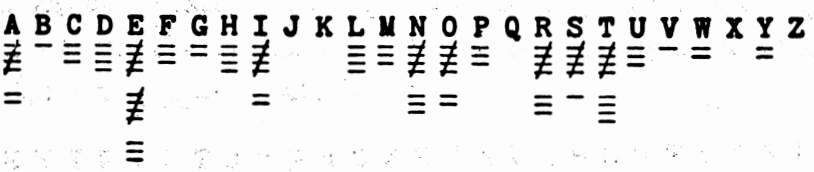
این عبارت را به‌صورت اختصاری زیر نشان می‌دهند:

$$\sum_{i=A}^{i=Z} P_i = ۱$$

که عبارت سمت چپ آن چنین خوانده می‌شود: «مجموع مقادیر P_i وقتی که i به‌نوبت مقادیر از A تا Z را اختیار می‌کند». A حد پایین و Z حد بالای مجموع نامیده می‌شود.

هر متنی از زبان متداول را، که به‌اندازهٔ کافی طولانی باشد، بررسی کنیم، نتیجه‌ای مشابه با آنچه از نمونهٔ هزارحرفی به‌دست آوردیم به‌دست خواهیم آورد. بسته به موضوع متن، زبان آن، سبک نگارش، و غیره، ممکن است که فراوانی نسبی تک‌تک حرفها در متون متفاوت، متفاوت باشد. اما به‌هر حال واقعیت این است که بعضی حروف، به‌ویژه حروف صدادار و تعداد کمی از حروف بی‌صدا مانند T، N، R، S، از فراوانی نسبی زیادی برخوردارند، در حالی‌که فراوانی نسبی حرفهای دیگری، مانند J، K، Q، V، W، X، Y، Z، کم است. همچنین درصد تعداد دفعات به‌کار رفتن هر حرفی در نمونه‌های طولانی، که آن را فراوانی مشخصهٔ آن حرف می‌نامیم، معمولاً در نمونه‌های متفاوت، تفاوت زیادی نمی‌کند. اگر پیامی بسیار کوتاه باشد، ممکن است فراوانی نسبی بعضی از حروف در آن پیام با فراوانی مشخصهٔ آنها تفاوت زیادی داشته باشد. اما هرچه پیام طولانیتر باشد، احتمال کمتری وجود دارد که تفاوتهای زیادی با فراوانیهای مشخصه وجود داشته باشد.

اکنون اطلاعات مربوط به شمارش فراوانیها را که در صفحهٔ قبل یادداشت کردیم به شکل یک نمودار میله‌ای نمایش می‌دهیم. برای سادگی، مقدار هریک از فراوانیهای نسبی را به نزدیکترین عدد صحیح گرد می‌کنیم، به‌گونه‌ای که بتوان فراوانی مشخصهٔ هر حرف را مانند زیر با نشانخط‌هایی نمایش داد:



در این نوع نمایش، نموداری می‌بینیم که واضحتر از جدول ارقام، زیاد و کم بودن فراوانی مشخصهٔ حرفها را آشکار می‌سازد. در این نمودار یک الگوی بااهمیت وجود دارد. در بین حروفی که فراوانیهای زیاد دارند، A و E و I را می‌بینیم که به فاصله‌های برابر (سه

حرف در میان) قرار دارند، و E بیشترین فراوانی را دارد، همچنین زوج متوالی N و O، و نیز سه‌تایی متوالی R و S و T را می‌بینیم. در بین حروفی که فراوانیهای کم دارند، زوج متوالی J و K و دنبالهٔ U، V، W، X، Y، Z قرار دارند.

این الگوی فراوانیهای زیاد و کم، با فاصله‌های مذکور، مشخصهٔ الفبای معمولی در زبان صریح، و یک ابزار اساسی رمزگشایی است.

حال ببینیم هنگامی که پیامی از راه انتقال الفبای معمولی نسبت به خود این الفبا به رمز درآید، چه اتفاقی می‌افتد. من‌باب مثال، فرض کنید میزان انتقال، هشت حرف باشد. پس هربارکه حرف A در پیام صریح ظاهر می‌شود به‌جای آن I گذاشته می‌شود. برای نمایش نمادی این جایگذاری، قرار می‌گذاریم که حروف زبان صریح را با اندیس p و حروف رمزی را با اندیس c مشخص کنیم. پس قراردادن I از زبان رمزی به‌جای A از زبان صریح را به‌صورت $A_p = I_c$ نشان می‌دهیم. همچنین هربارکه B در پیام ظاهر شود، به‌جای آن J گذاشته خواهد شد، یعنی $B_p = J_c$. به‌جای هر حرف از پیام اصلی، هرجا که ظاهر شود، همیشه یک حرف، که معادل آن است، می‌آید. نتیجه آن است که نمودار توزیع فراوانی پیام رمزی همان نمودار توزیع فراوانی پیام صریح اولیه خواهد بود، با این تفاوت که به‌اندازهٔ ۸ مکان انتقال یافته است. اگر کلید ویژه عدد دیگری مانند n باشد، (نمودارِ) توزیع نیز به‌اندازهٔ n مکان انتقال می‌یابد.

اکنون باردیگر پیام رمزی صفحهٔ ۱۴ را در نظر می‌گیریم و تعداد هر یک از حرفهای آن را می‌شماریم. یک راه ساده برای این‌کار آن است که تمام حرفهای الفبا را بنویسیم و سپس پیام رمزی را حرف‌به‌حرف مرور کنیم، و برای هر حرف هربارکه پیش می‌آید یک نشانخط بگذاریم. استفاده از کاغذ شطرنجی مفید خواهد بود و نشانخط‌ها را می‌توان به دسته‌های ۵تایی دسته‌بندی کرد، به‌این ترتیب که هر پنج خط را، همان‌طور که در شکل صفحهٔ ۱۹ نشان داده شده است، یک دسته کنیم. وقتی‌که این عمل برای پیام رمزی کاملاً انجام شود، توزیع زیر به‌دست خواهد آمد:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
𝍸	𝍸	𝍷		𝍷				𝍸		𝍹	𝍷	𝍸	𝍺	𝍷	𝍹	𝍸		𝍷	𝍷	𝍺	𝍸	𝍸	𝍷		𝍸
𝍷	𝍺							𝍹				𝍸									𝍷	𝍹			𝍹
												𝍸													
												𝍸													

از آنجا که این نمودار، فراوانی تک‌تک حروف را نشان می‌دهد، توزیع فراوانی تک‌حرفی نامیده می‌شود. سعی می‌کنیم الگوی الفبای معمولی را در این توزیع بیابیم، مشاهده می‌کنیم که:

I و M و Q (همه با فراوانی زیاد) سه حرف در میان هستند، و M بیشترین فراوانی را دارد؛

V و W زوجی از حروف متوالی با فراوانیهای زیاد است؛

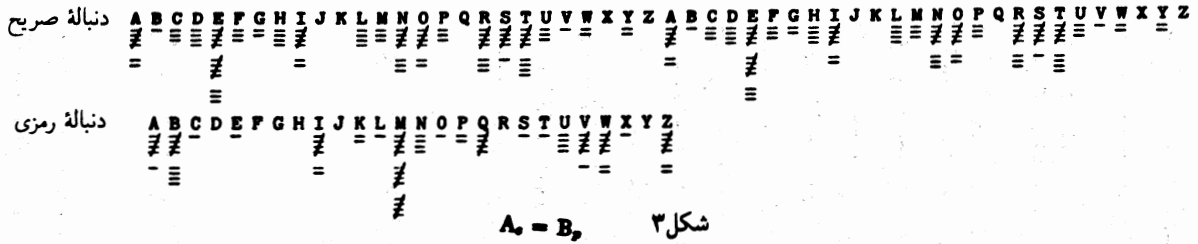
Z و A و B یک سه‌تایی از حروف متوالی با فراوانیهای زیاد است؛

C، D، E، F، G، H دنباله‌ای طولانی از حروف متوالی با فراوانیهای کم را تشکیل می‌دهند.

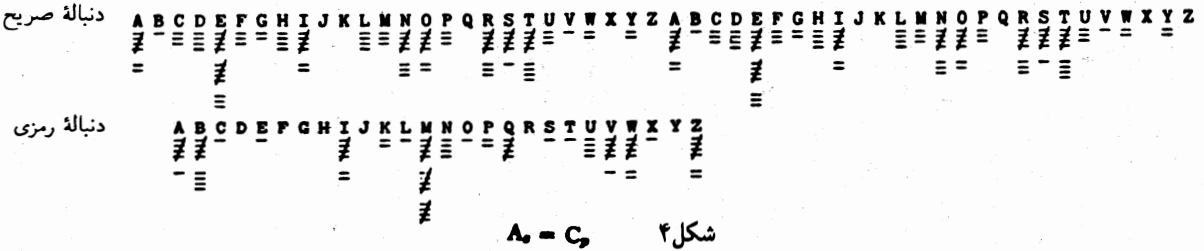
اگر قرار دهیم $I_c = A_p$، آنگاه تمام این مطالب با وضعیت یک الفبای متعارف مستقیم جور درمی‌آید؛ بنابراین، حرف I در این توزیع باید متناظر حرف A در الفبای معمولی باشد.

روش دیگر مشاهدهٔ این مطلب لغزاندن توزیع مربوط به رمز در مقابل توزیع مربوط به زبان صریح به‌گونه‌ای است که آنها با یکدیگر متناظر شوند. ابتدا توزیع زبان صریح را می‌نویسیم و برای آنکه عمل متناظرکردن ممکن باشد، آن را دوبار به‌دنبال هم می‌نویسیم. آنگاه توزیع رمز را مقابل آن قرار داده و هر بار به‌اندازهٔ یک حرف آن را می‌لغزانیم تا اینکه یک تناظر خوب از فراوانیها، یعنی زیادها در مقابل زیادها وکم‌ها در مقابل کم‌ها، به‌دست آید. اگر این دو توزیع را در دو صفحهٔ متفاوت قرار دهیم، آنگاه لغزاندن یکی در مقابل دیگری ساده‌تر خواهد شد. کار را با قراردادن A_c در مقابل B_p شروع می‌کنیم (شکل ۳ را ببینید). در این وضعیت، در تعداد کمی از مکانها می‌بینیم که فراوانیهای زیاد متناظر با فراوانیهای زیاد قرار گرفته‌اند، به‌عنوان مثال N_p و M_c، O_p و N_c، R_p و Q_c، A_p و Z_c. و نیز در تعداد کمی از مکانها فراوانیهای کم متناظر یکدیگر قرارگرفته‌اند: K_p و J_c، Y_p و X_c، Z_p و Y_c. اما موارد مهمی هم از عدم سازگاری وجود دارد: E_p، که بیشترین فراوانی را دارد، مقابل حرفی است که اصولاً ظاهر نمی‌شود؛ و سازگاری فراوانیها در زوجهای B_p و A_c، I_p و H_c، S_p و R_c، T_p و S_c، X_p و W_c بسیار ضعیف است. نتیجه می‌گیریم که این تناظر مناسب نیست.

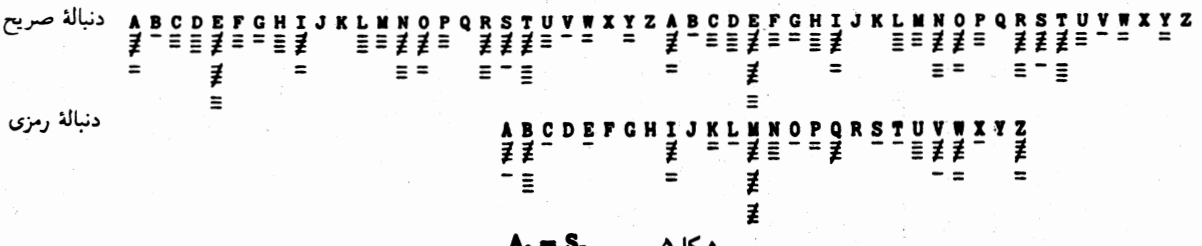
حال توزیع رمز را چنان انتقال می‌دهیم که $A_c = C_p$ و دو توزیع را مقایسه می‌کنیم (شکل ۴). دوباره نتیجه می‌گیریم که تناظر خوبی نداریم.



$A_0 = B_0$ شکل۳



$A_0 = C_0$ شکل۴



$A_0 = S_0$ شکل۵

این فرایند را ادامه می‌دهیم و هربار با تناظرهایی که رضایتبخش نیستند مواجه می‌شویم، تا اینکه به $A_c = S_p$ می‌رسیم (شکل ۵). در این وضعیت ملاحظه می‌کنیم که تناظر خوبی به‌دست آورده‌ایم. حروف با فراوانی زیاد از یک توزیع مقابل حروف با فراوانی زیاد از دیگری واقع‌اند؛ حروف با فراوانی کم نیز مقابل حروف با فراوانی کم قرار دارند. حتی یک جفت ناسازگار وجود ندارد. با به‌دست آوردن این تناظر از دو الگوی فراوانی، نتیجه می‌گیریم که سیستم کلی، یک الفبای متعارف مستقیم بوده است، و در الفبای جایگذاری مربوطه داریم $A_p = I_c$. خود الفبای جایگذاری از تناظر مکانهای دو توزیع فراوانی به‌دست می‌آید. وقتی از این الفبا در مورد پیام رمزی استفاده کنیم، پیام به زبان صریح به‌دست خواهد آمد، که دلیل قطعی صحت کار است.

تمرین

پیامهای زیر را با متناظر قراردادن توزیع آنها با توزیع فراوانی زبان صریح بگشایید:

۹. CQSOB KOHSF WG PZIS PSQOIGS RWFH DOFHWQZSG WB HVS KOHSF FSTZSQH GIBZWUVH PIH HVS KOHSF OPGCFPG FSR OBR MSZZCK HVS UFSSBG OBR PZISG HVOH OFS ZSTH AOYS HVS RSSD PZIS CQSOB

۱۰. SNHPJQ NX F MJFAD XNQAJW BMNYJ RJYFQQNH JQJRJSY NY NX RFLSJYNH YFPJX F MNLM UTQNXM FSI ITJX STY YFWSNXM TW WZXY JFXNQD

۶.۱ الفباهای مبتنی بر طرحهای چند درمیان دنبالهٔ معمولی

از آنجا که رمزسزاری ـ و همچنین تعمیم آن، یعنی انتقال به‌اندازهٔ تعداد دلخواهی حرف ـ نسبتاً به‌سهولت گشوده می‌شود، روشن است که چنین سیستمی دارای ایمنی بسیار کمی است.

اکنون روش متفاوتی را برای به رمز درآوردن پیام در نظر می‌گیریم. به‌جای افزودن یک عدد کلیدی به اعداد معادل حروف زبان صریح، آنها را در این عدد ضرب می‌کنیم. برای اینکه مثال ساده‌ای زده باشیم، عدد کلیدی ۲ را به‌کار می‌بریم.

به‌روشی مشابه با روشی که قبلاً، در صفحهٔ ۷، به‌کار بردیم عمل می‌کنیم:
(۱) به‌جای هر حرف از حروف الفبا عدد متناظرش را قرار می‌دهیم.
(۲) هر عدد را در ۲ ضرب می‌کنیم؛ اگر حاصل از ۲۶ تجاوز کرد، به‌جای آن ماندهٔ هم‌ارزش [به پیمانهٔ ۲۶] را قرار می‌دهیم.
(۳) به‌جای اعداد حاصل حروف متناظرشان را قرار می‌دهیم تا دنبالهٔ رمزی حاصل شود.

صریح :	A	B	C	D	E	F	G	H	I	J	K	L	M
(۱) :	1	2	3	4	5	6	7	8	9	10	11	12	13
(۲) :	2	4	6	8	10	12	14	16	18	20	22	24	26
مانده‌ها :	2	4	6	8	10	12	14	16	18	20	22	24	26
(۳) :	B	D	F	H	J	L	N	P	R	T	V	X	Z

صریح .:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(۱) :	14	15	16	17	18	19	20	21	22	23	24	25	26
(۲) :	28	30	32	34	36	38	40	42	44	46	48	50	52
مانده‌ها :	2	4	6	8	10	12	14	16	18	20	22	24	26
(۳) :	B	D	F	H	J	L	N	P	R	T	V	X	Z

الفبای جایگذاری حاصل عبارت است از:

صریح : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
رمزی : B D F H J L N P R T V X Z B D F H J L N P R T V X Z

اما این الفبای جایگذاری قابل‌قبول نیست. هر حرف دنبالهٔ رمزی در دو محل آمده است و بنابراین معادل دو حرف مختلف از زبان صریح خواهد بود. لذا نتیجهٔ فرایند از رمز درآوردن یگانه نخواهد بود، زیرا برای هر حرف رمزی دو امکان از زبان صریح وجود خواهد داشت. چنین سیستم ارتباطی سیستمی غیرقابل‌قبول است، زیرا هنگام از رمز درآوردن مواردی وجود خواهند داشت که حروف متفاوتی را می‌توان در مقابل حروف رمزی برگزید و راهی وجود ندارد که معلوم شود قصد فرستنده کدام‌یک بوده است.

این چندگانگی از کجا ناشی شده است؟ پاسخ آن است که حاصلضرب هر عددی در عدد ۲ همواره عددی زوج است و از آنجا که پیمانه نیز عددی زوج است، ماندهٔ هر عدد زوج همواره باید زوج باشد. به‌عبارت دیگر اگر a عددی زوج باشد، مثلاً $a = 2c$، آنگاه

رابطهٔ

$$a = b + k(۲۶)$$

نشان می‌دهد که

$$b = ۲c - k(۲۶) = ۲[c - k(۱۳)]$$

یعنی مانده زوج است. بنابراین وقتی x (معادل عددی حرف صریح) مقادیر از ۱ تا ۲۶ را اختیار می‌کند، $۲x$ (مقدار رمز) فقط اعداد زوج ۲،۴،۶، ... ،۲۶ را، هرکدام دوبار، اختیار می‌کند. یعنی، بااستفاده از این فرایند، به‌دست آوردن یک مجموعهٔ کامل مانده‌ها امکانپذیر نیست.

اگر هر عدد زوج دیگری نیز غیر از مضارب ۲۶ به‌عنوان ضریب به‌کار برده می‌شد، همین نتیجه به‌دست می‌آمد، یعنی در الفبای جایگذاری تنها ۱۳ حرف رمزی متفاوت وارد می‌شد.

اگر از ضرب در ۱۳ استفاده می‌کردیم، وضعیت از این هم بدتر می‌شد؛ برای تمام الفبا، تنها دو مانده وجود می‌داشت که عبارت بود از: ۱۳ و ۲۶. برای اینکه اگر عددی فرد باشد، از ضرب آن در ۱۳ عددی همنهشت با ۱۳ به‌دست می‌آید: زیرا هر عدد فرد به‌صورت $۲n + ۱$، که n عددی صحیح است، نوشته می‌شود، و از ضرب آن در ۱۳، عدد $۲۶n + ۱۳$ به‌دست می‌آید که با ۱۳ همنهشت است. اگر عددی زوج باشد به‌صورت $۲n$ نوشته می‌شود که وقتی در ۱۳ ضرب شود، $۲۶n$ که با ۲۶ همنهشت است به‌دست می‌آید.

آنچه موجب این مشکل می‌شود این واقعیت است که ۲ و ۱۳ مقسوم‌علیه‌های ۲۶ هستند. هر عدد که مضرب ۲ یا ۱۳ باشد، اگر به‌عنوان ضریب به‌کار رود، یک مجموعهٔ کامل مانده‌ها (به پیمانهٔ ۲۶) را تولید نخواهد کرد.

در اینجا مشاهده می‌کنیم که عمل ضرب در حساب همنهشتی ویژگیهایی دارد که آن را از ضرب معمولی متمایز می‌سازد. خصوصاً، از آنجا که هر عدد فردِ مضرب ۱۳، با هر عدد فرد دیگر مضرب ۱۳ همنهشت است، نتیجه می‌شود که ممکن است ax با bx همنهشت باشد بدون آنکه a با b همنهشت باشد. این موضوع در مورد تساوی معمولی صادق نیست. بدین معنی که ممکن است در حساب همنهشتی، در عکس عمل ضرب، یک مسألهٔ تقسیم بیش از یک جواب داشته باشد. برای مثال، اگر (پیمانهٔ ۲۶) $۲x \equiv ۲$، آنگاه $x = ۱$ و $x = ۱۴$ هردو جواب هستند.

به‌ازای هر پیمانهٔ دلخواه n، اگر ضریب a با n عامل مشترکی داشته باشد، از ضرب a در عددهای از ۱ تا n، مجموعهٔ کامل مانده‌ها تولید نخواهد شد. ولی اگر a و n نسبت به هم اول باشند (یعنی هیچ عامل مشترکی نداشته باشند) این مشکل پیش نخواهد آمد. در چنین موردی اگر x را به‌نوبت برابر با ۱، ۲، ... ، $n-1$، n بگیریم، آنگاه از ضرب a در x همهٔ این اعداد، گرچه با ترتیبی دیگر، تولید خواهند شد، یعنی هیچ عددی تکرار نخواهد شد.

قبل از اثبات این مطلب، آن را با یک مثال ساده روشن می‌سازیم. فرض کنید پیمانه ۱۲ و ضریب ۵ باشد. اعداد ۱، ۲، ... ، ۱۲ را در ۵ ضرب کرده و حاصلضربها را به پیمانهٔ ۱۲ تحویل می‌کنیم:

	1	2	3	4	5	6	7	8	9	10	11	12
اعداد ضرب در ۵ :	5	10	15	20	25	30	35	40	45	50	55	60
مانده‌ها :	5	10	3	8	1	6	11	4	9	2	7	12

سطر مانده‌ها، با ترتیبی غیر از ترتیب عددها، شامل ۱ تا ۱۲ است.

حال ثابت می‌کنیم که اگر ضریب a و پیمانهٔ n نسبت به هم اول باشند، آنگاه تمام مانده‌های حاصل از a، $2a$، ... ، na متمایزند.

فرض کنید a عامل مشترکی با n نداشته باشد. همچنین فرض کنید که x و y اعداد مختلفی از مجموعهٔ $\{1, 2, \ldots, n\}$، و x کوچکتر از y باشد. این مطلب با نماد $1 \leq x < y \leq n$ نمایش داده می‌شود. می‌خواهیم ثابت کنیم که به پیمانهٔ n، ax با ay همنهشت نیست.

فرض کنید

$$a \text{ و } n \text{ نسبت به‌هم اول‌اند} \qquad \text{و} \qquad ay \equiv ax \ (\text{پیمانهٔ } n)$$

در این صورت

$$ay - ax \equiv 0 \ (\text{پیمانهٔ } n)$$

با توجه به تعریف همنهشتی، این رابطه به مفهوم آن است که $ay - ax$ مضربی از n، مثلاً kn، است:

$$ay - ax \equiv a(y - x) = kn.$$

از آنجا که a و n عامل مشترکی ندارند، $x - y$ باید همهٔ عاملهای n را شامل باشد، یعنی $x - y$ مضربی از n است.* اما از آنجا که $1 \leq x < y \leq n$، داریم $0 < y - x < n$، بنابراین $x - y$ نمی‌تواند مضربی از n باشد. از این تناقض برمی‌آید که اگر a نسبت به پیمانهٔ n اول باشد، و اگر x و y اعداد متمایزی از مجموعهٔ مانده‌های $\{1, \ldots, n\}$ باشند، آنگاه ax با ay همنهشت نیست.

نتیجه می‌شود که هر همنهشتی به شکل $ax \equiv b \ (n)$ (پیمانهٔ n)، که در آن اعداد صحیح a و n نسبت به هم اول باشند، دارای جوابی یکتاست. زیرا هرگاه x به‌نوبت مقادیر ۱، ...، n را اختیار کند، ax دارای n ماندهٔ متمایز خواهد بود (طبق آنچه هم‌اکنون ثابت کردیم، هیچ دوتایی از اینها باهم مساوی نیستند)، و هرکدام به مجموعهٔ $\{1, 2, \ldots, n\}$ تعلق خواهند داشت. بنابراین، ماندهٔ b (از این مجموعه) دقیقاً با یکی از مانده‌های متمایز ax برابر می‌شود، و آن x که این مانده را نتیجه می‌دهد جواب یگانهٔ معادلهٔ (پیمانهٔ n) $ax \equiv b$ است.

اگر n زیاد بزرگ نباشد، عدد x را می‌توان با امتحانِ هر یک از مقادیر ممکن از ۱ تا n به‌دست آورد.

مثال:

۱. $3x \equiv 1 \ (7)$ (پیمانهٔ ۷) $\qquad x = 5$

۲. $4x \equiv 2 \ (5)$ (پیمانهٔ ۵) $\qquad x = 3$

برای حل چنین معادله‌های همنهشتی، روشهای کلی وجود دارند که بحث آن خارج از حوزهٔ این کتاب است. اما این به آن معنی نیست که خواننده مجبور است اعداد متوالی را یکی پس از دیگری امتحان کند تا جواب صحیح را بیابد. با ضرب دو طرف یک همنهشتی در عددی که نسبت به پیمانه اول باشد، آن را به یک همنهشتی معادل تبدیل کنید. این عدد را که در دو طرف ضرب می‌کنید چنان انتخاب کنید که مقدار ضریب x را کاهش دهد. این کار را با همنهشتی جدید تکرار کنید و کاهش ضریب x را تا آنجا ادامه دهید که

* این حکم نتیجهٔ قضیهٔ اساسی حساب است، که بنابر آن، برای تجزیهٔ n، a و $x - y$ به عوامل اوّل تنها یک راه وجود دارد. برای اثبات این حکم، می‌توانید قضیهٔ ۲.۴ از کتاب اعداد : گویا و گنگ [از همین مجموعه کتب پیش‌دانشگاهی] را ببینید.

به ۱ یا ۱− تبدیل شود.

برای روشن‌شدن مطلب، فرض کنید که مقصود حل معادلهٔ زیر باشد:

$$۱۹x \equiv ۱ \quad (\text{پیمانهٔ } ۲۶)$$

چون (پیمانهٔ ۲۶) $-۷ \equiv ۱۹$، می‌توانیم بنویسیم:

$$-۷x \equiv ۱ \quad (\text{پیمانهٔ } ۲۶)$$

با ضرب دو طرف در ۳ به‌دست می‌آید:

$$-۲۱x \equiv ۳ \quad (\text{پیمانهٔ } ۲۶)$$

و از آنجا که

$$-۲۱ \equiv ۵ \quad (\text{پیمانهٔ } ۲۶)$$

می‌نویسیم.

$$۵x \equiv ۳ \quad (\text{پیمانهٔ } ۲۶)$$

با ضرب دو طرف در ۵ به‌دست می‌آید:

$$۲۵x \equiv ۱۵ \quad (\text{پیمانهٔ } ۲۶)$$

و با استفاده از

$$۲۵ \equiv -۱ \quad (\text{پیمانهٔ } ۲۶)$$

به دست می‌آید:

$$-x \equiv ۱۵ \quad (\text{پیمانهٔ } ۲۶)$$

با ضرب دو طرف در ۱− جواب به‌صورت زیر به‌دست می‌آید:

$$x \equiv -۱۵ \equiv ۱۱ \quad (\text{پیمانهٔ } ۲۶)$$

جواب x برای معادلهٔ همنهشتی $ax \equiv ۱$ (پیمانهٔ n)، وارونِ a نسبت به ضرب نامیده شده و با $a^{-۱}$ نمایش داده می‌شود. وارون هر عدد را معکوس آن عدد نیز می‌نامند. بنابراین، از مثال بالا معلوم می‌شود که در همنهشتی به پیمانهٔ ۲۶، عدد ۱۹ معکوس عدد ۱۱ است. یک عدد در حساب همنهشتی دارای معکوس است اگر و فقط اگر نسبت به پیمانه اول باشد.

اگر جدولی از اعداد و معکوس‌آنها را در همنهشتی به پیمانهٔ ۲۶ داشته باشیم، آنگاه یک جواب (پیمانهٔ ۲۶) $ax \equiv b$ بلافاصله از ضرب b در معکوس a، یعنی در a^{-1}، به‌دست می‌آید، زیرا

$$x \equiv a^{-1}b \text{ (پیمانهٔ ۲۶)}$$

حال به موضوع ساختن الفبای جایگذاری از راه عمل ضرب برمی‌گردیم، و عدد ۳ را به‌عنوان ضریب در نظر می‌گیریم.

صریح :	A	B	C	D	E	F	G	H	I	J	K	L	M
(۱) :	1	2	3	4	5	6	7	8	9	10	11	12	13
(۲) :	3	6	9	12	15	18	21	24	27	30	33	36	39
مانده :	3	6	9	12	15	18	21	24	1	4	7	10	13
(۳) :	C	F	I	L	O	R	U	X	A	D	G	J	M

صریح :	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
(۱) :	14	15	16	17	18	19	20	21	22	23	24	25	26
(۲) :	42	45	48	51	54	57	60	63	66	69	72	75	78
مانده :	16	19	22	25	2	5	8	11	14	17	20	23	26
(۳) :	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

الفبای جایگذاری قابل‌استفاده‌ای که حاصل می‌شود عبارت است از:

صریح :	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی :	C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z

به‌همین روش می‌توان هر عدد فرد دیگری (به‌استثنای مضربهای ۱۳) را به‌عنوان ضریب به‌کار برد و یک الفبای جایگذاری بنا کرد.

حال الفبای حاصل از ضرب در عدد ۳ را با نگرش دیگری بررسی می‌کنیم. از آنجا که مقدارهای عددیِ حروف در الفبای معمولی اعداد صحیح متوالی‌اند و ما آنها را در عدد ۳ ضرب کرده‌ایم، فاصلهٔ هر دو عدد متوالی از دنبالهٔ رمزیِ معادلهای عددی، سه واحد است. به‌عبارت دیگر، برای به‌دست آوردن دنبالهٔ رمزی از دنبالهٔ صریح می‌توان پس از هر حرفی سومین حرف بعد از آن را نوشت. بنابراین اگر دنبالهٔ رمزی را مانند مثال بالا با حرف C آغاز کنیم، حرف بعد از آن، سه حرف پس از C، یعنی F است؛

آنگاه سه حرف بعد از F، I می‌شود؛ سه حرف بعد از I، L است و الی آخر. هرگاه در این فرایند به‌حرف X برسیم، سه حرف بعد از آن A خواهد بود، سپس D و ... . با ادامهٔ این فرایند، دنبالهٔ کامل رمزی به‌دست خواهد آمد. این شیوه که هربار یک حرف از دنباله به فاصلهٔ ثابتی از حرف قبلی انتخاب شود، شیوهٔ طرح چند در میان خوانده می‌شود. الفبایی که در آن دنبالهٔ رمزی، به‌شیوهٔ طرح چند در میان، از دنبالهٔ صریح به‌دست آید، الفبای باطرح چند در میان نامیده می‌شود. استفاده از طرح چند در میان با یک فاصله، معادل است با استفاده از عمل ضرب در عدد متناظر با آن فاصله.

جالب توجه است که الفبای متعارف وارونه، که در رمزنگاری ارتش آمریکا به‌کار می‌رفت (صفحهٔ ۱۲)، یک طرح چند در میان الفبای معمولی است که متناظر است با ضریب ۲۵ (یا معادل آن، ۱−).

استفاده از عمل ضرب، یک نوع سیستم کلی به‌دست می‌دهد که با سیستم کلی الفبای متعارف مستقیم متفاوت است. عدد کلیدی منسوب به هر پیام بخصوص، امکان آن را فراهم می‌آورد که با عمل ضرب به روش بالا، یک الفبای جایگذاری ساخته شود؛ و با این الفبا، فرایندهای به رمز درآوردن و از رمزدرآوردن انجام‌پذیر هستند.

تمرین

۱۱. معادله‌های همنهشتی زیر را حل کنید:

الف) (پیمانهٔ ۱۷) $۴y + ۲ \equiv ۲y + ۵$ ب) (پیمانهٔ ۹) $۶x \equiv ۳$

۱۲. معکوس ۵ را در همنهشتی به پیمانهٔ ۷ به‌دست آورید.

۱۳. در همنهشتی به پیمانهٔ ۶، چه عددهایی معکوس ندارند؟ به پیمانهٔ n چطور؟

۱۴. الف) در یک طرح چند در میان الفبای معمولی، حرفهای U، B، I، P پشت سرهم واقع شده‌اند. فاصلهٔ طرح چند درمیان چقدر است؟

ب) این فاصله را به‌عنوان ضریب درنظر بگیرید و الفبای جایگذاری را بسازید.

ج) با این الفبای جایگذاری پیام زیر را از رمز درآورید:

AVBIV KC DIGXITC PKVCJ FGE

۷.۱ گشودن الفباهای متعارفِ با طرح چند در میان

با الفبایی که به‌روش طرح چند در میان فراهم شده است، یک پیام به رمز درآمده است. رمزگشا چگونه می‌تواند از عهدهٔ گشایش این پیام برآید؟ فرض کنیم پیام رمزیی که به گشایش آن علاقه‌مندیم به‌صورت زیر باشد:

VNY BYRVEIWR BLYDYLQ VNEV OWRQOLSBVSWRQ TALSRI
VNY RYPV VNLYY MWRVNQ JY METY SR VNY EIY JLEOCYVQ
RSRYVYYR VW VKYRVU WRY

به‌عنوان اولین قدم، توزیع فراوانی حرفهای رمزی را به‌دست می‌آوریم:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
−	≡	−	−	≠				≡	=	−	≠	=	≠	≡	−	≠	≠	≠	=	−	≠	≠		≠	
											−		−				≠				≠	−		≠	
																	≡				≠			≠	
																								≡	

به‌نظر نمی‌رسد که الگوی فراوانیهای به‌دست آمده با الگوی یک الفبای متعارف مستقیم مطابقت کند. اگر این توزیع را در مقابل توزیع الفبای معمولی بلغزانیم، در وضعیتهایی، برای حرفهای خاصی فراوانیهای زیاد را با فراوانیهای زیاد مطابق خواهیم یافت، اما این تطابق برای حروف دیگر بسیار ضعیف خواهد بود. هیچ وضعیتی که در آن یک تطابق سرتاسری مناسب برای دو توزیع داشته باشیم به‌دست نخواهیم آورد. از این‌رو باید نتیجه بگیریم که سیستم رمز، سیستم الفبای متعارف مستقیم نیست.

یک شیوهٔ عملی ممکن، کوشش برای شناسایی بعضی از حروف است. برای مثال، می‌توانیم حدس بزنیم که Y_c، که بیشترین فراوانی را دارد، احتمالاً E_p است. و نیز V_c یا اینکه R_c ممکن است T_p باشد.

برای مشاهدهٔ اینکه این حدسها تا چه‌اندازه مناسب‌اند، به مکانهایی در متن رمزی که آن حروف ظاهر شده‌اند نگاه می‌کنیم. متوجه می‌شویم که کلمهٔ رمزی VNY سه مرتبه ظاهر شده است. اگر V_c همان T_p و Y_c همان E_p باشد، آنگاه بدون شک VNT همان کلمهٔ THE خواهد بود، که نتیجهٔ خوبی به‌نظر می‌رسد، یعنی ظاهراً معقول است که

تشخیص سه حرف رمزی مذکور را قطعی بدانیم. حال معادلهای عددی این حروف رمزی و حروف صریح را می‌نویسیم:

	صریح	رمزی
T	۲۰	۲۲
H	۸	۱۴
E	۵	۲۵

اگر سیستم کلی سیستمی مبتنی بر ضرب باشد، انتظار می‌رود که سه همنهشتی زیر

$$۲۰k \equiv ۲۲ \pmod{۲۶}$$

$$۸k \equiv ۱۴ \pmod{۲۶}$$

$$۵k \equiv ۲۵ \pmod{۲۶}$$

سازگار باشند، و جواب مشترک آنها برای k ضریبی باشد که در جستجوی آن هستیم. در دو همنهشتی اول، اعداد ۲۰ و ۸ در عامل ۲ با ۲۶ مشترک‌اند. بنابراین در این همنهشتیها بیش از یک مقدار برای k صدق می‌کند. اما از آنجا که ۵ و ۲۶ عامل مشترک ندارند، همنهشتی سوم تنها یک جواب دارد. به‌سادگی معلوم می‌شود که این جواب عبارت است از $k = ۵$.

اگر در دو همنهشتی اول و دوم، ۵ را به‌جای k قرار دهیم، به‌دست می‌آوریم:

$$۲۰(۵) = ۱۰۰ \equiv ۲۲ \pmod{۲۶}$$

$$۸(۵) \equiv ۴۰ \equiv ۱۴ \pmod{۲۶}$$

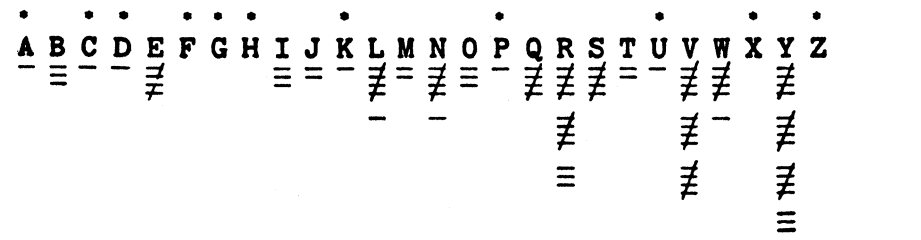
که مؤید صحت تشخیصِ T_p و H_p است. بنابراین $k = ۵$ جواب مربوط به همهٔ حالتهاست. به‌نظر می‌رسد که الفبای جایگذاری از راه طرح چند در میان و با ضریب ۵ ساخته شده باشد. اگر این الفبا را بسازیم و آن را برای رمزگشایی به‌کار ببریم، درخواهیم یافت که این موضوع صحیح است، و با استفاده از این الفبا، پیام صریح اولیه به‌دست می‌آید.

روشی که هم‌اکنون ارائه شد، راحتترین راه برای گشایش پیام رمزی مفروض بود. این روش بر این پایه است که قسمتی از متن صریح را حدس می‌زنیم و سپس فرض می‌کنیم که سیستم کلی رمز، الفبایی با طرح چند در میان است. اکنون روش متفاوتی را به‌کار

می‌بریم تا همین مسأله را حل کنیم. روشی که مبتنی بر هیچ فرضی نیست، بلکه صرفاً مبتنی بر استفاده از توزیع فراوانی است.

قبلاً توزیع فراوانی پیام رمزی مفروض را در مقابل توزیع الفبای معمولی بررسی کرده‌ایم و دریافته‌ایم که امکان مطابقت دو توزیع، با لغزاندن یکی در مقابل دیگری، وجود ندارد. این موضوع ما را متقاعد می‌سازد که سیستم کلی، الفبای متعارف مستقیم نبوده است و در الفبای جایگذاری مربوطه به‌جای حروف متوالی دنبالهٔ صریح حرفهایی گذاشته شده که در الفبای معمولی احتمالاً متوالی نیستند، یعنی پس‌وپیش شده‌اند. شاید مطابقت توزیع رمز و توزیع معمولی را به‌روش دیگری نیز بتوان پیدا کرد. شاید بر اساس فراوانیهای حروف رمزی بتوان جایگشت منظمی از آنها به‌دست آورد که ترتیب آنها را در دنبالهٔ رمزی معین کند. آنگاه شاید با استفاده از آن بتوان الفبای جایگذاری را بازسازی کرد.

بهترین راه برای جستجوی چنین جایگذاری، کوشش در کشف زوجهایی از حروف رمزی است که با حرفهایی متوالی از دنبالهٔ صریح معادل باشند. متذکر می‌شویم که در توزیع فراوانی حرفهای زبان صریح، جفت O ،N و نیز سه‌تایی R، S، T از حروف با فراوانی زیاد هستند. به‌علاوه جفت J، K و دنبالهٔ U، V، W، X، Y، Z از حروف با فراوانی کم هستند. باتوجه به اینکه چنین دنباله‌ای از حروف با فراوانی کم داریم، ابتدا به حرفهای با فراوانی کم نگاه می‌کنیم. توزیع رمز را درنظر گرفته و بالای هر حرف رمزیی که فراوانی آن کم است، مثلاً بیش از یک بار ظاهر نشده، یک علامت می‌گذاریم. (بدیهی است که این روش، روشی آماری است و تمام حروفی که به آنها علاقه‌مندیم در این روش مورد بررسی قرار نمی‌گیرند. اگر در یک پیام برخی از واژه‌های غیرعادی به‌کار رفته باشند، حرفی که آن واژه‌ها شاملش هستند، ولی معمولاً دارای فراوانی بسیار کمی است، ممکن است چند باری ظاهر شود. برعکس، یک یا چند حرف که معمولاً فراوانی زیادی دارند، ممکن است در این پیام بخصوص به‌ندرت ظاهر شوند یا حتی اصلاً ظاهر نشوند. بنابراین مجموعهٔ حروفی که بررسی خواهیم کرد، ممکن است دقیقاً مجموعهٔ حروف موردنظر ما نباشد، اما اگر بخت یار باشد، بیشتر آنها به این مجموعه تعلق خواهند داشت.)



برای مشاهدهٔ آنکه آیا حروف انتخاب شده در یک نوع وضعیت منظم قرار گرفته‌اند یا نه، علامتها را بررسی می‌کنم. اولین چیزی که مشاهده می‌کنیم آن است که K، P، U، Zبه فاصله‌های مساوی از یکدیگر قرار گرفته‌اندـیعنی چهار حرف در میان. اگر از Kبه‌اندازهٔ ۵ محل به عقب برگردیم به F می‌رسیم؛ ۵ محل قبل از F نیز حرف A قرار دارد، و تمام این ۶ حرف علامتگذاری شده‌اند. به‌علاوه، X، C و Hنیز به همین فاصله از یکدیگر قرار دارند. رشته حرفهای A، F، K، P، U، Z با وضعیت حروف نادر از U تا Z در الفبای معمولی مطابقت می‌کند. رشتهٔ X، C، H ممکن است شامل J، K باشد، اما به سومین حرف، یعنی H، باید توجه کرد. سه‌تایی مذکور احتمالاً I، J، K نیست، شاید J، K، L باشد. در این رشتهٔ طولانی حروف شواهد کافی برای اظهار این عقیده وجود دارد که احتمالاً با یک الفبای با طرح چند در میان سروکار داریم. در واقع پیش از امتحان طرح چند در میان، نیازی به جستجوی شواهد بیشتر نیست، اما جالب است مشاهده کنیم که از بین حروف با فراوانی زیاد، فاصلهٔ R و W پنج حرف است، و فاصلهٔ بین حروف L، Q، V نیز همین‌قدر است؛ دوتایی اول حروف صریح N و O، و سه‌تایی بعدی حروف R، S و T را تداعی می‌کند.

این واقعیتها ما را برآن می‌دارد که دنبالهٔ رمزی را چهار در میان (یعنی با فاصلهٔ پنج) طرح کرده و ببینیم چه وضعیتی پیش می‌آید. با شروع از حرف A، دنباله‌ای می‌سازیم که هر حرفِ آن ۵ محل دورتر از حرف ماقبل خود در الفبای معمولی قرار داشته باشد. ضمن این عمل، زیر هر حرف، نشانهٔ فراوانی آن را در رمز، مطابق آنچه در توزیع فراوانی تک‌حرفی آمده، می‌آوریم.

A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V
−		−	−	−		≠	=	≡	=	≠	−	≡	≠	≠		−		=	≠	≠	≡		≠	≠	≠
										≠			−						≠	−			−		≠
										≠									≡						≠
										≡															

حال در الگوی مشخصهٔ فراوانیهای زیاد و کم حرفها، ظاهر کلی یک الفبای معمولی را مشاهده می‌کنیم. علاوه بر مجموعهٔ حروفی که در پاراگراف قبل ذکر شد، الگوی A، E، Iرا در حروف E، Y، S مشاهده می‌کنیم. برای اینکه کاملاً مطمئن شویم، این توزیع را

در مقابل توزیع معمولی می‌لغزانیم و در حالت $A_p = E_c$، یک تطابق عالی به‌دست می‌آوریم. در این وضعیتِ تطابق، الفبای جایگذاری ساخته شده عبارت است از:

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V	A	F	K	P	U	Z

و به‌دنبال آن این امکان را به‌دست می‌آوریم که تمام پیام را از رمز درآوریم. متن پیام چنین‌است:

THE PENTAGON PREFERS THAT CONSCRIPTIONS DURING
THE NEXT THREE MONTHS BE MADE IN THE AGE BRACKETS
NINETEEN TO TWENTY ONE.

[پنتاگون ترجیح می‌دهد که سربازگیری در طی سه ماههٔ آینده در محدودهٔ سنی ۱۹ تا ۲۱ سال انجام گیرد.]

به این نکته توجه کنید که رشتهٔ X C H، از دنبالهٔ رمزی نمایانگر رشتهٔ J K L از دنبالهٔ صریح است و درعین‌حال L در متن صریح ظاهر نمی‌شود.

تمرین

پیامهای رمزی زیر را بگشایید:

۱۵. SPSV CV XTS MIXTSMIXCAID OACSVASO EGF NFCVACNID
CVOXFGMSVXO XE JCOAEPSF XTS XFGXT IFS CVJGAXCEV IVJ
IVIDEKQ

۱۶. SV SQ VNY OWMMWR KWRTYL WD EHH MYR NWK EMWRI QW MERU
MSHHSWRQ WD DEOYQ VNYLY QNWAHT JY RWRY EHSCY

۸.۱ رمزهای تک‌الفبایی مبتنی بر تبدیلهای خطی

فرض کنید دو ایده‌ای که برای ساختن سیستم کلی شرح داده شد، یعنی انتقال الفبا و ضرب در یک عدد ثابت، با هم ترکیب شوند. به‌عنوان مثال، فرض کنید دنبالهٔ رمزی را الفبای سزاری بگیریم و هر حرف را در ۵ ضرب کنیم:

صریح :	A	B	C	D	E	F	G	H	I	J	K	L	M
معادل عددی :	1	2	3	4	5	6	7	8	9	10	11	12	13
C_1 (جمع با ۳) :	4	5	6	7	8	9	10	11	12	13	14	15	16
ضرب در ۵ :	20	25	30	35	40	45	50	55	60	65	70	75	80
مانده :	20	25	4	9	14	19	24	3	8	13	18	23	2
C_2 :	T	Y	D	I	N	S	X	C	H	M	R	W	B

صریح :	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
معادل عددی :	14	15	16	17	18	19	20	21	22	23	24	25	26
C_1 (جمع با ۳) :	17	18	19	20	21	22	23	24	25	26	1	2	3
ضرب در ۵ :	85	90	95	100	105	110	115	120	125	130	5	10	15
مانده :	7	12	17	22	1	6	11	16	21	26	5	10	15
C_2 :	G	L	Q	V	A	F	K	P	U	Z	E	J	O

در این‌صورت الفبای جایگذاری که C_2 دنبالهٔ رمزی آن است با رابطهٔ $C = 5(P + 3)$ یا $C = 5P + 15$ متناظر خواهد بود، که در آن، C نمایانگر معادل عددی حروف رمزی و P نمایانگر معادل عددی حروف صریح است.

این الفبای جایگذاری را، که در دو مرحله به‌دست آمد، می‌توان با محاسبهٔ $5P + 15$ برای هر حرف صریح در یک مرحله ساخت.

رابطه‌ای مانند

$$C = aP + b$$

که در آن a و b ثابت‌اند به تبدیل خطی معروف است، زیرا متغیرهای C و P با رابطه‌ای خطی، یعنی رابطه‌ای که تنها شامل توانهای اول متغیرهاست به‌هم مربوط‌اند.

سیستمِ مبتنی بر انتقال و سیستم مبتنی بر ضرب در مقدار ثابت که قبلاً بررسی شدند موارد خاصی از تبدیلهای خطی هستند. در مورد الفبای متعارف مستقیم، a برابر ۱ است. بنابراین رابطهٔ خطی تبدیل می‌شود به $C = P + b$؛ b مقداری است که هر حرف صریح به‌اندازهٔ آن انتقال داده می‌شود و ماندهٔ $P + b$ به پیمانهٔ ۲۶ حروف رمزی را نتیجه می‌دهد. در مورد طرح چند در میان، b مساوی صفر است، بنابراین رابطه به $C = aP$ تبدیل می‌شود؛ a ضریبی است که طرح چند در میان را نتیجه می‌دهد.

اگر دو طرف مکاتبه قرارگذارند که از تبدیل خطی استفاده کنند، تدبیری می‌اندیشند که به طریقی به هر پیام دو عدد نسبت دهند. این دو عدد، a و b، رابطهٔ خطی $C = aP + b$

را معین خواهند کرد که با آن می‌توان الفبای جایگذاری را به‌دست آورد.

اکنون گشایش یک پیام رمزی را، که فرض می‌کنیم بااستفاده از یک الفبای رمزی نوشته شده باشد که از الفبایی معمولی از راه یک تبدیل خطی به‌دست آمده، بررسی می‌کنیم. یک شیوهٔ کار این است که حرفهای صریحِ معادل بعضی از حرفهای رمزی را تشخیص دهیم. معادل عددی هر حرف رمزی همنهشت با معادل عددی حرف صریحِ معادل با آن است؛ از این همنهشتیها باید دو مجهول a و b، یعنی مقادیر ثابت تبدیل خطی را پیدا کنیم. بنابراین امکان دارد که تنها تشخیص دو حرف برای رسیدن به جواب کافی باشد. برای این تشخیص، از فراوانی حرفها و نیز حدسهایی دربارهٔ کلمات زبان صریح استفاده می‌کنیم.

فرض کنید پیام زیر را داریم:

GYOMXNOGNG QUGN ETNMX MPLMZOMXYM K TMMJOXA XEN
TKZ ZMQEBMF TZEQ KJKZQ EX YEXNMQLJKNOXA NHM TJEEF
ET XMI CXEIJMFAM IHOYH MKYH WMKZ RZOXAG IONH ON

برای این پیام توزیع فراوانی به‌قرار زیر است:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
≡	−	−		≠	≡	≠	≠	≡	≠	≠	=	≠	≠	≠	−	≠	−		≠	−		−		≠	≠	≠
				≠						=		≠	≠	≡					−				≠		=
												≠												−		
												=														

اگر فرض کنیم حرفی که بیشترین فراوانی را دارد، یعنی M_c، همان E_p باشد، و یکی از حرفهای رمزی E، N، O، X، همان T_p باشد، آنگاه محتمل به‌نظر می‌رسد که NHM معادل رمزی کلمهٔ THE باشد.

رمزی	معادل‌عددی	صریح	معادل عددی
N	۱۴	T	۲۰
H	۸	H	۸
M	۱۳	E	۵

از این تشخیص آزمایشیِ سه‌حرف، سه رابطهٔ همنهشتی که شامل معادلهای عددی آنها هستند به دست می‌آید. هر کدام از این همنهشتیها با جایگزین کردن معادلهای عددی حروف مشخص‌شدهٔ فوق در همنهشتی زیر به‌دست می‌آید:

$$C \equiv aP + b \quad (\text{پیمانهٔ } ۲۶)$$

که در اینجا a و b به‌ترتیب ضریب و اندازهٔ انتقال هستند. بنابراین:

$$۱۴ \equiv ۲۰a + b \quad (\text{پیمانهٔ } ۲۶)$$

$$۸ \equiv ۸a + b \quad (\text{پیمانهٔ } ۲۶)$$

$$۱۳ \equiv ۵a + b \quad (\text{پیمانهٔ } ۲۶)$$

اگر همنهشتی سوم را از دومی کم کنیم، خواهیم داشت:

$$۳a \equiv -۵ \equiv ۲۱ \quad (\text{پیمانهٔ } ۲۶)$$

$$a = ۷$$

این مقدار a را در همنهشتی سوم قرار می‌دهیم تا مقدار b را به‌دست آوریم:

$$۳۵ + b \equiv ۱۳ \quad (\text{پیمانهٔ } ۲۶)$$

$$b \equiv -۲۲ \equiv ۴ \quad (\text{پیمانهٔ } ۲۶)$$

$$b = ۴$$

جوابهای a و b بدون استفاده از همنهشتی زیر

$$۱۴ \equiv ۲۰a + b \quad (\text{پیمانهٔ } ۲۶)$$

به‌دست آمدند، اما در این همنهشتی صدق می‌کنند، زیرا

$$۲۰(۷) + ۴ \equiv ۱۴۴ \equiv ۱۴ \quad (\text{پیمانهٔ } ۲۶)$$

بنابراین، الفبای جایگذاری با استفاده از تبدیل خطی $C = ۷P + ۴$ ایجاد می‌شود:

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X	E	L	S	Z	G	N	U	B	I	P	W	D

با این الفبا پیام را از رمز درمی‌آوریم. متن اصلی عبارت است از:

SCIENTISTS MUST OFTEN EXPERIENCE A FEELING NOT FAR REMOVED FROM ALARM ON CONTEMPLATING THE FLOOD OF NEW KNOWLEDGE WHICH EACH YEAR BRINGS WITH IT

[دانشمندان باید در بررسی سیل اطلاعات جدیدی که هر سال فرا می‌رسد، اغلب اوقات احساسی تقریباً شبیه احساس نگرانی داشته باشند]

از خواننده می‌خواهیم نشان دهد که مانند مثال قبل، از راه به‌کار بردن توزیع فراوانی نیز می‌توان همین نتیجه را به‌دست آورد. با علامتگذاری حروفِ با فراوانی کم و امتحان فواصل ممکن بین آنها مشاهده می‌شود که فاصلهٔ ۷ محتملترین فاصله است. دسته‌های زیر شش حرف در میان هستند: V و C؛ U و B؛ P و W و D. از آنجا که فاصلهٔ B تا P برابر ۱۴ است، می‌توانیم دو مجموعهٔ اخیر را به‌ترتیب زیر در یک گروه ترکیب کنیم:

$$U, B, \ldots, P, W, D$$

این مجموعه، با مجموعهٔ حروف U تا Z از زبان صریح که W_p از آن حذف شده باشد، متناظر است.

اگر حروف الفبا را با فاصلهٔ ۷ طرح کنیم، و فراوانی آنها را نیز همراهشان بیاوریم (چنانکه در صفحهٔ ۳۴ عمل کردیم)، دنبالهٔ جدید در وضعیت $A_p = K_c$، با دنبالهٔ معمولی مطابقت می‌کند. از این راه همان الفبای جایگذاری بالا فراهم می‌شود و می‌توان پیام را از رمز درآورد.

وقتی متن صریح بازسازی شد، معلوم می‌شود که علت وجود جای خالی در دنبالهٔ D، W، P، ـ ، B، U آن بوده که حرف صریح W چهار مرتبه در پیام آمده، و در نتیجه فراوانی آن در این پیام کم نبوده است.

تمرین

۱۷. همنهشتیهای زیر را حل کنید:

الف) (پیمانهٔ ۱۱) $۳x + ۷ \equiv ۹$

ب) (پیمانهٔ ۱۳) $۴y + ۶ \equiv ۰$

ج) (پیمانهٔ ۲۳) $۲x + ۱ \equiv ۹x - ۴$

۱۸. همنهشتیهای زیر را حل کنید:

الف) (پیمانهٔ ۹) $۳x \equiv ۶$

ب) (پیمانهٔ ۲۶) $۵x - ۱ \equiv ۳x + ۱$

۱۹. معکوس عددهای زیر را پیدا کنید:

الف) (پیمانهٔ ۱۷)۷

ب) (پیمانهٔ ۲۶)۹

ج) (پیمانهٔ ۳۱)۳

پیامهای رمزی زیر را بگشایید:

۲۰. JDI HVANGNKFKJS JDGJ EI MGS PGKF KT G EAVJDS UGQCI KC TAJ CQPPKUKITJ RQCJKPKUGJKAT PAV AQV VIPQCKTW JA CQHHAVJ KJ

۲۱. MZ WZOGZWWJ GS EIZEWJZWN ZIB IZHU CGBX BXW NWSGOZ IF MRRMJMBKS VKB CGBX GBS IRWJMBGIZ VU XKQMZ VWGZOS

۲۲. PU AOL AOLVYF VM UBTILYZ PA OHWWLUZ YHAOLY MYLXBLUASF AOHA IF ZVTL BULEWLJALK SBJR AOL TVZA LSLNHUA ULD AYBAOZ ZWYPUN BW IF PUKBJAPVU

۲۳. R FX SNO FGYFRQ NG ONXNYYNZ GNY R WFEL TLLS PLTOLYQFP FSQ R CNEL ONQFP

۲۴. Z UZMZGRX RH Z KVIHLM DSL RH SRTSOB VMGSFHRZHGRX ZYLFG HLNVGSRMT RM DSRXS BLF ZIV MLG VEVM IVNLGVOB RMGVIVHGVW

۲۵. LE ULK LMC KZIE WZ LWC DWPE EFVERWEZIET NLE HKQ KP CIWEZNWPWI IREMNWKZ UWDD ZEJER PKRAEN WN LE UWDD XE DKZAWZA NK REZEU WN

۲۶. BDSTGC WXHIDGN AXZT P STPU BPC PCHLTGH FJTHIXDCH CD DCT PHZTS

۲۷. AH TNA PEPC UPBNTP DCPNQ HC DHHI PSBPOQ QKCHXDK TNAZ NAI DCPNQ TRJQNFPJ

۲

جایگذاری تک‌الفبایی کلی

۱.۲ الفبای درهم‌ریخته

در فصل اول دیدیم که برای گشودن یک الفبای جایگذاری که با تبدیل خطی از دنبالهٔ معمولی الفبا به‌دست آمده باشد، حداکثر با دو مقدار مجهول مواجهیم: یکی فاصلهٔ طرح چند در میان، یعنی فاصلهٔ حرفیِ بین حروف متوالی دنبالهٔ رمزی، و دومی مقدار تغییرمکان دنبالهٔ رمزی نسبت به دنبالهٔ صریح. برای گشایش متن رمزیی که از این راه ایجاد شده باشد، معمولاً پیداکردن معادل غیررمزی دو حرف رمزی کافی است. زیرا، اگر بدانیم حروف رمزی با معادلهای عددی C_1 و C_2، با حروفی از دنبالهٔ صریح متناظرند که معادلهای عددی آنها P_1 و P_2 است، می‌توانیم دو همنهشتی زیر را بنویسیم:

$$C_1 \equiv aP_1 + b \pmod{۲۶} \qquad a = \text{فاصلهٔ طرح چند در میان}$$

$$C_2 \equiv aP_2 + b \pmod{۲۶} \qquad b = \text{اندازهٔ انتقال}$$

که از حل آنها مقدارهای a و b به‌دست می‌آید. (بعضی وقتها ممکن است ابهامی پیش آید، مانند زمانی که یک همنهشتی بیش از یک جواب داشته باشد، اما در چنین وضعیتی تنها لازم است که جوابهای ممکن بررسی شوند تا معلوم شود که کدام‌یک از آنها پیام صریح را به‌دست خواهد داد.) اگر رمزگشا بتواند معادل تعداد بیشتری از حروف یا معادل یک کلمهٔ کامل را در زبان صریح به‌دست آورد، آنگاه تعداد بیشتری همنهشتی در

اختیار خواهد داشت که عدم وجود ابهام در تعیین عددهای کلیدی را تضمین خواهند کرد.

بنابراین چنین به‌نظر می‌رسد که اگر کسی خواهان ایمنی پیام باشد، باید الفبای جایگذاری خود را با روشی پیچیده‌تر از روش استفاده از رابطهٔ خطی طرح کند. اگر الفبای جایگذاری با چنان شیوه‌ای ساخته شده باشد که دانستن معادل چند حرف رمزی، اطلاعاتی دربارهٔ معادلهای حروف دیگر به‌دست ندهد، آنگاه بازسازی الفبای جایگذاری بسیار مشکلتر خواهد بود. برای مثال، دنبالهٔ رمزی را می‌توان با انتخاب تصادفی حروف الفبا ساخت. مثلاً، فرض کنید ۲۶ حرف الفبا را روی تکه‌های کاغذ نوشته و در کلاهی قرار دهیم، سپس آنها را به‌هم زده و هر بار یکی از آنها را انتخاب کنیم. از این دنبالهٔ حروف انتخابی، یک الفبای جایگذاری حاصل می‌شود که در آن معادل صریح هر حرف رمزی مستقل از معادلهای دیگر است. یک مثال از چنین الفبایی، که الفبای تصادفی نامیده می‌شود، به‌قرار زیر است:

صریح : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
رمزی : Q N T L R A X U G C P K B Z F I V D H M O W E Y S J

در بیشتر مسأله‌های رمزنگاری که در مجله‌ها و روزنامه‌ها مطرح می‌شوند از الفباهایی استفاده می‌شود که به‌طور تصادفی تولید شده‌اند. از نظر ارتباطی، یک اشکال چنین الفباهایی، مشکل به خاطر سپردن دنبالهٔ رمزی آنهاست. اگر نوشتن دنباله لازم باشد، خطر گم‌شدن یا دزدیده شدن آن وجود دارد. از اینجا این فکر پیش می‌آید که برای ایجاد دنبالهٔ رمزی، روشی با نظامی خاص به‌کار رود که هم ساختن دنباله را آسان کند و هم آن‌قدر درهم‌ریختگی پدید آورد که بیشتر مزایای روش تصادفی حاصل شود. برای به‌دست آوردن چنین دنباله‌هایی طرحهای مبتکرانهٔ بسیاری ارائه شده است؛ بدون شک خواننده هم می‌تواند طرحهایی را ابداع کند. به‌عنوان مثال، دو شیوه‌ای را که بیشتر مورد استفاده واقع می‌شوند به‌اختصار شرح می‌دهیم.

در روش اوّل دنباله‌ای رمزی به‌دست می‌آید که به دنبالهٔ درهم مبتنی بر کلمهٔ کلیدی موسوم است. مخاطب چنین پیامهایی برای از رمز درآوردن آنها تنها به حفظ کردن یک کلمهٔ مهم، یعنی کلمهٔ کلیدی، نیاز دارد. به‌عنوان مثال، فرض کنید کلمهٔ کلیدی DEMOCRATIC باشد. در ساختن دنبالهٔ رمزی، اولین مرحله آن است که کلمهٔ کلیدی را حرف‌به‌حرف نوشته و هر حرف تکراری را حذف کنیم. اگر این کار را با کلمهٔ DEMOCRATIC انجام دهیم، کلمهٔ DEMOCRATI به‌دست می‌آید؛ حرف Cی آخر کلمه حذف شده، زیرا قبلاً در

پنجمین محل آمده است. سپس دنبالهٔ رمزی را با نوشتن سایر حروف الفبا به‌ترتیب معمولی کامل می‌کنیم. اگر در مثال خود این کار را انجام دهیم، دنبالهٔ رمزی زیر را به‌دست می‌آوریم:

D E M O C R A T I B F G H J K L N P Q S U V W X Y Z

حال الفبای جایگذاری با نوشتن دنبالهٔ رمزی زیر دنبالهٔ صریح معمولی به‌دست می‌آید. البته، باید دربارهٔ نحوهٔ قراردادن دنباله‌ها در مقابل یکدیگر قراری گذاشته شده باشد. این کار را می‌توان با ذکر معادل یک حرف رمزی انجام داد. معمول آن است که حرف اول کلمهٔ کلیدی را در زیر حرف A از دنبالهٔ صریح بنویسند. در این‌صورت، در مورد مثال بالا، خواهیم داشت $A_p = D_c$.

صریح : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
رمزی : D E M O C R A T I B F G H J K L N P Q S U V W X Y Z

اگر چنین الفبای جایگذاری برای به رمز درآوردن پیامی به‌کار رود، رمزگشایی که می‌کوشد آن را بگشاید، پیش از بازسازی تمام دنبالهٔ رمزی، باید به تعداد کافی معادل صریح حروف رمزی برای یافتن کلمهٔ کلیدی تعیین کند.

اگر به‌نظر آید که از این فرایند به‌اندازهٔ کافی درهم‌ریختگی حاصل نمی‌شود، می‌توان آن را به‌طریق زیر اصلاح کرد. پس از اینکه کلمهٔ کلیدی را بدون حرفهای تکراری آن نوشتیم، بقیهٔ حروف الفبا را در سطرهایی متوالی زیر این کلمهٔ کلیدی می‌نویسیم:

D E M O C R A T I
B F G H J K L N P
Q S U V W X Y Z

سپس حروف را به‌روش معروف به انتقال ستونی به‌طور قائم می‌خوانیم: نخست ستون ۱ را می‌خوانیم ، پس از آن ستون ۲، سپس ستون ۳، تا به‌آخر که نتیجهٔ آن دنبالهٔ درهم‌ریختهٔ زیر خواهد بود:

D B Q E F S M G U O H V C J W R K X A L Y T N Z I P

این دنبالهٔ رمزی که آن را با عنوان دنبالهٔ درهم‌ریختهٔ انتقالی مبتنی بر کلمهٔ کلیدی نام می‌بریم، هم بیشتر مزیتهای الفبای به‌دست آمده از فرایند کاملاً تصادفی را داراست، و هم می‌توان آن را با یک کلمهٔ کلیدی قراردادی، مطابق قاعده ساخت.

استفاده از چنین دنباله‌ای ایرادی جزئی دارد که در فرایند از رمز درآوردن بروز می‌کند، اما به‌سادگی می‌توان آن را برطرف کرد. اگر قرار باشد الفبای جایگذاریِ

صریح: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
رمزی: D B Q E F S M G U O H V C J W R K X A L Y T N Z I P

برای از رمز درآوردن پیامی به‌کار رود، لازم است که در دنبالهٔ رمزی دنبال حرفی که می‌خواهیم از رمز درآوریم بگردیم. برای رفع این مشکل، می‌توان الفبا را چنان مرتب کرد که حروف رمزی به ترتیب معمولی الفبایی واقع شوند. ضمن این کار، در عین اینکه هر حرف رمزی را در موضع الفبایی خود قرار می‌دهیم، حرف صریح متناظرش را نیز با آن جابه‌جا می‌کنیم. از این ترتیب مجدد الفبای جایگذاری دنباله‌های زیر حاصل می‌شود:

صریح: S B M A D E H K Y N Q T G W J Z C P F V I L O R U X
رمزی: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

در این ترتیب جدید (که می‌توان تغییر دیگری هم در آن داد، به‌این ترتیب که دنبالهٔ رمزی را بالای دنبالهٔ صریح نوشت) الفبای جایگذاری را الفبای از رمز درآوری می‌نامند، و در مقابل آن الفبایی را که دنبالهٔ صریح آن به‌ترتیب معمولی است الفبای به رمز درآوری می‌نامند. بدیهی است که این دو شکل، یک الفبای جایگذاری به‌دست می‌دهند. این دو نمایانگر این واقعیت‌اند که برای به‌دست آوردن الفبای درهم‌ریخته، تفاوتی ندارد که دنبالهٔ صریح را درهم بریزیم یا دنبالهٔ رمزی را.

تمرین

۲۸. کلمه‌های کلیدی پدیدآورندهٔ هر یک از دنباله‌های درهم زیر را تعیین کنید. (نقطه‌ها به‌جای حروف مجهول به‌کار رفته‌اند.) توجه کنید که انتهای دو دنبالهٔ اوّل نشان می‌دهد که انتقال ستونی در کار نبوده است:

(الف) S E C R T M A G B D F H I J K L N O P Q U V W X Y Z
(ب) U N I T E D A O S B C F G H J K L M P Q R V W X Y Z
(ج) U B M Y N C O Z I F P T G Q E H R D J V S K W A L X
(د) W A H . Y I B J Q Z R . K T E D . . L F N V S G O X
(ه) N A U E B V W C X . D Z O F R G . H T J I L M . S Q

۲.۲ گشودن الفباهای درهم‌ریخته

اکنون به بررسی گشایش پیامی رمزی می‌پردازیم که با الفبایی درهم‌ریخته به رمز درآمده باشد. طبق معمول برای روشن ساختن مطلب، مثالی می‌زنیم تا به ارائهٔ ایده‌های لازم کمک کرده باشیم. پیام از این قرار است:

UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ

برای اقدام به حل این مسأله، در قدم اول توزیع تک‌حرفی آن را تشکیل می‌دهیم:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
=	=		≠	≠	≡	=	≠	−	−			≠		≠	≠	≡		≠	≡	≠	≠	≡	≠	=	≠
			−	−			=					≡		≡	≠			≠		≠					≠
															≠										≡
															−										

اگر کوشش کنیم توزیع فراوانی معمولی را با این توزیع مطابقت دهیم، هیچ وضعی نخواهیم یافت که در آن توزیعها با یکدیگر مطابقت کنند. اگر از راه طرح چند در میان هم برای تبدیل این توزیع مجهول به توزیع معمولی تلاش کنیم توفیقی نمی‌یابیم. نتیجهٔ این مطالب آن است که این رمز با تبدیلی خطی به‌دست نیامده است. بنابراین الفبای جایگذاری باید درهم‌ریخته باشد.

برای گشایش رمزی که بر پایهٔ یک الفبای جایگذاری درهم‌ریخته بنا شده است، تعیین معادلهای صریح بعضی از حروف رمزی و درپی آن از رمز درآوردن یک یا چند کلمهٔ متن اصلی لازم است. اگر بتوانیم به قسمتی از پیام اصلی دست یابیم، معمولاً خواهیم توانست تمام متن را بازسازی کنیم. شیوه‌های مؤثر برای چنین دستیابی به قسمتی از پیام، برپایهٔ ویژگیهای زبان، و برپایهٔ چگونگی ترکیب حَروف با یکدیگر برای ساختن کلمه‌های زبان، بنا شده‌اند. این شیوه‌ها تحت سه عنوان اصلی قرار می‌گیرند.

درگشایش یک پیام رمزی، از آن‌گونه که ما سعی درگشایش آن داریم، فراوانی نسبی ظاهرشدن حرفها یک وسیلهٔ کمکی اولیه است. بااستفاده از توزیع تک‌حرفی که ارائه کردیم،

می‌توانیم حروفی را با فراوانی زیاد، حروف دیگری را با فراوانی متوسط، و همین‌طور حروفی را با فراوانیهای دیگر، تشخیص دهیم. ممکن است این اطّلاعات به‌تنهایی برای تشخیص قطعی کافی نباشد، به‌ویژه اگر پیام چندان طولانی نباشد. به‌طور کلی، با استفاده از این اطلاعات تنها می‌توان برای بعضی حرفهای رمزی مجموعه‌ای از معادلهای صریح احتمالی تعیین کرد. مثلاً در مسألهٔ موردبحث، محتمل به‌نظر می‌رسد که P_c و Z_c معادل E_p و T_p باشند، امّا حتی اگر چنین باشد، باز این سؤال باقی است که کدام‌یک معادل کدام یک است. حروف H_c، M_c، D_c، S_c، U_c، که فراوانی زیادی دارند، احتمالاً با حرفهای متعلق به مجموعهٔ $\{A, I, N, O, R, S\}$ از زبان صریح معادل‌اند. همچنین محتمل است که اغلب حروف با فراوانی کم، یعنی A_c، B_c، I_c، J_c، Q_c، T_c، Y_c با حروفی از مجموعهٔ $\{G, J, K, Q, V, W, X, Y, Z\}$ معادل باشند.

اطلاعات قابل‌استنتاج از فراوانیهای تک‌حرفی را می‌توان با اطلاعات مربوط به حرفهای آغاز و پایان کلمه‌ها تکمیل کرد: در بررسی متنی از روزنامه که بالغ بر ۱۶۰۰۰ کلمه بوده، از ده حرفی که بیش از حرفهای دیگر در آغاز یا در پایان کلمه‌ها ظاهر شده‌اند، فهرستی به‌شرح زیر به‌دست آمده است:

حرف آغازی	تعداد کلمات	حرف پایانی	تعداد کلمات
T	**2,614**	**E**	**3,325**
A	**1,802**	**S**	**2,077**
S	**1,213**	**D**	**1,649**
O	**1,176**	**N**	**1,592**
I	**922**	**T**	**1,587**
C	**918**	**R**	**906**
W	**833**	**Y**	**903**
P	**768**	**F**	**745**
B	**757**	**O**	**744**
F	**666**	**L**	**599**

حال بااستفاده از این داده‌ها نشان می‌دهیم که چگونه می‌توان P_c و Z_c را با معادلهای احتمالی آنها، E_p و T_p، متناظر کرد. در پیام موردبحث ما Z_c هم به‌عنوان حرف آغازی و هم به‌عنوان حرف پایانی دارای فراوانی زیاد بوده، اما P_c به دفعات به‌عنوان حرف پایانی

ظاهر شده، و ابداً به‌عنوان حرف آغازی ظاهر نشده است. بنابراین محتملتر به‌نظر می‌رسد که T_p معادل Z_c باشد نه P_c.

هریک از حروف نادر (بافراوانی کم) Q_c و T_c آغاز دو کلمه‌اند. احتمالاً معادلهای آنها در مجموعهٔ حرفهای نادر $\{C, W, P, B, F\}$، آن حرفهایی هستند که معمولاً در آغاز کلمه‌ها ظاهر می‌شوند.

به‌طور کلی، بااستفاده از فراوانیهای تک‌حرفی و فراوانیهای حروف آغازی و پایانی، ممکن است مجموعه‌ای از معادلهای احتمالی برخی از حروف رمزی به‌دست آید. معمولاً نباید انتظار داشته باشیم که تنها با بررسی فراوانیها، اطلاعات دقیقتری دربارهٔ معادلهای صریح به‌دست آوریم.

روش عمدهٔ بعدی درگشایش رمزهای تک‌الفبایی، تلاش برای تشخیص حروف صدادار از حروف بی‌صداست. یک راه مهم برای این منظور، بررسی کلمه‌های کوتاه، مثلاً دو، سه یا چهارحرفی است. می‌دانیم که چنین کلماتی باید شامل یک حرف صدادار باشند. شاید بااستفاده از این کلمات کوتاه بتوان حرفهایی از پیام رمزی را یافت که نمایشگر حروف صدادار باشند. چنین اطلاعاتی کمک زیادی در به‌دست آوردن جواب خواهد کرد. از این‌رو در پیام موردبحث به کلمه‌های دوحرفی UZ، MB، UD توجه می‌کنیم. از کلمهٔ MB نتیجه می‌گیریم که M_c یا B_c حرفی صدادار است و از آنجا که فراوانی B_c بسیار کم است، محتملتر به‌نظر می‌رسد که M_c حرفی صدادار باشد، البته این احتمال هم هست که $B_c = Y_p$. از کلمات UZ و UD، نتیجه می‌گیریم که یا U_c حرفی صدادار است یا اینکه هم Z_c و هم D_c حروف صدادارند. درصورت اخیر، U_c حرفی بی‌صدا خواهد بود. اما اگر U_c حرفی بی‌صدا باشد، آنگاه کلمه‌های UZ و UD چه کلمات صریحی ممکن است باشند؟ ممکن است ME و MY، یا BE و BY باشند و به‌نظر می‌رسد که اینها تقریباً تنها حالتهای ممکن باشند. از آنجا که فراوانی U_c بیشتر از آن است که این حرف متناظر با B_p یا M_p باشد، این حالتها چندان محتمل به‌نظر نمی‌رسند.

پس محتمل به‌نظر می‌رسد که U_c حرفی صدادار و Z_c و D_c حروفی بی‌صدا باشند. اگر Z_c حرفی بی‌صدا باشد، آنگاه از کلمهٔ ZWP استنباط می‌شود که یکی از حرفهای W_c یا P_c صدادار است. اما از آنچه قبلاً باتوجه به فراوانیها دربارهٔ P_c و Z_c ملاحظه شد، نتیجه می‌شود که P_c حرف صدادار احتمالی کلمهٔ ZWP است.

سوّمین روشی که به‌کار می‌بریم، روش «کلمات الگودار» است. از کلمه‌هایی که در آنها حرفهایی تکرار می‌شوند و این تکرار الگوی مشخصی دارد، نمونه‌های زیادی وجود دارد. این الگو در رمز نیز حفظ می‌شود، زیرا در فرایند جایگذاری، به‌جای هر حرف از متن صریح، هربار که ظاهر شود، همواره یک حرف رمزیِ معادل گذاشته می‌شود. برای مثال، کلمه‌هایی مانند BEGINNING، COMMITTEE، PEOPLE، TOMORROW، DIVISION، NONSENSE را اغلب می‌توان از وضعیت نسبی حرفهای تکراریشان شناخت، به‌ویژه اگر اطلاعات مربوط به فراوانی، با فراوانی نسبی حرفهای آنها سازگار باشد، همچنین اگر دانسته‌های مربوط به حرفهای صدادار و بی‌صدا با کلمه سازگار باشند. با تمرین و تجربه می‌توان بسیاری از کلمه‌های الگودار را تشخیص داد. کتابهایی دربارهٔ مجموعهٔ الگوهای کلمه‌ها انتشار یافته است که در آنها این الگوها چنان مرتب شده‌اند که جستجو و یافتن کلمه‌ها، برطبق الگوی کلمه‌های پیام رمزی ممکن است. علاوه بر این گاهی قراین خاص مربوط به پیام، دال بر موضوع کلی آن است. مثلاً ممکن است احتمال داده شود که پیامی شامل کلمهٔ خاصی باشد، مانند اسم یک فرد یا یک محلّ یا یک کالا، و این اسم الگویی مشخص از تکرار حرفهایی در املای خود داشته باشد. اگر پیام شامل چنان کلمه‌ای باشد، با تعیین حرفهای تکراری آن می‌توان به‌کمک الگوی این تکرار، محل آن کلمه را در پیام رمزی کشف کرد.

لزومی ندارد که این کلمه‌های الگوارِ قابل‌استفاده طولانی باشند. بعضی وقتها، کلمه‌هایی مانند THAT، WHICH، WHERE را می‌توان براساس حرفهای تکراریشان شناخت. حتی عدم وجود الگو نیز ممکن است مفید واقع شود. بنابراین یک کلمهٔ بسیار طولانی بدون هیچ حرف تکراری ـباتوجه به فراوانی حرفهای آن‌ـ ممکن است تنها یک معادل صریح احتمالی داشته باشد.

به‌علاوه، لازم نیست الگوها منحصر به کلمات باشند. عبارتهایی مانند FROM TIME TO TIME، AS SOON AS و ON ACCOUNT OF به‌آسانی قابل تشخیص‌اند. در یک پیام رمزی، ممکن است که از تشخیص تنها یک کلمه، یا یک عبارت، یا حتی تعداد کمی از حرفهای پراکنده، قسمتی از پیام مشخص شود که مدخلی برای گشودن تمام پیام باشد.

حال ببینیم چگونه می‌توانیم این شیوه‌ها را برای حل مسأله‌ای که با آن مواجهیم به‌کار ببندیم. بافرض آنکه U_c حرفی صدادار و Z_c حرفی بی‌صدا (و احتمالاً همان T_p) باشد،

ملاحظه می‌کنیم که کلمهٔ ZWSZ شبیه THAT است. اگر این فرض درست باشد، آنگاه ZWP ممکن است کلمهٔ بسیار معمول THE باشد و در این‌صورت ترکیب

```
WSFP  APPD
h..e  .ee.
```

عبارت HAVE BEEN را تداعی می‌کند.

اگر این کلمه‌ها را در جای خود در پیام قرار دهیم و سپس زیر هر حرف از رمز که در آنها به‌کار رفته است (یعنی هر حرف از رمز که به‌طور آزمایشی تشخیص داده شده است) معادل صریح آن را بنویسیم، به‌دست می‌آوریم:

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
 t  a          e   e te  a  that  eve a   n     a  b t

VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
  e t   nta t  have been  a e   th      t  a

EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
 e  e e tat ve     the v et   n   n
```

حال نتیجه می‌شود که اولین کلمهٔ پیام AT یا IT است. اما توجه کنید که A_p را معادل S_c دانسته بودیم، بنابراین $U_c = I_p$.

با تعیین این حرف جدید، آشکار می‌شود که کلمهٔ رمزی QUZW همان WITH است و آنگاه از اینکه W_p معادل Q_c است معلوم می‌شود که کلمهٔ دوّم پیام باید WAS باشد. فراوانی حروف I_p، W_p، S_p با فراوانی معادلهای احتمالی آنها، یعنی U_c، Q_c و O_c، متناسب است. I_p و S_p، چنانچه باید باشند، حرفهایی با فراوانی زیاد هستند، و W_p حرفی با فراوانی کم است. اکنون پیام به‌صورت زیر ظاهر می‌شود:

```
UZ QSO VUOHXMOPV GPOZPEVSG ZWSZ OPFPESX UDBMETSX AIZ
it was  is   se   este  a  that seve a  in    a  b t

VUEPHZ HMDZSHZO WSFP APPD TSVP QUZW YMXUZUHSX
 i e t   nta ts have been  a e with    iti a

EPYEPOPDZSZUFPO MB ZWP FUPZ HMDJ UD TMOHMQ
 e  esentatives    the viet   n   n   s  w
```

از حرفهایی که تا اینجا به‌دست آمده‌اند ترکیبهای واقعاً خوبی را ملاحظه می‌کنیم، و ممکن است قادر باشیم دربارهٔ بعضی از کلمه‌هایی که بیشتر حروفشان پیدا شده‌اند، حدسهای نسبتاً خوبی بزنیم. برای مثال، کلمه‌های YESTERDAY، SEVERAL و REPRESENTATIVES، همه الگوهایی قابل تشخیص دارند که بایستی بررسی شوند. بدیهی به‌نظر می‌رسد که کلمه‌های نزدیک به انتهای پیام VIET CONG باشند.

به‌جای حدس کلمه فوق، باتوجه به اینکه حرفهای بافراوانی زیاد N_p، O_p، R_p هنوز تشخیص داده نشده‌اند، می‌توان این حرفهای صریح را به‌نوبت با حرفهایی از رمز امتحان کرد که آنها نیز فراوانی زیادی دارند و هنوز شناخته نشده‌اند. چنین فرایندی قطعاً به تشخیص حروف بیشتری منجر خواهد شد. تنها با مقداری کار دیگر، متن کامل پیام قابل‌حصول خواهد شد. این متن چنین است:

IT WAS DISCLOSED YESTERDAY THAT SEVERAL INFORMAL BUT DIRECT CONTACTS HAVE BEEN MADE WITH POLITICAL REPRESENTATIVES OF THE VIET CONG IN MOSCOW

[دیروز فاش شد که چند تماس غیررسمی ولی مستقیم با نمایندگان سیاسی ویت‌کنگ‌ها در مسکو انجام گرفته است.]

به‌عنوان گام نهایی در حل این مسأله علاقه‌مندیم که درصورت امکان الفبای جایگذاری کامل را بازسازی کرده و تعیین کنیم که چگونه ایجاد شده است. چنین اطلاعاتی ممکن است در رمزگشایی مکاتبات دیگر طرفین همان مکاتبه باارزش باشد. اطلاع از فرایندها و روشهای رمزنگاریِ فرستندگان پیامها ممکن است بسیار مفید باشد.

الفبای جایگذاری به‌دست آمده از پیامی که هم‌اکنون گشوده شد عبارت است از:

صریح : **A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**
رمزی : **S A H V P B J W U . . X T D M Y . E O Z I F Q . G .**

دنبالهٔ رمزی چند جای خالی دارد، زیرا متن اصلی پیام همهٔ ۲۶ حرف الفبا را شامل نبوده است.

به‌این نکته توجه کنید که در دنبالهٔ رمزی، حرفهای V، W، X، Y، Z سه در میان واقع شده‌اند. اگر این حرفها را در یک ردیف بنویسیم، و سپس بالای هرکدام از آنها سه‌حرفی را بنویسیم که در دنبالهٔ رمزی، قبل از آن آمده‌اند، به‌دست خواهیم آورد:

S P U T .
A B . D E
H J . M O
V W X Y Z

حال حرفهای شناخته‌شده و استفاده نشده از بقیهٔ دنبالهٔ رمزی را چنان به جدول می‌افزاییم که حرفهای F و G در سطر دوم واقع شده جای خالی بین E و H را پر کنند:

S P U T . I .
A B . D E F G
H J . M O Q .
V W X Y Z

حرف C را که تا به‌حال تشخیص نداده‌ایم می‌توانیم بین B و D قرار دهیم. حال مشاهده می‌کنیم که یک دنبالهٔ درهم‌ریختهٔ انتقالی ستونی مبتنی بر کلمهٔ کلیدی در اختیار داریم. کلمهٔ کلیدی شامل ۷ حرف است که ۵تای آنها تشخیص داده شده‌اند. حرف ششم باید N باشد (که حرف جاافتادهٔ بین M و O است)، حرف هفتم این کلمه نیز یا Kاست یا L. بسیار محتمل به‌نظر می‌رسد که کلمهٔ کلیدی کلمهٔ SPUTNIK باشد که در آن‌صورت تمام دنبالهٔ رمزی قابل بازسازی خواهد بود.

مثال بالا نشان می‌دهد که در اغلب موارد چگونه می‌توان یک رمز تک‌الفبایی را گشود. سرنخهایی که از فراوانی نسبی حرفهای رمزی و از کلمه‌های کوتاه به‌دست می‌آیند با اطّلاعات مربوط به الگوها همراه می‌شوند و تعیین معادل بعضی از حرفها را ممکن می‌سازند. سپس این حرفها به‌جای حرفهای رمزی معادلشان در هر جای پیام که ظاهر شده باشند قرار داده می‌شوند؛ از آنجا معادلهای حرفهای دیگری تداعی می‌شوند، و متن به‌تدریج آشکار می‌شود.

حلّ چنین مسأله‌هایی اساساً فقط به تمرین و تجربه بستگی دارد. اگر پیام به‌اندازهٔ کافی طولانی باشد دستیابی به مدخلی برای گشودن پیام فقط محتاج صرف وقت است.

گشایش رمزهایی از این‌گونه را بیش از این ادامه نخواهیم داد، زیرا این‌گونه رمزها حالت خاصی از رمزهای مطرح شده در مبحث بعدی‌اند.

تمرین

متنهای رمزی زیر را بگشایید:

۲۹. XTEIA DSL ASQA FKSF FKY IVYOPYUJQ NI PAY NI LNVRA TU
SMYVTJSU UYLAESEYV YUCDTAK SUR FKYTV VSUG NVRYV SVY
JDNAYDQ VYDSFYR

۳۰. HCB RWOEUWY NXHY QM QWIUFOKBN SQLOBHY OS HQ BFPUWIB HCB POTBS UFN OFLWBUSB HCB SHUFNUWN QM POTOFI QM UPP HCB RBQRPB

۳.۲ گشودن رمزهای تک‌الفبایی که در دسته‌های پنج‌حرفی نوشته شده‌اند

روشن است که در مثال قبل دسته‌بندی حرفها در متن رمزی برطبق طول واقعی کلمه‌ها فایدهٔ زیادی درگشایش آن داشته است. اطلاع از طول کلمه‌ها ـ و استفادهٔ احتمالی از الگوی آنها ـ اساس کار درگشایش اغلب متنهای رمزی روزنامه‌ای و مجله‌ای است. اگر اطلاعی از محلّ آغاز و پایان کلمه‌ها نداشته باشیم، وضعیت کاملاً متفاوت خواهد بود. درواقع، ایجاد چنین وضعیتی ـ یعنی حذف طول کلمه‌ها ـ گام بعدی در بهترکردن، یعنی پیچیده‌ترکردن متنهای رمزی است.

فرض کنید متنی رمزی در دسته‌های پنج‌حرفی نوشته شده است. (علت انتخاب این عدد آن است که در مکاتبات تجاری مرتباً با آن مواجه می‌شویم و این دسته‌بندی معمولترین دسته‌بندی در مکاتبات رمزی است.) به‌عنوان مثال، پیامِ

MYTKI JIRUL AZOAH MIJAC UYGII JIUJA CHETR JMRUY MJFAG
RMRPJ FTMEX ALAZU YMRQM OAZEX OAZRU ARTRI TGELG IJHAR
JITJU AVYMO YVTLV IFMPY UXIOM XIUAP A

را چگونه می‌توان گشود؟

اگر توزیع فراوانی تک‌حرفی آن را تشکیل دهیم، خواهیم داشت:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
≠		=		≡	≡	≡	=	≠	≠	−	≡	≠		≠	≡	−	≠		≠	≠	≡		≡	≠	≡
≠								≠	≠			≠					≠		=	≡				=	
≡								=				−													

اگر فرض بر این باشد که این رمز مبتنی بر تبدیل خطی است، با این توزیع هیچ کوششی به نتیجه نخواهد رسید.

به‌کمک توزیع فراوانی تک‌حرفی می‌توانیم حرفهای رمزی را به دسته‌هایی با فراوانی زیاد، متوسط و کم تقسیم کنیم. آنگاه، مثلاً، می‌توان گفت که حرفهای رمزیِ با فراوانی

زیاد، یعنی حرفهای A، I، J، M، R، T، U و Y احتمالاً دارای معادلهایی صریح در بین حرفهای E، T، N، R، O، I، A و S هستند.

سپس بد نخواهد بود که اطلاعاتی دربارهٔ حرفهای بی‌صدا و صدادار به‌دست آوریم، شاید بتوانیم حرفهایی رمزی را تعیین کنیم که معادلشان در بین حرفهای A، E، I و Oباشند یا حرفهای دیگری را به‌دست آوریم که معادلشان بین حرفهای N، R، S و Tباشند. در مثال قبل کلمه‌های کوتاهی که هر کدام می‌بایست شامل یک حرف صدادار باشد، به کمک ما آمدند. فعلاً از این کمک محرومیم. اما می‌توانیم از این مطلب استفاده کنیم که هر بخش یک کلمه [انگلیسی] باید شامل یک حرف صدادار باشد. برای آنکه در این راه پیشرفتی داشته باشیم، از اطلاعات مربوط به چگونگی ترکیب حرفها با یکدیگر استفاده می‌کنیم.

در مقایسه با فراوانی مشخصهٔ حرفهای مجزا، از الگوهای زبانی، اطلاعات بیشتری قابل‌استنتاج است. در تعداد بسیار زیادی از متنها، دوحرفیها (ترکیبهای دوحرفی) و سه‌حرفیها (ترکیبهای سه‌حرفی) را شمرده‌اند. مانند تک‌حرفیها، این ترکیبها نیز با فراوانیهای مشخصه‌ای ظاهر می‌شوند، که معمولاً در بین نمونه‌های متفاوت تفاوت چندانی نمی‌کند. این فراوانیهای مشخصه در حل برخی از مسائل رمزگشایی دارای اهمیت‌اند. برای منظور فعلی خود، کافی است تنها بعضی از ویژگیهای اصلی مربوط به ترکیبهای مذکور را بررسی کنیم.

متنهایی از روزنامه که مجموعاً بیش از ۸۰۰۰۰ حرف داشته‌اند بررسی شده‌اند. از دوحرفیهای به‌کار رفته در این متنها ۳۰ ترکیب زیر بیش از دیگر ترکیبات به‌کار رفته‌اند (صورت کامل در جدول ضمیمهٔ الف آمده است):

TH	2161	ED	890	OF	731
HE	2053	TE	872	IT	704
IN	1550	TI	865	AL	681
ER	1436	OR	861	AS	648
RE	1280	ST	823	HA	646
ON	1232	AR	764	NG	630
AN	1216	ND	761	CO	606
EN	1029	TO	756	SE	595
AT	1019	NT	743	ME	573
ES	917	IS	741	DE	572

توجه داشته باشید که این ۳۰ ترکیب، که کل تعداد دفعاتی که به‌کار رفته‌اند بیش از ۲۸۰۰۰ است، حدود یک‌سوم تمام دوحرفیها را تشکیل می‌دهند. علاوه بر آن به ویژگیهای زیر از این دوحرفیها توجه کنید: بیست‌وپنج ترکیب از این ۳۰ ترکیب شامل یک حرف صدادار هستند. موردهایی از دوحرفیهای مقلوب مانند ER و RE، ES و SE، ED و DE در این ۲۵ ترکیب وجود دارند. از پنج ترکیب متشکل از دو حرف بی‌صدا، سه‌تای آنها شامل T و سه‌تای آنها شامل N هستند. در این مجموعهٔ دوحرفیهای با فراوانی زیاد، حتی یک مورد ترکیب دو حرف صدادار وجود ندارد.

به‌عنوان خلاصه‌ای از اطلاعات کلی به‌دست آمده از این فهرست می‌توان گفت:

۱. حرفهای صدادار بیشتر با حرفهای بی‌صدا ترکیب می‌شوند تا با یکدیگر.

۲. هر حرفی که در تعداد زیادی از انواع دوحرفیهای متفاوت بیاید، به‌احتمال زیاد حرفی صدادار است.

۳. حرفهای بی‌صدا ـ به‌استثنای T و N ـ غالباً با حرفهای صدادار ترکیب می‌شوند.

۴. اگر یک دوحرفی و مقلوب آن هر دو ظاهر شوند، محتملاً یک حرف آن، حرفی صدادار است.

در مورد سه‌حرفیها، نتایج زیر برای دوازده ترکیبی که بیش از ترکیبات سه‌حرفی دیگر به‌کار رفته‌اند، از همان نمونه به‌دست آمده است:

THE	**1717**	**TER**	**232**
AND	**483**	**RES**	**219**
TIO	**384**	**ERE**	**212**
ATI	**287**	**CON**	**206**
FOR	**284**	**TED**	**187**
THA	**255**	**COM**	**185**

در اینجا نیز حرفهای صدادار و بی‌صدا در هر ترکیبی دیده می‌شوند.

چگونه می‌توانیم از این نوع اطلاعات استفاده کنیم؟ ابتدا باید فراوانی دوحرفیها را در پیامی که می‌خواهیم بگشاییم بررسی کنیم. برای این منظور، به‌ازای هر بار ظاهر شدن یک حرف رمزی، حرفهای بلافاصله قبل و بعد از آن را زیر آن می‌نویسیم و به‌این ترتیب یک

توزیع فراوانی سه‌حرفی تهیه می‌کنیم. در چنین توزیعی دوحرفیها را با نگاه‌کردن به حرفهای اوّل و دوّم و نیز نگاه‌کردن به حرفهای دوم وسومِ هر سه‌حرفی می‌توان دید.

برای اینکه شیوهٔ تهیهٔ این توزیع روشن شود به جدول مربوط به پیام رمزی ابتدای این بخش که در صفحهٔ ۵۶ آمده است نگاه کنید. دنبالهٔ حروف الفبا را می‌نویسیم. سپس حروف پیام را از ابتدای پیام تک‌تک در نظر می‌گیریم و به‌ازای هریک، به‌جای نشانخط، خود حروف قبل و بعد آن را زیر آن حرف از دنبالهٔ الفبا می‌آوریم. چنانکه زیر حرف اوّل پیام، یعنی M، Y، ۰ را می‌آوریم تا نشان دهیم که حرفی قبل از آن نیامده و حرف بعد از آن Y است. همچنین در زیر Y دوحرفی MT را می‌آوریم تا نشان دهیم Mقبل از Y و T بعد از آن آمده است. همچنین در زیر T، دوحرفی YK را می‌آوریم و این کار را تا انتهای پیام ادامه می‌دهیم. توزیعی که به‌این ترتیب حاصل می‌شود، نشاندهندهٔ فراوانی هرحرف و نیز نشاندهندهٔ حروف ماقبل و مابعد آن حرف در پیام است. موضوع دیگری که حاوی اطلاعاتی برای ماست، تکرار بعضی سه‌حرفیهاست. این موضوع در توزیع فراوانی با رسم خطی در زیر آنها مشخص می‌شود. هنگام تشکیل این توزیع، سه‌حرفیهای تکراری را علامتگذاری می‌کنیم. همچنین باید آنها را در پیام رمزی یافته و علامتگذاری کنیم. ضمناً باید دقت کنیم که آیا بخشهای تکراری، علاوه بر سه‌حرف، شامل حرفهای دیگری نیز هستند یا خیر. ممکن است آشکار شود که آنها کلمات (یا عبارات) کاملی هستند که تکرار شده‌اند. این موضوع نیز می‌تواند در تلاش برای استخراج متن اصلی مفید واقع شود.

به‌عنوان قدم بعدی در گشایش متن رمزی، تلاش می‌کنیم که حرفهای صدادار را از بی‌صدا تشخیص دهیم. حرفهای رمزیِ با فراوانی زیاد، یعنی A، I، J، M، R، U، T و Y را در نظر می‌گیریم و دوحرفیهای تکراری شامل این حرفها را همراه با فراوانی هریک فهرست می‌کنیم:

A	I	J	M	R	T	U	Y
O:3 Z:4	J:3 J:4	I:4 I:3	Y:3 R:3	M:3 U:3	I:2 R:2	R:3 Y:3	U:3 M:3
L:2 C:2	G:2 U:2	R:2 A:2	0:2	T:2 J:2		I:2 A:3	
J:2 R:2	X:2 T:2	F:2		A:2			
U:3							

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
LZ		AU		HT	JA	YI	AM	KJ	II	TI	UA	.Y		ZA	RJ	RM	IU		YK	RL	AY		EA	MT	AO
OH		AH		MX	JT	AR	CE	JR	IA		AA	HI		MA	MY		TJ		ER	CY	YT		EO	UG	AU
JC				ZX	IM	TE	JA	MJ	II		EG	JR		XA	AA		MU		FM	IJ	LI		UI	UM	AE
JC				GL		LI		GI	UA		TV	YJ		MY			GM		RR	RY			MI	UM	AR
FG								IJ	RM			RR		IM			MP		IG	ZY				VM	
XL								JU	MF			TE					MQ		IJ	RA				OV	
LZ								RT	PF			YR					ZU		VL	JA				PU	
OZ								GJ	IH			QO					AT			YX					
OZ								JT	RI			YO					TI			IA					
UR								VF	TU			FP					AJ								
HR								XO				OX													
UV								XU																	
UP																									
P.																									

این جدول نشان می‌دهد که دوحرفی OA سه مرتبه ظاهر شده است، AZ چهار مرتبه، وقس علی‌هذا.

تعداد زیاد و تنوع دوحرفیهای تکراری شامل A_c نشاندهندهٔ آن است که A_c محتملاً صدادار است؛ دوحرفیهای مقلوب IJ و JI که به دفعات تکرار شده‌اند، به‌علاوهٔ ظاهرشدن دوحرفیهای مقلوب IR و RI نشان می‌دهد که I_c حرف صدادار است، که شاید همان E_p باشد. این موضوع که هیچ‌جا AI یا IA نیامده است، شاید دلیل دیگری باشد بر اینکه A_c و I_c هر دو حرفهایی صدادارند. علاوه بر این J_c غالباً با I_c و A_c ترکیب شده است. پس فرض می‌کنیم که A_c و I_c حرفهایی صدادار و J_c حرفی بی‌صدا باشد. از اینجا نتیجه می‌شود که U_c احتمالاً حرفی بی‌صداست زیرا غالباً همراه با A_c و I_c یک دوحرفی می‌سازد.

در بررسی حرفهای با فراوانی کم، که تقریباً مطمئنیم حروف بی‌صدا هستند، و مشاهدهٔ اینکه آنها به کرات با A_c و I_c ترکیب شده‌اند، نشانهٔ دیگری برای صدادار بودن حرفهای A_c و I_c دیده می‌شود. از آنجا که دوحرفی II دوبار ظاهر می‌شود، I_c احتمالاً نه A_p است و نه I_p پس یا باید E_p باشد یا O_p. اما وجود دوحرفیهای مقلوب IJ، JI و IR، RI دال بر این است که از دو معادل احتمالی فوق برای I_c، E_p معادل مناسبتری است. حال در مورد M_c، که رتبهٔ سوم را در حرفهای با فراوانی زیاد دارد، چه می‌توان گفت؟ این حرف که هیچ‌گاه با A_c ترکیب نشده و تنها یک‌بار با I_c ترکیب شده، ممکن است حرفی صدادار باشد، زیرا به‌ندرت با حرفهای رمزیی که به‌طور آزمایشی به‌عنوان حرفهای صدادار تعیین کرده‌ایم ترکیب شده است. M_c با حرفهایی با فراوانی کم مانند Q_c و P_c و H_c ترکیب شده است. همچنین M_c اغلب با R_c ترکیب شده که ظاهراً حرفی بی‌صداست، زیرا هم با A_c و هم با I_c ترکیب شده، و با I_c از دوطرف ترکیب شده است.

با خلاصه کردن تمام این احتمالات، خواهیم داشت:

M_c، A_c، I_c: احتمالاً حرفهای صدادارند؛

$I_c = E_p$ ؟

U_c، R_c، J_c: احتمالاً حرفهای بی‌صدا هستند؛

J_c احتمالاً N_p، R_p، یا S_p است (به‌علت دوحرفیهای مقلوبی که با I_c تشکیل داده است).

از آنجا که هر بخش یک کلمه باید دارای حداقل یک حرف صدادار باشد، بررسی مکان حرفهای صدادار در تمام طول پیام شیوه‌ای است برای آزمایش اینکه آیا هویت حرفهای صدادار را به‌درستی تعیین کرده‌ایم یا نه. حال پیام را مرور می‌کنیم و حرفهای صدادار را که به‌طور آزمایشی تعیین شده‌اند مشخص می‌کنیم:

```
MYTKI JIRUL AZOAH MIJAC UYGII JIUJA CHETR JMRUY MJFAG
 *   *  *    *  *  **  *     **  *  *        *    *  *

RMRPJ FTMEX ALAZU YMRQM OAZEX OAZRU ARTRI TGELG IJHAR
 *     *    *  *   *  *   *     *   *  *        *  *

JITJU AVYMO YVTLV IFMPY UXIOM XIUAP A
 *    *  *        *  *     *  *  *  *
```

فاصله‌ها مناسب به‌نظر می‌رسند. تنها دو مکان وجود دارند که در آنها حرفهای صدادار مجاورند و تنها چهار رشتهٔ متشکل از پنج حرف یا بیشتر وجود دارند که شامل هیچ حرف صدادار نیستند. غیرممکن نیست که به چنین تعدادی حروف بی‌صدای متوالی داشته باشیم ـ در واقع می‌توان در یک کلمهٔ تنها، پنج حرف بی‌صدای متوالی یافت (برای مثال، STRENGTHS، EIGHTHS). اما چندان محتمل نیست که هر چهار رشتهٔ

C H E T R J, R P J F T, T G E L G, O Y V T L V

بدون حرف صدادار باشند. از قرار معلوم از بین چهار حرف صدادار با فراوانی زیاد، یعنی A، E، I، O سه‌تا را قبلاً به‌دست آورده‌ایم. آیا در این رشته‌ها می‌توانیم حرفی رمزی را پیدا کنیم که بتواند چهارمین حرف صدادار باشد؟ به‌نظر معقول می‌آید که این حرف یکی از حروف E_c، T_c یا L_c باشد، و احتمال آنکه T_c باشد بیشتر است، به این دلیل که در هر چهار رشته آمده است. E_c با M_c که آن را حرفی صدادار دانسته‌ایم ترکیب شده، بنابراین صدادار بودن E_c بعید به‌نظر می‌رسد. L_c تنها چهارمرتبه ظاهر شده و از هر دوطرف با حرف صدادار احتمالی A_c ترکیب شده است. بنابراین احتمال اینکه T_c حرفی صدادار باشد بیشتر است.

تا اینجا اطلاعاتی دربارهٔ غالب حرفهای با فراوانی زیاد به‌دست آورده‌ایم. در مورد حرفهای U_c و R_c که معتقدیم حروف بی‌صدا هستند چه می‌توان گفت؟ اگر یکی از اینها T_p باشد، ممکن است آن حرف با جستجوی دوحرفیِ با فراوانی زیادی که یکی از حرفهایش T_p باشد، به‌خصوص با جستجوی TH، که رایجترین دوحرفی در زبان صریح

است قابل‌تشخیص باشد. R_c سه‌بار قبل از U_c آمده، اما U_c بیشتر از آن ظاهر شده که بتوان احتمال داد H_p باشد. U_c سه‌بار قبل از Y_c آمده که احتمالاً ممکن است H_p باشد، و سه‌بار هم پس از R_c می‌آید که در نتیجه R_c می‌تواند N_p یا S_p باشد.

اکنون برای اینکه ببینیم آیا می‌توان از طریق یک حدس مفید در پیام رمزی رخنه کرد، باید بخشهایی از متن را بیابیم که شامل الگوهایی باشند که بتوان کلمه‌هایی را بر آنها منطبق کرد. البته اگر بتوان بخشهایی را یافت که شامل حرفهای زیادی باشند که بر پایهٔ اطلاعات فوق قابل‌تشخیص‌اند، بهتر است.

الگوهای جالبی را می‌توان یافت، به‌عنوان مثال:

O A Z E X O A Z
V Y M O Y V
U X I O M X I U
U Y G I I J I U J

در تلاش برای حدس کلمه‌هایی که با یکی از این الگوها تطبیق کند، باید نخست حدس بزنیم ابتدا و انتهای کلمه‌ها کجاست.

آخرین الگو از الگوهای فوق تنها شامل حرفهای با فراوانی زیاد است، که برخی از آنها را به‌طور آزمایشی معین کرده‌ایم. اگر معادلهایی را که داریم جایگذاری کنیم، متن به‌صورت زیر درمی‌آید:

. . . U Y G I I J I U J A C H . . .

. . . t.h . e e{n r s} t{n r s} . . . . . .

به‌نظر می‌رسد که G_c ممکن است R_p باشد تا با کلمهٔ THREE جور باشد، در این‌صورت J_c باید N_p یا S_p باشد.

. . . U Y G I I J I U J A C H . . .

. . . t h r e e{n s} t{r. s} . . . . . .

از این دو، S_p بهتر به‌نظر می‌رسد، زیرا با کلمه‌های THREE SETS جور می‌آید. مثل اینکه راه دستیابی به قسمتی از متن را یافته‌ایم. راه خود را دنبال می‌کنیم و هرجا که حرفهای U، Y، G، I و J در متن رمزی آمده‌اند به‌جای آنها به‌ترتیب T، H، R، E و S را قرار می‌دهیم:

```
MYTKI JIRUL AZOAH MIJAC UYGII JIUJA CHETR JMRUY MJFAG
 h  e se t       es   three sets      s  th  s  r

RMRPJ FTMEX ALAZU YMRQM OAZEX OAZRU ARTRI TGELG IJHAR
   s         t h              t    e  r  r es

JITJU AVYMO YVTLV IFMPY UXIOM XIUAP A
se st   h   h    e   h t e   et
```

ترکیبهایی ظاهر می‌شوند که بسیار مناسب به‌نظر می‌رسند ـ هیچ چیز غیرقابل‌قبولی در مورد آنها مشاهده نمی‌شود. اگر این معادلها درست باشند، آنگاه می‌توانیم برای تشخیص حروف صدادار M_c، A_c، T_c، که هر یک از آنها باید با یکی از حروف A_p، I_p، O_p معادل باشد، تلاش کنیم. همچنین می‌دانیم که R_c که فراوانی زیادی دارد حرفی بی‌صداست. از آنجا که قبلاً حروف صریح T، R، S را شناسایی کرده‌ایم، R_c احتمالاً N_p است ـ قبلاً هنگام تلاش برای تعیین T_p، احتمال داده بودیم که R_c معادل N_p یا S_p باشد ـ با جایگذاری این معادلها در بخشی از متن که شامل هشتمین، نهمین و دهمین دسته از حرفهای رمزی است، به‌دست خواهیم آورد:

J M R U Y M J F A G R M R P J

s{a,i,o}n t h {a,i,o}s . . r n{a,i,o}n . s

که اگر $M_c = I_p$، خواهیم داشت:

sinthis.{o,a}rnin.s,

که عبارت زیر از آن به‌دست می‌آید:

in this mornings

حال باقی متن را به‌سرعت می‌توان معلوم کرد. حاصل عبارت است از:

I HAVE SENT YOU COPIES OF THREE SETS OF PLANS IN THIS MORNINGS MAIL DO YOU THINK I COULD COUNT ON AN EARLY RESPONSE AS TO WHICH WAY WE MIGHT DECIDE TO GO

[نسخه‌هایی از سه مجموعه نقشه را با پست صبح امروز برای شما ارسال داشته‌ام. آیا برایتان امکان دارد که پاسخ این سؤال را که ازکدام راه باید برویم، سریعاً ارسال کنید؟]

به‌عنوان تمرین پیشنهاد می‌کنیم خواننده الفبای جایگذاری و کلمهٔ کلیدی تولیدکنندهٔ آن را تعیین کند. (توجه: برای یافتن کلمهٔ کلیدی، از الفبای به رمزدرآوری استفاده کند. الفبای از رمزدرآوری اطلاعات مطلوب را به‌دست نخواهد داد [انتهای بخش ۱.۲ را ببینید].)

فرایندی که هم‌اکنون شرح داده شد نشان می‌دهد که گشایش پیام رمزی تک‌الفبایی را اغلب می‌توان چنین انجام داد: استفاده از توزیع فراوانی تک‌حرفی و دوحرفی برای تشخیص حرفهای صدادار و بی‌صدا در بین حرفهای با فراوانی زیاد، و سپس استفاده از این اطلاعات برای تشخیص قسمتی از متن اصلی بر پایهٔ الگوهای تکرار. هرگاه با چنین فرایندی مدخلی برای گشودن پیام یافت شود، آنگاه بقیهٔ پیام، معمولاً بدون مشکل، گشوده خواهد شد.

تمرین

رمزهای زیر را بگشایید:

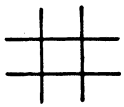
۳۱. **GJGNX BBWBJ LMGTX BGQCB ODBTL BXOGD VJGJB MWSUS LGXDO XGRLA SUUMC SQCXY UBTVY LRVXL CBIXB TBJLG JDUVL LBXDU SFBXG JOVWT BUBQL SVJTD TLBWL VOBLB XWSJB LCBVX OBXVR SJOYQ LSVJ**

۳۲. **ETYOQ PYRFZ DIROD RSRRD LRHYP MYOFY TPSMF ISFRY BDFQS FDTOU DTFIY LRQFY POFSF YOSRP ESRSJ SISVY SBTYY PDRRY WFTYS FQYOB DVYTR QRBFI YHDRF TDCPY UYROY SRPRY LFTSC QFMDU FIYES RSJSH SRSC**

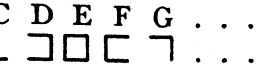
۴.۲ رمزهای تک‌الفبایی با معادلهای رمزی نمادین

اکنون هنگام آن است که به رمزهایی اشاره کنیم که متشکل از نمادهایی غیر از حروف الفبا هستند. در این مورد در داستان حشرهٔ طلایی اثر ادگار آلن‌پو مثالی جالب دیده می‌شود که یکی از اولین نمونه‌های رمزنگاری در ادبیات است. شیوهٔ رایجی از این نوع رمزنگاری

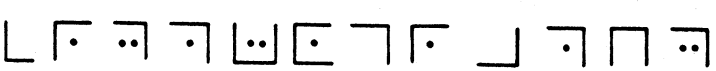
به‌صورت زیر است: حرفهای از A تا I را به‌ترتیب از چپ به راست با نه خانهٔ یک نمودارِ دوزبازی نشان می‌دهند:



صریح : A B C D E F G . . .

رمزی : 

حرفهای از J تا R را با همین خانه‌ها به‌اضافهٔ یک نقطه نشان می‌دهند و حرفهای از S تا Z را با همین خانه‌ها به‌اضافهٔ دو نقطه. با این شیوه، کلمهٔ CRYPTOGRAPHY به‌صورت زیر به رمز درمی‌آید:

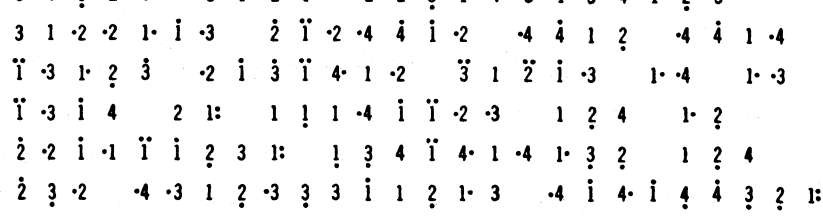


اگر رمزهای مبتنی بر نمادها تک‌الفبایی باشند (که بیشتر اوقات نیز چنین‌اند)، روشهای گشایش آنها به همان طرقی است که قبلاً شرح داده شد. در واقع اگر در چنین رمزی، یک جایگذاری دلخواه از حرفها به‌جای نمادهای به‌کار رفته انجام بگیرد، پیام رمزی دقیقاً شبیه همان نوعی خواهد شد که قبلاً دربارهٔ آن بحث کرده‌ایم. البته کار با حروف آشنای الفبا آسانتر است. اما رمزگشا باید به این نکته توجه کند که ممکن است نمادهای به‌کار رفته مبتنی بر سیستمی باشند ـ سیستمی برای نسبت‌دادن معادلهای صریح به نمادها ـ که اگر به‌جای آنها به‌طور دلخواه حرفهای الفبا را قرار دهد، شاید تشخیص آن سیستم دیگر کار آسانی نباشد.

تمرین

رمزهای زیر را بگشایید:

۳۳.



۳۴.

```
15  "&&  *(@  .*"/.  *(@  ._%  ;.  %@"/@.*  *!  *(@
@"/*(  "%'  ;*  ;.  *(@  2@%*@/  15  *(@  .!&"/  .$.*@3
"&&  *(@  ,&"%@*.  31:@  "/!_%'  ;*
```

۳۵.

متنهای رمزی زیر را بگشایید:

۳۶.

```
JTLR RQ VJQFIJU FCTJ RQ KTIYT HJ QWWQERXJIRS RCT DQKR
IDWQERHJR RCIJU IJ MIZT IK RQ VJQF FCTJ RQ ZQETUQ HJ
HONHJRHUT
```

۳۷.

```
MOOGA NBOIF HBIPN FIHFM OOIAL CKNRY NTVYN YQIVZ IFBRV
PNTCA NTVVZ IFVNR PZMVZ LHVOI VLFLY OKMTY LVGAL PSHKN
RQAMH GLVBN OYOKM TYLVH HGLTI HPARF BOI
```

۳۸.

```
KDBEW IKUET WXKPG KKBQD GUQPV HBCBV WTEBG KLDUQ DDPIP
IIUIK BHUGK DBAUX KDWRQ WEEYG UQPKU WGKDB WXSUI KDPKW
RKBVB OXPTD S
```

۳۹.

```
RFDIM ERDLM BREOM KKDYI QERGY OIMYE JROLB GQDHD YRDLB
KOVED RQDKO JIREO MYOML DTMEM UEKQB DJBML YBJJE MUZOQ
BPIJJ ABYSO ZEKQB DJERQ OOPKZ QOTBQ BARDQ QEROQ G
```

۴۰.

```
NXRPC GACPU RFCAW UVFSW QWRXU OBXVW AQXVF KRFWP KRTCK
XWARF SVFKD CFCLO VXEGK VPECZ PDWFS COCGK CXAWO BYKUV
GGCGL CXCIV ACGKR FIVGK PWGCG BXVEC XGGWR AUWPE VQRFP
CFKRT CGWPP VYFKC AQVXK DCXWK DCXUW PEUYG KCXKX CFAVQ
KDCUR GK
```

۳

جایگذاری چندالفبایی

۱.۳ رمزهای چندالفبایی

در فصل قبل معلوم شد که چگونه می‌توان یک رمز تک‌الفبایی راگشود. حتی اگر طول اصلی کلمات مشخص نباشد و الفبای جایگذاری تصادفی باشد، با استفاده از فراوانی حرفها، الگوهای تکرار و اطلاعات مربوط به نحوهٔ ترکیب حرفها با یکدیگر، می‌توان رمز راگشود. آنچه گشودن رمز را ممکن می‌سازد، این واقعیت است که هر حرف صریح مفروض همواره با یک حرف ثابت رمزی نمایش داده می‌شود. در نتیجه، همهٔ ویژگیهای زبان صریح مانند فراوانیها و ترکیبها به متن رمزی انتقال می‌یابند و می‌توان از آنها برای گشودن رمز استفاده کرد. در واقع می‌توانیم بگوییم که چنین ویژگیهایی همگی بدون تغییر می‌مانند و فقط نام حرفها تغییر می‌کند.

از این رو به نظر می‌رسد که برای به دست آوردن ایمنی بیشتر در به رمز در آوردن یک پیام، یک راه آن است که از بیش از یک الفبا استفاده شود. سیستم کلی می‌تواند سیستمی باشد که در آن از چندین الفبای متفاوت برای به رمز درآوردن استفاده شود، به شرط آنکه دو طرف مکاتبه با یکدیگر قرار گذارند که الفباهای متفاوت را به چه ترتیب به کار برند.

من باب مثال روشی کلاسیک را شرح می‌دهیم که ویژنر، رمزنگار فرانسوی، آن را ابداع کرده است. در این روش از مربعی استفاده می‌شود که به نام او ـ مربع ویژنر ـ معروف است و ما آن را در فصل ۱ شرح دادیم (صفحات ۱۳ و ۱۴). این مربع را که سطرهای متوالی آن شامل همان حرفهای الفبای معمولی است که به‌اندازهٔ ۱ مکان، ۲ مکان، و غیره انتقال

داده شده‌اند، هرگاه که مورد نیاز باشد به راحتی می‌توان ساخت. به علاوه، دو طرف مکاتبه قرار می‌گذارند که از کلمه‌ای کلیدی استفاده کنند، و این کلمه تنها چیزی است که لازم است به خاطر بسپرند. سیستم کلی عبارت از این است که برای به رمز درآوردن حرفهای متوالی متن صریح از الفباهایی که براساس کلمهٔ کلیدی مشخص می‌شوند متوالیاً استفاده کنیم.

برای مثال، فرض کنید کلمهٔ کلیدی SYMBOL باشد و پیامی که باید به رمز درآید چنین باشد:

THE ATOMIC ENERGY COMMISSION SAID YESTERDAY THAT RADIATION FROM AN UNDERGROUND NUCLEAR BLAST LEAKED INTO THE ATMOSPHERE TWO OR THREE HOURS AFTER A LOW YIELD NUCLEAR BOMB WAS TRIGGERED IN THE YUCCA BASIN

[کمیسیون انرژی اتمی دیروز اعلام کرد که دو یا سه ساعت پس از انفجار زیرزمینی یک بمب هسته‌ای کم قدرت در حوضهٔ یوکا، تشعشع حاصل از آن در جو زمین رخنه کرده است.]

فرایند به رمز درآوردن پیام به طریق زیر انجام می‌شود: اولین حرف از پیام، یعنی T_p، با استفاده از الفبای S (اولین حرف از کلمهٔ کلیدی SYMBOL)، به رمز در می‌آید. دنبالهٔ رمزی این الفبای جایگذاری سطری از مربع ویژنر است که با حرف S آغاز شده است. معادل رمزی T_p، حرفی است که در محل تقاطع ستون T و سطر S از این مربع یافت می‌شود. این حرف L_c است. دومین حرف از پیام، یعنی H_p، با استفاده از الفبای Y به رمز در می‌آید. رمز حاصل F_c است که در محل تقاطع ستون H و سطر Y واقع است. در این فرایند حرفهای کلمهٔ کلیدی متوالیاً معلوم می‌کنند که برای به رمز درآوردن حرفهای پیام، از کدام الفبا باید استفاده شود. این فرایند ادامه پیدا می‌کند تا زمانی که همهٔ حرفهای کلمهٔ کلیدی به کار روند، که در مثال ما زمانی است که ششمین حرف پیام به رمز در آید.

حرف کلیدی	**S Y M B O L**
صریح	**t h e a t o**
رمزی	**L F Q B H Z**

پس از این، وقتی با هفتمین حرف شروع می‌کنیم، همان مجموعه از الفباها باز به ترتیب برای به رمز درآوردن شش حرف بعدی به کار می‌رود، سپس شش تای بعدی، و پس از آن شش تای بعدی، تا اینکه تمام پیام به رمز در آید.

به رمز درآورنده (یا از رمز درآورنده) برای انجام دادن عملیاتِ لازم نیازی به تشکیل تمام مربع ندارد. تنها کافی است که سطرهایی از مربع را تشکیل دهد که با حرفهای کلمهٔ کلیدی متناظرند:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K

توجه داشته باشید که فرایند به رمز درآوردن را می‌توان با نوشتن تمام پیام در شش ستون [شش حرف به شش حرف در زیر هم] ساده‌تر کرد. در این صورت، تمام حرفهای واقع در یک ستون همه با یک الفبا به رمز در خواهند آمد. چنانکه با انتخاب الفبای S، به رمز درآورنده می‌تواند آن را برای تمام ستون ۱ به کار ببرد.

S	Y	M	B	O	L
t	h	e	a	t	o
L					
m	i	c	e	n	e
E					
r	g	y	c	o	m
J					
m	i	s	s	i	o
E					
.	.	.	.	.	.
.	.	.	.	.	.

با الفبای Y می‌تواند تمام حرفهای ستون ۲ را به رمز درآورد و به همین گونه تا به آخر. با این کار دیگر نیازی نخواهد بود که برای به رمز درآوردن حرف به حرف پیام مرتباً از یک الفبا به الفبای دیگر برود.

به زبان حساب همنهشتی، هر حرف که شمارهٔ ترتیب آن در پیام اصلی همنهشت با عدد a به پیمانهٔ ۶ باشد، با الفبایی به رمز در خواهد آمد که با a امین حرف از کلمهٔ کلیدی

مشخص می‌شود. این نوع سیستم کلی که در آن از الفباهای یک مجموعه الفبا مکرراً به ترتیب ثابتی استفاده می‌شود سیستم رمز چند الفبایی خوانده می‌شود.

اگر فرایند به رمز درآوردن پیام مورد مثال را با کلمهٔ کلیدی SYMBOL تا به انتها انجام دهیم، نتیجه عبارت خواهد شد از:

کلید	SYMBOL	SYMBOL	SYMBOL	SYMBOL	SYMBOL	
صریح	theato	micene	rgycom	missio	nsaidy	
رمزی	LFQBHZ	EGOFBP	JEKDCX	EGETWZ	FQMJRJ	
صریح	pstord	aythat	radiat	ionfro	manund	
رمزی	WQFFFO	SWFIOE	JYPJOE	AMZGFZ	EYZVBO	
صریح	ergrou	ndnucl	earbla	stleak	edinto	
رمزی	WPSSCF	FBZVQW	WYDCZL	KRXFOV	WBUOHZ	
صریح	theatm	ospher	etwoor	threeh	oursaf	
رمزی	LFQBHX	GQBISC	WRIPCC	LFDFSS	GSDTOQ	
صریح	teralo	wyield	nuclea	rbombw	astrig	
رمزی	LCDBZZ	OWUFZO	FSOMSL	JZANPH	SQFSWR	
صریح	geredi	ntheyu	ccabas	in		
رمزی	YCDFRT	FRTFMF	UAMCOD	AL		

سپس این پیام رمزی در دسته‌های پنج‌حرفی نوشته می‌شود و پس از آن ارسال می‌شود.

در این پیام رمزی، هر حرف رمزی خاص ممکن است به جای چند حرف صریح (حداکثر ۶ حرف) به کار رفته باشد، و بسته به محل خود در پیام، معرف یکی از آن شش حرف باشد. برای مثال، توجه کنید که کلمهٔ nuclear که دوبار در پیام اصلی آمده است، بار اول با حرفهای ZVQWWYD و بار دوّم با حرفهای FSOMSLJ به رمز درآمده است. هیچ ارتباطی بین این دو کلمهٔ رمزی وجود ندارد. حتی ملاحظه می‌کنیم که هرکدام از اینها شامل یک حرف تکراری است، در حالی که در کلمهٔ اصلی هیچ حرفی تکرار نمی‌شود. لذا ممکن نیست که فراوانی هر حرف از رمز را به فراوانی حرفی بخصوص از متن اصلی نسبت دهیم. ممکن است که به جای حرفهای تکراری متن اصلی حرفهای رمزی متفاوتی گذاشته شده باشد، و ممکن است حرفهای رمزی تکراری نشاندهندهٔ حرفهای متفاوتی از متن اصلی باشند.

اگر بین دو طرف مکاتبه مرتباً پیامهایی مبادله شود، آنها می‌توانند برای ایمنی بیشتر پیامها قرار بگذارندکه گاه‌به‌گاه، یا حتی پیام به پیام، کلمهٔ کلیدی عوض شود.

تمرین

۴۱. پیام زیر را که با مربع ویژنر با کلمهٔ کلیدی HOUSE به رمز درآمده است از رمز درآورید:

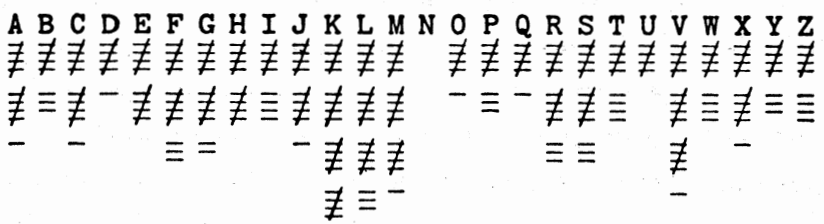
```
AVYUL HWLEE UCZLL LTYVI YOFJI ZSLNI ICUJH ZOCVC LGNWV
KOSLL HHULE EWHUV LOMWM ZBYWH LRHGA
```

۲.۳ تشخیص رمزهای چند الفبایی

روشهایی که در فصل ۲ برای گشودن رمزهای تک‌الفبایی به کار رفت، برای گشودن رمزهایی از نوع اخیر عملی نیست. پس رمزگشا، چگونه می‌تواند به گشودن چنین رمزهایی اقدام کند؟ شیوه‌های مورد استفاده را از راه به کار بردن آنها در یک مثال روشن می‌کنیم. فرض کنید پیام رمزیی که گشودن آن مورد نظر است چنین باشد:

```
APWVC DKPAK BCECY WXBBK CYVSE FVTLV MXGRG KKGFD LRLZK
TFVKH SAGUK YEXSR SIQTW JXVFL LALUI KYABZ XGRKL BAFSJ
CCMJT ZDGST AHBJM MLGEZ RPZIJ XPVGU OJXHL PUMVM CKYEX
SRSIQ KCWMC KFLQJ FWJRH SWLOX YPVKM HYCTA WEJVQ DPAVV
KFLKG FDLRL ZKIWT IBXSG RTPLL AMHFR OMEMV ZQZGK MSDFH
ATXSE ELVWK OCJFQ FLHRJ SMVMV IMBOZ HIKRO MUHIE RYG
```

توزیع تک حرفی این پیام به صورت زیر است:



این توزیع تغییرات زیادی را در فراوانی حرفهای متفاوت نشان می‌دهد. از K که ۲۰ بار ظاهر شده تا N که اصلاً ظاهر نشده است. با این‌حال به توزیع رمزهای تک‌الفبایی شباهتی ندارد، بلکه دارای نمایشی یکدست‌تر است. به ویژه توجه کنید که حروف با فراوانی کم تا چه اندازه کم هستند.

اگر به مثالی که پیش از این آوردیم توجه کنیم، می‌توانیم بفهمیم چرا باید انتظار توزیعی یکدست را داشته باشیم. از آنجا که در آن مثال کلمهٔ کلیدی شش حرفی SYMBOL را به کار برده‌ایم، هر حرف مفروض از رمز می‌تواند با شش حرف صریح متفاوت معادل باشد. بسته به مکان حرف رمزی مفروض در پیام، یکی از این شش حرف، معادل صحیح آن است. برای مثال، اگر A_c در ابتدا، یا در هفتمین محل، یا در سیزدهمین محل ـیعنی در اولین مکان (به پیمانهٔ ۶)ـ بیاید، حرف صریح معادل آن I_p، است زیرا برای به رمز درآوردن حرفهای این مکانها از الفبای S استفاده می‌شود، و در این الفبا A_c معادل I_p است:

رمزی :	S	T	U	V	W	X	Y	Z	A	B	.	.	.
صریح :	A	B	C	D	E	F	G	H	I	J	.	.	.

همچنین، اگر A_c در مکان دوّم (به پیمانهٔ ۶) بیاید، حرف صریح معادل آن C_p است زیرا برای به رمز درآوردن آن از الفبای Y استفاده می‌شود که معادل A_c در آن C_p است:

رمزی :	Y	Z	A	B	.	.	.
صریح :	A	B	C	D	.	.	.

اگر A_c در سوّمین، چهارمین، پنجمین و ششمین محل (به پیمانهٔ ۶) بیاید، به ترتیب با O_p، Z_p، M_p و P_p معادل می‌شود. اگر پیام رمزی رانیز در شش ستون بنویسیم، آنگاه j امین ستون نشاندهندهٔ حرفهای رمزی در مکانهای jاُم (به‌پیمانهٔ۶) از پیام خواهد بود، و هر ستون دارای الفبای از رمز درآوری متفاوتی است.

انتظار داریم که فراوانی یک حرف مفروض از متن صریح در ستونهای متفاوت، تفاوت نکند. به عبارت دیگر، انتظار می‌رود که فراوانی نسبی هر حرف مفروض از متن صریح، در هر ستون مساوی فراوانی نسبی آن درکل پیام باشد. در یک پیام طولانی، فراوانی نسبی هر حرف در یک ستون مفروض باید تقریباً برابر فراوانی مشخصهٔ آن حرف باشد. بنابراین تعداد دفعاتی که A_c در ستون ۱ می‌آید، با فراوانی مشخصهٔ I_p معین می‌شود. تعداد دفعاتی که A_c در ستون ۲ می‌آید، با فراوانی مشخصهٔ C_p معین می‌شود، و الی آخر. بنابراین فراوانی نسبی A_c در تمام پیام رمزی تقریباً برابر میانگین فراوانیهای مشخصهٔ مجموعهٔ حرفهای صریح P، M، Z، O، C، I است.

به همین نحو فراوانی نسبی هر حرف دیگر از رمز تقریباً برابر میانگین فراوانیهای مشخصهٔ مجموعه‌ای از شش حرف صریح است. در نتیجه فراوانیهای نسبی حروف رمزی

مقادیری متوسط دارند. بنابراین فراز و نشیب توزیع فراوانی پیام رمزی نسبت به فراز و نشیب توزیع متعارف زبان صریح کمتر است. البته، هر چه تعداد بیشتری از الفباهای متفاوت استفاده شود، توزیع رمز ظاهر یکدست‌تری خواهد داشت؛ و اگر تمام ۲۶ الفبا استفاده شوند، باید انتظار داشت که فراوانیهای نسبی تمام حرفهای رمزی تقریباً مساوی باشند.

بنابراین از روی توزیع فراوانی یک پیام رمزی چند الفبایی می‌توان تشخیص داد که این رمز با استفاده از یک الفبای تنها ساخته نشده است. اغلب تنها با بررسی توزیع فراوانی، این موضوع آشکار خواهد شد. اما اگر پیام کوتاه باشد، یا اگر تعداد کمی از الفباها به کار رفته باشند، ممکن است با نگاهی به توزیع فراوانی به نتیجهٔ قطعی نرسیم.

خصوصیتی که توزیع تک‌الفبایی را از توزیع چند الفبایی متمایز می‌کند آن است که در توزیع تک‌الفبایی، فراوانیهای حرفهای متمایز از تغییرات بیشتری برخوردارند.

منظور از میزان تغییرات یا «ناهمواری» یک توزیع، به بیان غیرکمّی، میزان تغییر فراوانی حرفهای متفاوت است. برای مثال، اگر همهٔ حرفها با یک فراوانی ظاهر شوند، توزیع شکل یکدست یا همواری خواهد داشت و تغییر فراوانی صفر خواهد بود. برای آنکه این مفهوم تغییر را همچون ابزاری درکار خود به کار ببریم، باید تعریف کمّی دقیقی از آن بدهیم که ما را قادر سازد تا این ویژگی توزیع را به دقّت اندازه‌گیری کنیم.

در نظریهٔ احتمال، فراوانی نسبی پیشامد x به صورت زیر تعریف می‌شود:

$$\frac{\text{تعداد کل دفعات وقوع پیشامد } x}{\text{تعداد کل آزمایشها}}$$

در اینجا، هر آزمایش عبارت است از بررسی یک حرف در یک متن، و ظاهر شدن یک حرف مشخّص، مثلاً B، می‌تواند پیشامد مورد نظر در این مسأله باشد. اگر B در یک متن ۱۰۰۰ حرفی، ۴۸ بار ظاهر شود، فراوانی نسبی B عبارت خواهد بود از

$$\frac{F_{\mathrm{B}}}{۱۰۰۰} = \frac{۴۸}{۱۰۰۰} = ۰٫۰۴۸,$$

که f_{B} نشان دهندهٔ تعداد دفعات ظاهر شدن B است.

واضح است که اگر فراوانیهای نسبی ۲۶ حرف الفبا را در متن نمونهٔ ۱۰۰۰ حرفی خود جمع بزنیم، خواهیم داشت:

$$\frac{f_{\mathrm{A}}}{۱۰۰۰} + \frac{f_{\mathrm{B}}}{۱۰۰۰} + \cdots + \frac{f_{\mathrm{Z}}}{۱۰۰۰} = \frac{۱۰۰۰}{۱۰۰۰} = ۱$$

احتمال وقوع پیشامد x برابر حد فراوانیهای نسبی x تعریف می‌شود وقتی که n، تعداد کل آزمایشها، افزایش یابد. به عنوان مثال p_B، احتمال ظاهرشدن B، عبارت است از:

$$p_{\mathrm{B}} = \lim_{n\to\infty} \frac{\text{تعداد دفعات ظاهر شدن B}}{n}$$

اگر همهٔ حرفهای الفبا با یک فراوانی ظاهر شوند، خواهیم داشت:

$$f_{\mathrm{A}} = f_{\mathrm{B}} = \cdots = f_{\mathrm{Z}}$$

و در آن صورت همهٔ فراوانیهای نسبی مساوی خواهند بود. از آنجا که

$$\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} \frac{f_i}{n} = ۱,$$

می‌توانیم نتیجه بگیریم که در چنین صورتی:

$$\frac{f_{\mathrm{A}}}{n} = \frac{f_{\mathrm{B}}}{n} = \cdots = \frac{f_{\mathrm{Z}}}{n} = \frac{۱}{۲۶},$$

و بنابراین همهٔ احتمالها برابر خواهند بود:

$$p_{\mathrm{A}} = p_{\mathrm{B}} = \cdots = p_{\mathrm{Z}} = \frac{۱}{۲۶}.$$

اما می‌دانیم که ۲۶ حرف الفبا با فراوانیهای برابر ظاهر نمی‌شوند و بنابراین احتمالهای آنها، یعنی p_{A}، p_{B}، ... همگی برابر نیستند. این احتمالها دارای مقادیر مثبت بین صفر و یک هستند و حاصلجمع آنها ۱ است:

$$\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} p_i = ۱.$$

مقدار اختلاف p_{A} با $\frac{۱}{۲۶}$، که انحراف آن از احتمال میانگین نامیده می‌شود، مساوی $p_{\mathrm{A}} - (\frac{۱}{۲۶})$ است. همچنین مقدار اختلاف احتمال ظاهر شدن B با میانگین عبارت است از $p_{\mathrm{B}} - (\frac{۱}{۲۶})$، و همین‌طور برای حرفهای دیگر. شاخص ناهمواری توزیع، تابعی از ۲۶ مقدار $p_i - (\frac{۱}{۲۶})$ است، که در آن متغیر i از A تا Z تغییر می‌کند.

این شاخص مطلوب نمی‌تواند صرفاً مجموع انحرافها باشد، زیرا بعضی از انحرافها مثبت و بعضی منفی‌اند، به طوری که مجموع آنها صفر است. زیرا،

$$\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} (p_i - \frac{۱}{۲۶}) = \sum_{i=\mathrm{A}}^{i=\mathrm{Z}} p_i - \sum_{i=\mathrm{A}}^{i=\mathrm{Z}} \frac{۱}{۲۶} = ۱ - ۲۶ \times \frac{۱}{۲۶} = ۰.$$

برای رهایی از این مشکل، می‌توانیم حاصلجمع قدر مطلق انحرافها را در نظر بگیریم:

$$\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} \left| p_i - \frac{۱}{۲۶} \right|.$$

اما این شاخص هم اشکالاتی دارد که تا حدی مربوط به مشکل کار با تابع قدرمطلق است.

راه دیگر برای مثبت کردن همهٔ جمله‌ها، مربع کردن مقدار هر انحراف است. حاصلجمع مربعهای انحرافها کمیتی است که معمولاً در کارهای آماری مورد استفاده قرار می‌گیرد. به این دلیل، کمیتی را که با رابطهٔ زیر تعریف می‌شود به منزلهٔ شاخص ناهمواری انتخاب می‌کنیم و آن را با M.R. نشان می‌دهیم:

$$\mathrm{M.R.} = (p_A - \frac{۱}{۲۶})^۲ + (p_B - \frac{۱}{۲۶})^۲ + \cdots + (p_Z - \frac{۱}{۲۶})^۲$$

یا به طور خلاصه

$$\mathrm{M.R.} = \sum_{i=\mathrm{A}}^{i=\mathrm{Z}} (p_i - \frac{۱}{۲۶})^۲.$$

این عبارت را می‌توان با روشهای جبری ساده‌تر کرد؛ اگر دوجمله‌ای $p_i - (\frac{۱}{۲۶})$ را مربع کنیم خواهیم داشت:

$$p_i^۲ - ۲p_i(\frac{۱}{۲۶}) + (\frac{۱}{۲۶})^۲$$

چون i از A تا Z تغییر کند، از جمع عبارتهای حاصل، به‌دست می‌آوریم:

$$\mathrm{M.R.} = \sum_{i=\mathrm{A}}^{i=\mathrm{Z}} p_i^۲ - \sum_{i=\mathrm{A}}^{i=\mathrm{Z}} ۲p_i(\frac{۱}{۲۶}) + \sum_{i=\mathrm{A}}^{i=\mathrm{Z}} (\frac{۱}{۲۶})^۲$$

از آنجا که $(\frac{۱}{۲۶})^۲$ به ازای هر مقدار i مقدار ثابتی است، جملهٔ آخر این عبارت برابر با $۲۶(\frac{۱}{۲۶})^۲$ یا $(\frac{۱}{۲۶})$ است. جملهٔ وسط مساوی است با

$$۲(\frac{۱}{۲۶}) \sum_{i=\mathrm{A}}^{i=\mathrm{Z}} p_i;$$

و چون $\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} p_i = ۱$، جملهٔ وسط برابر با $۲(\frac{۱}{۲۶})$ می‌شود. بنابراین

$$\text{M.R.} = \sum_{i=\text{A}}^{i=\text{Z}} p_i^{۲} - ۲(\frac{۱}{۲۶}) + \frac{۱}{۲۶} = \sum_{i=\text{A}}^{i=\text{Z}} p_i^{۲} - \frac{۱}{۲۶},$$

$$\text{M.R.} \approx \sum_{i=\text{A}}^{i=\text{Z}} p_i^{۲} - ۰\text{ر}۰۳۸.$$

اگر با توزیع مربوط به نمونه‌ای از زبان صریح سروکار داشته باشیم، .M.R را با جمع کردن مربعهای فراوانیهای مشخصه و تفریق ۰ر۰۳۸ از آن محاسبه می‌کنیم. فراوانیهای مشخصهٔ حرفهای نمونهٔ صریح را می‌دانیم (صفحهٔ ۱۸). اگر مربعهای آنها را جمع کنیم عدد ۰ر۰۶۶ را به‌دست خواهیم آورد. بنابراین .M.R برای متن صریح مساوی است با ۰ر۰۲۸ = ۰ر۰۳۸ − ۰ر۰۶۶. برای توزیعی که کاملاً هموار باشد، یعنی توزیعی که در آن همهٔ حرفها یک احتمال ظاهر شدن داشته باشند، به ازای همهٔ مقدارهای i داریم $p_i = \frac{۱}{۲۶}$ و در این حالت:

$$\text{M.R} = \frac{۱}{۲۶} - \frac{۱}{۲۶} = ۰ \quad \text{و} \quad \sum_{i=\text{A}}^{i=\text{Z}} p_i^{۲} = \sum_{i=\text{A}}^{i=\text{Z}} (\frac{۱}{۲۶})^{۲} = ۲۶(\frac{۱}{۲۶})^{۲} = \frac{۱}{۲۶}،$$

بنابراین اندازهٔ شاخص ناهمواری از ۰، که مربوط به توزیع کاملاً هموار است، تا مقدار ۰ر۰۲۸ که مربوط به توزیع تک‌الفبایی است تغییر می‌کند. این مقدار تغییر آن‌قدر هست که با استفاده از آن بتوانیم تک‌الفبابیها را از چندالفبابیها تشخیص دهیم، مشروط بر آنکه قادر به تعیین $\sum_{i=\text{A}}^{i=\text{Z}} p_i^{۲}$ باشیم.

اما اگر برای پیامی رمزی نظیر پیامی که می‌خواهیم بگشاییم، توزیعی داده شده باشد، هیچ اطلاعی از احتمالهای حروف صریح معادل نداریم. در مورد پیامی، نظیر مثال مورد بحث که در آن تمام الفباهای جایگذاری را می‌دانیم، و بنابراین تمام معادلهای صریحِ ممکن هر حرف رمزی را می‌دانیم، می‌توانیم این احتمالها را محاسبه کنیم. اما در وضعیتهای ناشناخته چنین اطّلاعاتی در دسترس نیست.

کاری که باید انجام دهیم یافتن روش دیگری برای تقریب زدن $\sum_{i=\text{A}}^{i=\text{Z}} p_i^{۲}$ است. یک جمله از این جمع، مثلاً $p_{\text{A}}^{۲}$ را در نظر بگیریم. آیا می‌توانیم مفهومی به این عدد نسبت دهیم؟ ابتدا ببینیم که p_{A} چه معنی دارد؟ احتمال اینکه یک حرف که به دلخواه از متن رمزی انتخاب شده حرف A باشد برابر p_{A} است. در این صورت $p_{\text{A}}^{۲}$ نشاندهندهٔ احتمال

آن است که دو حرف که به تصادف انتخاب شده‌اند، هر دو A باشند.* همچنین p_B^2 نشاندهندهٔ احتمال آن است که دو حرف که به تصادف انتخاب شده‌اند، هر دو B باشند، و به همین ترتیب برای حروف دیگر. احتمال آنکه دو حرف که به تصادف انتخاب شده‌اند، صرف نظر از هویتشان یکی باشند، عبارت است از:

$$p_A^2 + p_B^2 + \cdots + p_Z^2 = \sum_{i=A}^{i=Z} p_i^2.^{**}$$

به این ترتیب راهی برای تقریب $\sum_A^Z p_i^2$*** ، بدون اطلاع از کمیّتهای p_i، در اختیار داریم. این راه، محاسبهٔ احتمال انتخاب تصادفی دو حرف یکسان است. کاری که باید انجام دهیم آن است که حساب کنیم چند زوج از حروف یکسان در پیام رمزی وجود دارد و این تعداد را بر تعداد کل زوجهای ممکن تقسیم کنیم.

برای انجام‌دادن این کار باید به این سؤال پاسخ دهیم: از حروف مجموعه‌ای مفروض چند زوج می‌توان تشکیل داد؟ فرض کنیم در مجموعه، x حرف داشته باشیم. در این صورت تعداد زوجهایی که می‌توانیم به دست آوریم به طریق زیر تعیین می‌شود. در اوّلین انتخاب، هر یک از حروف را می‌توانیم انتخاب کنیم. یعنی x امکان در اختیار داریم. آنگاه $x-1$ حرف برای انتخاب دوّم باقی می‌مانند، به این ترتیب $x(x-1)$ امکان برای ساختن زوجها در اختیار داریم. امّا، در این محاسبه، هر زوج دوبار به حساب آمده است؛ زیرا هر زوج به دو ترتیب متفاوت به‌دست می‌آید. بنابراین، تعداد زوجهای حروف که می‌توانند از یک مجموعهٔ x حرفی انتخاب شوند عبارت است از $\frac{1}{2}x(x-1)$.

اگر تعداد Aها را در پیام رمزی بشماریم و حاصل، یعنی فراوانی A را با f_A نشان دهیم، آنگاه تعداد زوجهایی که از این f_A حرفِ A می‌توان تشکیل داد مساوی $\frac{1}{2}f_A(f_A-1)$ است. به همین ترتیب تعداد زوجهای Bها مساوی $\frac{1}{2}f_B(f_B-1)$ است. بنابراین تعداد کل زوجهایی که هر دو حرف آنها یکی است صرف نظر از هویت این حرف حاصلجمع زیر است:

---

* برای مثال به صفحهٔ ۲۹ از کتاب زیر نگاه کنید:

J. P. Hoyt, *Probability Theory*, International Textbook Co, Scranton, Penna., 1967.

** ایضاء صفحهٔ ۲۷.

*** نماد $\sum_A^Z$ خلاصهٔ شدهٔ $\sum_{i=A}^{i=Z}$ است.

$$\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} \frac{f_i(f_i-۱)}{۲}.$$

اگر تعداد کل حروف N باشد، تعداد کل زوجهای ممکن حروف $\frac{۱}{۲}N(N-۱)$ خواهد بود. از آنجا که احتمال اینکه دو حرف مشابه باشند برابر حاصل تقسیم تعداد زوجهای متشکل از حروف یکسان بر تعداد کلّ زوجهاست، به دست می‌آوریم:

$$\frac{\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} f_i(f_i-۱)}{N(N-۱)}$$

این عدد تخمین خوبی برای $\sum_{i=\mathrm{A}}^{i=\mathrm{Z}} p_i^۲$ است. از آنجا که این عدد نشاندهندهٔ احتمال آن است که دو حرف انتخابی از یک پیام مشابه باشند، آن را شاخص انطباق می‌نامند و با I.C. نمایش می‌دهند.

در رمزگشایی کارکردن با I.C. معمولتر از M.R. است. دیدیم که M.R. $= \sum_{\mathrm{A}}^{\mathrm{Z}} p_i^۲ -$ ۰٫۰۳۸ و نیز دیدیم که اندازهٔ M.R. از ۰ تا ۰٫۰۲۸ تغییرمی‌کند. بنابراین M.R. $+$ ۰٫۰۳۸ $= \sum_{\mathrm{A}}^{\mathrm{Z}} p_i^۲$ از ۰٫۰۳۸ تا ۰٫۰۶۶ تغییرمی‌کند. از آنجا که I.C.، $\sum_{\mathrm{A}}^{\mathrm{Z}} p_i^۲$ را تقریب می‌زند، دارای همان محدودهٔ تغییرات است، یعنی از ۰٫۰۳۸ تا ۰٫۰۶۶. حد پایین متناظر با توزیع کاملاً هموار است، و حد بالا متناظر با توزیع تک الفبایی.

شاخصی از چگونگی وابستگی این تغییر مقادیر به تعداد الفباها و در نتیجه به هموارِی توزیع را می‌توان با روشهای آماری که فراتر از محدودهٔ این متن است به دست آورد. اگر یک پیام N حرفی با m الفبا به رمز درآید، با فرض اینکه تعداد حروفی که با هر یک از این m الفبا به رمز در می‌آیند یکسان باشند، می‌توان نشان داد که مقداری که انتظار می‌رود برای I.C. به دست آید، عبارت است از:

$$\mathrm{I.C.} = \frac{۱}{m}\frac{\mathrm{N}-m}{N-۱}(۰٫۰۶۶) + \frac{m-۱}{m}\frac{N}{N-۱}(۰٫۰۳۸).$$

اگر N عددی نسبتاً بزرگ باشد، I.C. را برای مقادیر مشخص m (تعداد الفباها) می‌توان به سهولت به وسیلهٔ این عبارت تقریب زد؛ تعداد کمی از این مقادیر در زیر آورده شده‌اند:

m	I.C.
1	.066
2	.052
5	.044
10	.041
بزرگ	.038

باید تأکید کرد که این نتایج مربوط به شاخص انطباق ماهیتی آماری دارند. این نتایج در مواردی به کار می‌روند که N عدد بزرگی باشد، یعنی در مورد پیامهای بسیار طولانی. برای پیامهای کوتاه مقادیری که برای I.C. به دست می‌آید ممکن است تا حد زیادی با این مقادیر مورد انتظار تفاوت داشته باشند. بنابراین نباید دربارهٔ تعداد الفباهایی که در به رمز درآوردن یک پیام کوتاه به کار رفته‌اند، صرفاً برپایهٔ I.C.ی پیام نتیجه‌گیری قطعی کرد. برای روشن شدن مطلب، اگر I.C. را برای مثال آغاز فصل محاسبه کنیم، مقدار ۰٫۰۴۹ به دست می‌آید که تقریباً مقداری است که انتظار داریم رمزهای سه الفبایی داشته باشند، اما می‌دانیم که این رمز با استفاده از شش الفبا تهیه شده است.

نکتهٔ دیگری که باید به خاطر سپرد آن است که مقدار مورد انتظار I.C. مبتنی بر این فرض بود که هر الفبا برای تعداد یکسانی از حروف به کار رفته باشد. اگر در کلمهٔ کلیدی یک پیام چند الفبایی حروف تکراری وجود داشته باشد، این موضوع درست نخواهد بود. بنابراین، به نتیجه‌ای که از I.C. دربارهٔ تعداد الفباها در یک پیام رمزی به دست می‌آید، باید به دیدهٔ نتیجه‌ای تقریبی نگریست.

با این حال I.C. محققاً وسیلهٔ خوبی است برای دانستن اینکه آیا پیام تک‌الفبایی است یا نه. اگر I.C. را برای پیام ناشناختهٔ خود در صفحهٔ ۶۸ محاسبه کنیم، ۰٫۰۴۱ به دست می‌آید. دیده‌ایم که از لحاظ نظری باید انتظار داشت که این عدد مربوط به رمزی ده الفبایی باشد، بنابراین می‌توانیم تقریباً مطمئن باشیم که پیام ناشناختهٔ ما تک الفبایی نیست. در نتیجه تلاشی برای گشودن آن به وسیلهٔ شیوه‌های فصل ۲ نخواهیم کرد.

تمرین

۴۲. آزمون I.C. را برای توزیعهای تک حرفی (الف) صفحهٔ ۳۱ و (ب) صفحهٔ ۳۷ به کار برده و نشان دهید که نتایج حاصله حاکی از آن است که پیامها تک‌الفبایی‌اند.

۴۳. توزیعهای تک حرفی پنج پیام رمزی داده شده‌اند، I.C.ها را محاسبه کنید و تعیین کنید که کدامیک از این پیامها تک‌الفبایی‌اند. سپس بقیه را به ترتیبی که احتمال می‌رود تعداد الفباهای به کار رفته در آنها صعودی باشد مرتب کنید:

1.	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	7	6	9	3	5	6	8	3	4	7	13	10	7	0	1	5	3	6	8	5	4	8	4	8	5	5
2.	A	B		C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q		R	S	T	U	V	W	X	Y	Z
	5	3	10	0	1	4	9	0	0	9	3	10	5	2	0	6	5	10	4	2	0	0	1	0	8	0
3.	A	B	C	D		E	F	G	H	I	J	K	L	M	N	O	P	Q		R	S	T	U	V	W	X		Y	Z
	4	6	6	11	13	6	3	6	8	8	9	7	1	2	6	9	8	12	8	4	2	11	7	1	11	7

4. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
   3 0 3 6 17 1 0 1 5 1 8 6 2 7 0 4 1 5 0 1 4 1 13 1 0 9

5. A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
   3 7 4 2 8 5 6 4 10 5 8 6 8 3 7 9 5 6 4 9 5 7 3 7 6 3

۳.۳ تعیین تعداد الفباها

هنگامی که دانستیم در پیامی که برای گشودن آن کوشش می‌کنیم بیش از یک الفبا به کار رفته، مسألهٔ بعدی تعیین تعداد این الفباهاست و اینکه آیا آنها به یک شیوهٔ تکراری چند الفبایی* به کار رفته‌اند یا نه. اگر یک پیام چند الفبایی در ستونهایی که تعدادشان مساوی با تعداد حروف کلمهٔ کلیدی است نوشته شده باشد ، تمام حروف واقع در یک ستون با یک تک‌الفبا به رمز در می‌آیند. بنابراین اگر کلمه‌ای (یا دنباله‌ای از حروف) در متن صریح تکرار شود و اتفاقاً هر بار در ستونهای یکسان واقع شود، آن کلمه (یا دنباله) همواره به یک صورت به رمز در خواهد آمد. برای مثال، توجه کنید که چگونه در مثال صفحهٔ ۶۵ کلمهٔ آغازین *the* و دو حرف اول *atomic* در همان ستونهایی قرار دارند که کلمهٔ *the* و حروف *at* از *atmosphere*. در هر دو مورد، صورت رمزی *theat*، LFQBHاست. فاصلهٔ بین این صورتهای رمزی تکراری (یعنی تعداد حروف ما بین آنها) مساوی مضربی از «k»، یعنی مضربی از طول کلمهٔ کلیدی، است. برای مشاهدهٔ این مطلب، توجه کنید که هر دو حرف متناظر این صورتهای تکراری در مکانهایی قرار دارند که شمارهٔ آنها همنهشت با یک عدد به پیمانهٔ k است. بنابراین تفاضل شمارهٔ مکان آنها به پیمانهٔ k، همنهشت با صفر است.

البته ممکن است حروفی متفاوت واقع در ستونهای متفاوت از متن صریح با حروف یکسانی به رمز در آیند. همچنین ممکن است که دو حرفیها و سه حرفیهای متفاوتی از متن صریح به طور یکسان به رمز درآیند. برای مثال، در سطر آخر پیام صفحهٔ ۶۷ ، دنبالهٔ رمزی FRT، که دو بار پشت سرهم آمده، در مورد اول به جای حروف صریح *edi* و در مورد دیگر به جای *nth* آمده است. احتمال آنکه دو صورت رمزی تکراری، از این نوع «اتفاقی» باشند، با افزایش تعداد حروف آنها، کم و کمتر می‌شود. زیرا واضح است که هر چه صورت رمزی تکراری طولانیتر باشد، احتمال اینکه یک صورت تکراری در متن صریح سبب این وضعیت شده باشد بیشتر است.

بنابراین راهی برای تعیین اینکه پیام چند الفبایی است یا نه، آن است که تعیین شود چه

* تکنیک تشخیص رمزهای چند الفبایی را اولین بار افسر پروسی، فریدریش کازیسکی (Friedrich. W. Kasiski) در ۱۸۶۳ منتشر کرد.

صورتهای رمزی تکراری در آن وجود دارند و سپس تعیین شود که آیا فاصله‌های بین این تکرارها مقسوم علیه مشترکی دارند یا نه. چنین مقسوم علیه مشترکی را می‌توان تعداد محتمل حروف کلمهٔ کلیدی دانست. این طرز کار را با استفاده از پیام صفحهٔ ۶۸ شرح می‌دهیم.

برای یافتن صورتهای تکراری، به طریقی که در فصل ۲ تشریح شد، توزیع فراوانی سه حرفی پیام را تشکیل می‌دهیم. این توزیع در (شکل ۶) نشان داده شده است. رمزگشا با کمک آن از یافتن تمام صورتهای تکراری پیام رمزی اطمینان می‌یابد.

دو صورت تکراری بسیار طولانی می‌یابیم، و به مکان اولین حرف هرکدام از آنها در پیام توجّه می‌کنیم. فاصلهٔ بین این دو صورت تکراری مساوی است با تفاضل شمارهٔ مکان حروف متناظر آنها. (سه حرفیهای تکراری بسیاری نیز در پیام وجود دارند، امّا نیازی به در نظر گرفتن آنها نداریم، زیرا نتایجی که از صورتهای تکراری طولانی به دست می‌آید بسیار قابل توجّه‌تر است.)

دنبالهٔ تکراری	شمارهٔ مکانهای حرف اوّل	فاصله
KGFDLRLZK	۳۷،۱۸۴	۱۴۷
KYEXSRSIQ	۵۵،۱۳۲	۷۷

این صورتهای تکراری طولانیتر از آن هستند که اتفاقی باشند، و تنها مقسوم‌علیه مشترک دو فاصلهٔ مزبور عدد ۷ است. این نتایج دال بر آن است که پیام رمزی چند الفبایی و تعداد الفباهای آن هفت است. شاخص انطباقی که قبلاً محاسبه کرده بودیم (به صفحهٔ ۷۵ نگاه کنید) با این نتیجه سازگار است.

اگر این نتیجه‌گیری درست باشد، یعنی تعداد الفباها هفت باشد، آنگاه تمام حروف رمزی که شمارهٔ مکانهایشان به پیمانهٔ ۷ بایکدیگر همنهشت‌اند باید با یک الفبا به رمز درآمده باشند. برای بررسی صحت این موضوع، تمام پیام را در ۷ ستون می‌نویسیم.*

```
APWVCDK PAKBCEC YWXBBKC YVSEFVT LVMXGRG KKGFDLR LZKTFVK
HSAGUKY EXSRSIQ TWJXVFL LALUIKY ABZXGRK LBAFSJC CMJTZDG
STAHBJM MLGEZRP ZIJXPVG UOJXHLP UMVMCKY EXSRSIQ KCWMCKF
LQJFWJR HSWLOXY PVKMHYC TAWEJVQ DPAVVKF LKGFDLR LZKIWTI
BXSGRTP LLAMHFR OMEMVZQ ZGKMSDF HATXSEE LVWKOCJ FQFLHRJ
SMVMVIM BOZHIKR OMUHIER YG
```

* هرکدام از این هفت ستون آنقدر طولانی است که به دلیل محدودیتهای چاپی در اینجا آنها را هفت تا هفت تا دسته‌بندی کرده‌ایم، به این ترتیب با یک نظر معلوم می‌شود که کدام حرف در کدام ستون است.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
.P	KC	VD	CK	CC	EV	XR	KS	SQ	WX	DP	TV	VX		UJ	AW	IT	GG	VE	VL	GK	WC	PV	WB	CW	LK
PK	XB	BE	FL	SF	GD	RK	AB	UK	SC	AB	DR	CJ		LX	KA	IK	LL	HA	KF	LI	YS	YX	MG	CV	BX
SG	BK	EY	ZG	YX	TV	KF	XL	ZJ	MT	BC	RZ	JM		RM	RZ	LJ	SS	XR	QW	GO	FT	TJ	ES	KE	TD
LL	AZ	KY	QP	GZ	VL	AU	RS	SQ	BM	GK	FL	ML		KC	XV	VD	GK	RI	JZ	PM	LM	CM	JV	KA	ER
YB	LA	JC	FL	YX	AS	XR	MY	KW	IX	KG	LA	UV		BZ	LU	ZZ	ZP	FJ	SA	MH	FK	FJ	ZG	KE	PI
BF	HJ	CM	SF	WJ	KL	DS	MF	TB	OX	ZT	AU	VC		RM	YV	FF	SS	GT	CA		XF	SL	JP	XP	LK
TH	IX	MK		MM	JW	LE	FA	VM	QF	VH	KB	WC			DA		JH	XR	WI		PG	AW	JH	HC	VQ
TW	MO	KW		SE	KL	VU	LR	HK	WR	UY	MG	KH			TL		LL	RI	RP		MM	IT	ES	RG	QG
PV		MK		EL	GD	KF	ZI	HE	EV	IY	HP	AH					GT	HW	AX		PK	VK	OY		OH
LM		YT		IR	HR	SR	UI		CF	RL	FQ	OE					FO	XG			JQ		BS		
HT		OJ			DH	ZK			RS	CY	WO	EV					HJ	MD			AV		TS		
					JQ	Y.				QC	FK	KS					KO	XE			VK				
					QL					CF	DR	SV					EY	JM			MZ				
										VM	RZ	VV									LW				
										VF	PL	IB									MM				
										LG	LA	OU									MI				
										ZI	EV														
										GM	FH														
										WO															
										IR															

شکل۶

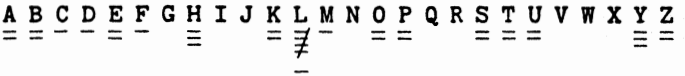
حال برای هر ستون یک توزیع تک حرفی تهیه می‌کنیم، که این توزیعها در زیر نشان داده شده‌اند.

این توزیعها شبیه توزیع تک‌الفبایی به نظر می‌آیند. اما نباید با ظواهر کلی قانع شویم. اکنون با استفاده از شاخصهای انطباق، می‌توانیم شاخصی عددی برای تک الفبایی بودن توزیع به‌دست آوریم. اگر .I.C‌ای این هفت توزیع را محاسبه کنیم، به‌دست می‌آوریم:

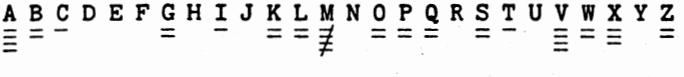
۱	۲	۳	۴	۵	۶	۷
۰٫۰۷۰	۰٫۰۵۰	۰٫۰۷۱	۰٫۰۷۲	۰٫۰۵۱	۰٫۰۷۱	۰٫۰۶۶

بجز نتایج مربوط به توزیعهای ۲و۵، سایر نتایج قویاً دلالت بر تک‌الفبایی بودن توزیعها دارند. حتی شاخصهای توزیعهای ۲ و ۵، بیشتر از شاخص کل پیام هستند که دیدیم .I.C‌ای آن مساوی ۰٫۰۴۱ است.

توزیع تک حرفی ستون۱

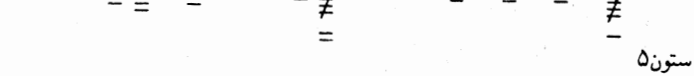


توزیع تک حرفی ستون۲



توزیع تک حرفی ستون۳

توزیع تک حرفی ستون۴



توزیع تک حرفی ستون۵

توزیع تک حرفی ستون۶

توزیع تک حرفی ستون۷

یک شاخص جامع برای این پیام را، بر اساس تقسیم آن به هفت الفبا، می‌توان با میانگین گرفتن از I.C. ها به دست آورد. حاصل این کار، ۰٫۰۶۴ خواهد بود که تقریباً مساوی I.C. زبان صریح است. حال قانع شده‌ایم که کارگشودن رمز را با فرض آنکه این رمز رمزی هفت‌الفبایی است، ادامه دهیم.

تمرین

تعداد الفباهای به کار رفته در به رمز درآوردن پیامهای زیر را تعیین کنید:

۴۴.
```
SBPRT LHMWW OAHHE SCNQO RWDPM UVZKG NDMAZ AGENB BBASH
YQEKU HWTBR XJOTI IAJHV PIWZK FOHCQ PNHFP QQBAK ZJXWH
RVCYG GOKES LNCEK VFPHW GKDMT OMAGT ZPNUN TLCMZ KBSWO
YDVGK YFLGX NXLCQ OPRUU SLIMA BAFZI URTLO YYBBL GFXPT
NZWBP RIAJE CCZIQ BSBNZ LUEHC ECMFK KBPZL RJLCC ZDRGD
GNDMA ZATTX ARIJS ENTBT YVTYL RTABE CMBIW OYYMR VK
```

۴۵.
```
CNPWV BAGYW OFGWC YYBQZ DELTY AABAD AAGHL DLPHD DNZYC
KFPPU UPPJC HUPFC FPBQX AACUF MPPNL OYPAL DNVAZ DDMWZ
JPMXF JYDKC YPVNF JLYKL TPLGY FDPAL FRIKK XUMYY JPMTB
CNPWV BAGYW OFGWC YIGNV MRDGD KFPKO ZARKK KAJGD DNBQF
QBVRL IQNQD MQGDF YPHHL DQGHQ MATGI JPMAT JEUKB UUDRK
KIVAC QACKN KIGIE FQKRK ZU
```

۴.۳ گشودن الفباهای پیام چند الفبایی، در صورتی که متعارف باشند

حال با موشکافی بیشتر به بررسی توزیعهای تک‌الفبایی می‌پردازیم. آیا امکان دارد آنها معرف الفباهای متعارف مستقیم باشند؟ اگر در سیستم به رمز درآوردن این پیام از مربع ویژنر استفاده شده باشد، همان‌گونه که در آغاز این فصل شرح داده شد، در آن صورت این الفباها معرف الفباهای متعارف خواهند بود، و باید قادر باشیم توزیع متعارف را با این توزیعها تطابق دهیم. زمانی که کوشش می‌کنیم این کار را انجام دهیم، مشکل به نظر می‌رسد که در تمام موارد از صحّت تطابق مطمئن باشیم. تعداد حروفی که در توزیعها نمایش داده شده‌اند زیاد نیست و فراوانیهای مشخصه چندان به وضوح قابل تشخیص نیستند.

با این حال، وقتی در الفبای ۳ حرف S_c را مقابل A_p قرار می‌دهیم، به نظر می‌رسد که تطابق بسیار خوبی به دست آورده‌ایم. در الفبای ۴، $I_c = A_p$، و در الفبای ۶، $R_c = A_p$ مناسب به نظر می‌رسد. اگر این معادلها درست باشند، می‌توانیم تمام حروف ستونهای مربوطه را از رمز درآوریم و ببینیم چه نتیجهٔ احتمالیی می‌توان گرفت. در اینجا حاصلِ از رمز درآوردن دوازده حرف اوّلِ ستونهای ۳، ۴، و ۶ آمده‌اند:

```
E  C  .  M
S  I  .  N
F  I  .  T
A  L  .  E
U  E  .  A
O  M  .  U
S  A  .  E
I  N  .  T
A  Y  .  R
R  E  .  O
T  B  .  T
H  E  .  A
```

ترکیبات خوب به نظر می‌رسند. تعدادی دوحرفی با فراوانی زیاد در ستونهای ۳ و ۴ مشاهده می‌شود و هیچ ترکیبی که غیر ممکن به نظر برسد مشاهده نمی‌شود. شواهد دال بر اینکه این الفباها الفباهای متعارف مستقیم‌اند بسیار قوی به نظر می‌رسند.

برای نتیجه‌گیریهای بیشتر، قدم بدیهی بعدی، تلاش برای گشودن ستون ۵ است. اگر الفبای مربوطه، الفبای متعارف مستقیم باشد، چنانکه بسیار محتمل به نظر می‌رسد، آنگاه تمام معادلهای غیر رمزی ممکن حروف آن از راه تکمیل دنبالهٔ صریح، همان طوری که در صفحات ۱۶ و ۱۷ شرح داده شد، به‌دست خواهند آمد.

دوازده حرف اول ستون ۵ را در یک سطر می‌نویسیم و از روش تکمیل دنبالهٔ صریح استفاده می‌کنیم [یعنی تمام معادلهای غیررمزی ممکن این سطر را در ۲۵ سطر زیر آن می‌نویسیم]. سپس هر یک از سطرها را، در جستجوی مجموعهٔ مناسبی از حروف متن صریح که به جای حروف غایب در ترکیبات از رمز درآمدهٔ قبلی بنشینند، بررسی می‌کنیم. معلوم می‌شود که انتخاب سطری که با O آغاز شده است، انتخاب صحیح

است.

		حاصلجمع فراوانیها	حاصلجمع وزنهای لگاریتمی
C	C B F G D F U S V I G	38	17.067
D	D C G H E G V T W J H	48	16.963
E	E D H I F H W U X K I	60	17.956
F	F E I J G I X V Y L J	42	15.188
G	G F J K H J Y W Z M K	18	10.836
H	H G K L I K Z X A N L	40	14.657
I	I H L M J L A Y B O M	49	17.432
J	J I M N K M B Z C P N	36	13.390
K	K J N O L N C A D Q O	48	15.782
L	L K O P M O D B E R P	56	18.162
M	M L P Q N P E C F S Q	49	16.885
N	N M Q R O Q F D G T R	60	18.043
O	O N R S P R G E H U S	74	20.726
P	P O S T Q S H F I V T	58	18.718
Q	Q P T U R T I G J W U	47	15.650
R	R Q U V S U J H K X V	34	15.161
S	S R V W T V K I L Y W	48	17.259
T	T S W X U W L J M Z X	38	13.217
U	U T X Y V X M K N A Y	38	15.531
V	V U Y Z W Y N L O B Z	31	13.680
W	W V Z A X Z O M P C A	35	14.122
X	X W A B Y A P N Q D B	35	14.959
Y	Y X B C Z B Q O R E C	40	14.466
Z	Z Y C D A C R P S F D	43	15.918
A	A Z D E B D S Q T G E	66	17.645
B	B A E F C E T R U H F	67	19.201

در واقع، سطر صحیح را می‌توان صرفاً با استفاده از فراوانی حروف جدول فوق و بدون بررسی چگونگی قرارگرفتن حروف مناسب در قسمتهای خالی متنِ صفحهٔ ۸۲ ، انتخاب کرد. سطر مطلوب سطری است که دارای مناسبترین مجموعهٔ حروف متن صریح باشد. این سطر را می‌توان با یادداشت‌کردن فراوانی مشخصهٔ هر حرف، جمع‌کردن فراوانی حروف

هر سطر، و توجه به آنکه کدام سطر بیشترین حاصلجمع را دارد معین کرد. حاصلجمعها در سمت راست هر سطر نمایش داده شده‌اند. چنانکه مشاهده می‌شود بزرگترین حاصلجمع متعلق به سطری است که با حرف O آغاز شده است. در واقع، از لحاظ نظریهٔ احتمالات، شیوهٔ صحیح برای نسبت دادن وزن به هر سطر، محاسبهٔ حاصلضرب تمام فراوانیهای مشخصه‌ای است که در آن سطر ظاهر می‌شوند. این کار مستلزم محاسبات خسته‌کننده‌ای است که برای سهولت می‌توان به جای آن لگاریتم فراوانیها را محاسبه کرد و سپس این به اصطلاح وزنهای لگاریتمی را با هم جمع کرد. جدولی از وزنهای لگاریتمی، یعنی لگاریتم فراوانیها، با سه رقم اعشاری، در ضمیمهٔ ب آمده است. اگر وزنهای لگاریتمی حروف هر سطر را با هم جمع کنیم، باز هم در خواهیم یافت که سطر O بهترین انتخاب است.

وقتی حروف سطر O را به متن متشکل از ستونهای ۳، ۴، و ۶ بیفزاییم، نتایجی که از همین ۱۲ حرف اول به دست آمده ما را متقاعد می‌کند که در مسیری درست هستیم.

E	C	O	M
S	I	O	N
F	I	N	T
A	L	R	E
U	E	S	A
O	M	P	U
S	A	R	E
I	N	G	T
A	Y	E	R
R	E	H	O
T	B	U	T
H	E	S	A

قدم بعدی استفاده از روش تکمیل‌دنبالهٔ صریح برای ستون ۲ است تا حروف صریحی را بیابیم که قبل از چهار حرفیهای فوق می‌آیند، همچنین به جای ستون ۲ می‌توانیم با ستون ۷ کار کنیم تا حروفی را که بعد از چهار حرفیهای فوق می‌آیند بیابیم. اگر به این طریق ادامه دهیم، متن صریح اصلی مشخص می‌شود و پیام عبارت خواهد بود از:

THE COMMISSIONER OF INTERNAL REVENUE SAID
COMPUTERS ARE MAKING TAXPAYERS MORE HONEST BUT
AT THE SAME TIME SEVERAL MILLIONS OF DOLLARS ARE
BEING RETURNED TO TAXPAYERS DUE TO THEIR MISTAKES
AGAINST THEMSELVES WHICH THE COMPUTERS PICK UP
AND CREDIT TO THEM THIS SYSTEM HAS BEEN GENERALLY
INSTALLED THROUGHOUT THE COUNTRY

[مأمور عواید مالیاتی گفت که کامپیوتر موجب شده مالیات دهندگان درستکارتر شوند، اما در عین حال با کشف اشتباهاتی که مالیات دهندگان به ضرر خود مرتکب می‌شوند و واریزکردن مبلغ این اشتباهات به حساب آنها میلیونها دلار به مالیات دهندگان برگردانده می‌شود. این سیستم در سراسر کشور برقرار شده است.]

معادلهای A_p در هفت الفبای به کار رفته عبارت‌اند از:

1	H
2	I
3	S
4	T
5	0
6	R
7	Y

که کلمهٔ کلیدی برای به رمز درآوردن پیام را به دست می‌دهند.

تمرین

پیامهای زیر را بگشایید:

۴۶. پیام داده شده در تمرین ۴۴.

۴۷. POMMG EAMVL PHBWL YVUET JKVWT NZIAZ KUIFG KBVUX ZFMKM
AYLSR POILM DPZLX AUBZH QZIFW WTMJB YHVKH QAPNB AAVSF
AZMSN OAZSE EHVSG ZUMOS AHTSG ZMWJV AZPSO ASIMG YOMVT
JLEGY BLVKB RLIYT EUALM DLDAX PJWFZ BPNLR IPTWL AHALH
BZIAZ KU

۵.۳ رمزهای چند الفبایی با دنبالهٔ صریح درهم‌ریخته

همان گونه که رمزنگاران مطّلع می‌دانند، استفاده از الفباهای متعارف مستقیم در سیستم ویژنر، متضمن زیان ناشی از خطی بودن است که در نتیجهٔ آن با تشخیص یک حرف در یک الفبای متعارف مستقیم تمام الفبا معین می‌شود.

اگر الفباها فاقد سیستم باشند، ایمنی پیام خیلی بیشتر است. یادآوری می‌کنیم (صفحهٔ ۴۴ را ملاحظه کنید) که برای ساختن الفبای تصادفی ، هر یک از دو دنبالهٔ رمزی یا صریح را می‌توان درهم‌ریخت. بنابراین به سهولت می‌توان تمام ۲۶ الفبای مربع ویژنر را با درهم‌ریختن دنبالهٔ صریح، فاقد سیستم کرد. اگر این کار انجام شود، دیگر تطبیق یک توزیع متعارف با هیچ‌یک از توزیعهای پیام رمزی ممکن نیست.

مسأله‌ای که اکنون می‌خواهیم بررسی کنیم همین مسأله است. فرض کنید می‌خواهیم پیام رمزی زیر را بگشاییم:

```
SWWJR GPRDN FMWJE XEWGR ZJQDN VJZRV SZXOJ VWWRO VBHRM
MOFDL IPAXV EZWUT CZOZA AQQJL UPKZZ XUMJA PCZOE BAWZR
ZYKZI POFOL UOCRE NYKRI CAMOX IOORR ZJKOL VWWJN VPKZA
AFOCA MZOMR CJZDY EJXEL XRFQI ZJCMA RJVWI DSWZX ASOTR
BJBZO QPXMI PDJVZ ZXHGQ SZFDQ FJZJR BMWIC EZMWL MECVY
VWZOX TWHSR UUBMT NSJDW SSOOW CUNJY VJEWI PPFSL MOQVY
CVWRI SMMHW XMEJY NUZMV MXWCR NBRDE SNB
```

شاخص انطباق ۰٫۰۴۶ است. تقریباً مسلّم است که پیام تک‌الفبایی نیست.

از بررسی توزیع سه حرفی این پیام ـکه آن را در اینجا نمی‌آوریمـ معلوم می‌شود که در این رمز هیچ صورت تکراری (دنبالهٔ تکراری حروف) با بیش از سه حرف وجود ندارد. اما نُه سه حرفی تکراری با فواصل مذکور در زیر، وجود دارند:

CZO	21	WWJ	125	CAM	28
RZJ	100	PKZ	60	JVW	132
VWW	90	ZAA	70	ZZX	121

در اینجا وضعیت به سادگی مسألهٔ قبل نیست. اگر عدد فاصله‌های بین صورتهای تکراری را تجزیه کنیم، در خواهیم یافت که عدد ۵ عامل مشترک پنج فاصله است و ۷ عامل

مشترک سه فاصله است. به نظر می‌رسد که انتخاب عدد پنج انتخاب صحیحی است، امّا از آنجا که تکرار سه‌حرفیها ممکن است اتفاقی باشد، به شواهد بیشتری نیاز داریم.

برای به دست آوردن این شواهد، کاری که می‌توانیم انجام دهیم این است که تمام متن را یک بار در پنج ستون و یک بار در هفت ستون بنویسیم و مشاهده کنیم که در کدام یک تک‌الفبایی بودن توزیع مربوط به ستونها محتملتر است.

بدون ارائهٔ محاسبات به طور مفصل، نتایج این محاسبات را می‌آوریم. شاخصهای انطباق عبارت‌اند از:

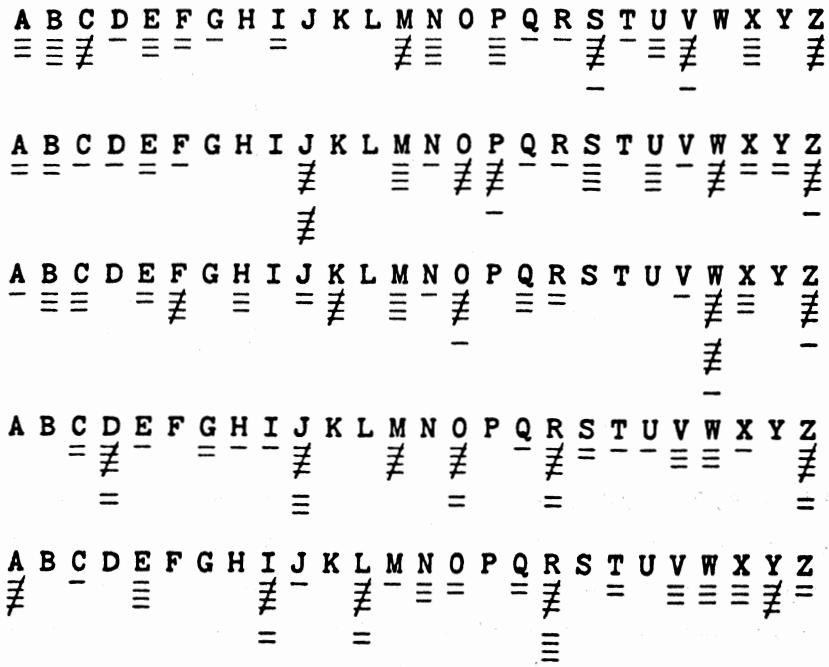
حالت هفت الفبایی		حالت پنج الفبایی	
۱	۰٫۰۴۷	۱	۰٫۰۵۲
۲	۰٫۰۴۰	۲	۰٫۰۶۴
۳	۰٫۰۳۷	۳	۰٫۰۷۰
۴	۰٫۰۴۷	۴	۰٫۰۷۴
۵	۰٫۰۵۳	۵	۰٫۰۶۸
۶	۰٫۰۵۱		
۷	۰٫۰۴۶		
شاخص میانگین:	۰٫۰۴۶	شاخص میانگین:	۰٫۰۶۶

به وضوح انتخابِ ۵ بسیار بهتر است. در حالت هفت الفبایی، ستونها به منزلهٔ ستونهای تک‌الفبایی قابل قبول نیستند. شاخصها همگی بسیار کم هستند، و به ویژه، دو تا از شاخصها حتی کمتر از شاخص کل پیام هستند. درست است که در حالت پنج الفبایی نیز یکی از شاخصها کم است، اما در وضعیت آماری چنین چیزهایی ممکن است اتفاق افتد. ممکن است اتفاقاً حروف با فراوانی کم بیش از سهم متناسبشان در آن ستون واقع شده باشند. به‌علاوه، شاخص میانگین در حالت پنج‌الفبایی بسیار خوب است اما در حالت هفت‌الفبایی ضعیف است.

در اینجا باید توجه کرد که با استفاده از شاخصهای انطباق به طریق فوق تعیین تعداد الفباها در یک پیام چند الفبایی ممکن خواهد شد، حتی اگر اصلاً تکراری وجود نداشته باشد تا به وسیلهٔ آن بتوان عرض احتمالی مناسب ستونها (طول کلمهٔ کلیدی) را به دست آورد. زیرا، می‌توان به ازای هر عرض مفروضی توزیعهایی ساخت و .I.Cهای آنها را

محاسبه کرد. اگر پیام به‌قدر کافی طولانی باشد، در عرض صحیح، . I.Cای ستونها معرف تک‌الفبایی بودن آنهاست.

تا اینجا شواهد خوبی داریم دال بر اینکه پیام مورد بحث پیامی پنج‌الفبایی است. بنابراین قاعدتاً هرکدام از پنج ستون متناظر یک تک‌الفباست. در زیر توزیعهای مربوط به این ستونها را می‌آوریم.



از آنجا که از سیستم کلی به‌کار رفته آگاه نیستیم، ابتدا تلاش می‌کنیم یک توزیع معمولی را بر این الفباها منطبق کنیم. چنین کوششهایی به نتایج سودبخشی منجر نمی‌شود. پس باید فرض کنیم که هر یک از الفباهای جایگذاری الفبایی درهم است. راهی کلی برای حل این مسأله این است که سعی کنیم هر ستون را به طور مجزا، به عنوان یک رمز تک‌الفبایی بگشاییم. فراوانی نسبی حروف مجزا را در تک‌الفباهایشان می‌دانیم. به علاوه، اطلاعاتی دربارهٔ نحوهٔ ترکیب حروف با یکدیگر داریم، و از فراوانی دو حرفیها نیز می‌توانیم در تشخیص

حروف صدادار از بی‌صدا استفاده کنیم. اما کار بسیار مشکلتر از وضعیتی است که در فصل ۲ با آن مواجه شدیم. حروفی که در یک ستون قرار دارند و بنابراین با یک الفبا به رمز در آمده‌اند، در متن پیام مجاور هم نیستند. اطلاعاتی که از دوحرفیهای متشکل از حروف یک ستون با حروف ستون قبل به دست می‌آید، باید مستقل از اطلاعاتی در نظر گرفته شود که از دوحرفیهای متشکل از حروف این ستون با حروف ستون بعد به دست می‌آید، زیرا ستونهای قبل و بعد آن با الفباهای متفاوتی به رمز در آمده‌اند. بنابراین از چنین خصوصیاتی نمی‌توان برای یافتن معادل این دوحرفیها استفاده کرد. با وجود این، احتمال دارد که بتوان قسمتی از متن را استخراج کرد. اگر پیام برای به دست دادن فراوانیهای تک حرفیِ مناسب به اندازهٔ کافی طولانی باشد، ممکن است بتوان معادلهای غیر رمزی احتمالیی برای بعضی حروف ارائه کرد. کلمات یا عبارات احتمالیی را که انتظار داریم در پیام باشند می‌توانیم با در نظر گرفتن فراوانیها و به وسیلهٔ یک نوع الگوی بخصوص مربوط به چندالفبایی بودن پیام بررسی کنیم. اگر یک کلمه یا عبارت احتمالی در یک فاصلهٔ پنج تایی (یا مضربی از پنج) دارای حروف تکراری باشد، این حروف به طور یکسان به رمز در خواهند آمد. برای ملاحظهٔ چند مثال از چنین خاصیتی معادلهای احتمالی زیر را ملاحظه کنید:

P R E S I D E N T J O H N S O N
A T O M I C E N E R G Y C O M M I S S I O N
T O M O R R O W
A S S O O N A S

حروفی که زیر آنها خط کشیده شده است در متن رمزی نیز باید یکسان باشند، وگرنه امکان ندارد فرض پنج الفبایی بودن متن مفروض درست باشد.

البته این احتمال وجود دارد که بیش از یک پیام در دسترس باشد. وضعیتی را در نظر بگیرید که رمزگشا به پیامهایی که منظماً یک سازمان ارسال می‌کند دسترسی دارد و می‌خواهد آنها را بگشاید. فرض کنید دنبالهٔ صریح همهٔ پیامها یکی باشد. در این صورت، حتی اگر هر پیام کلید خاصّی داشته باشد، الفباهایی که مربوط به حروف یکسانی از کلمات کلیدی‌اند با یکدیگر مطابق‌اند و می‌توانند ترکیب شوند. به این ترتیب اطلاعاتی که برای بررسی الفباهای مجزا در دسترس داریم انباشته شده و احتمال معلوم کردن قسمتی از رمز را افزایش می‌دهد. اما حتّی در چنین حالات خاصی نیز کار دشوار است. پس

رمزگشا چه می‌تواند بکند؟

۶.۳ تطبیق الفباها

حال به مربع ویژنر برگردیم که فرض کرده‌ایم کار به رمز درآوردن بر اساس آن صورت گرفته است، و قدری به آن توجه کنیم. فرض بر این است که در این سیستم یک دنبالهٔ صریح درهم‌ریخته و چند دنبالهٔ رمزی معمولی به کار می‌رود. دو سطر اول بالای مربع را در نظر بگیرید و فرض کنید حروف A و B هر دو در کلمهٔ کلیدی باشند.

دنبالهٔ صریح ناشناخته است

```
. . . . . .
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
```

دنبالهٔ صریح بالای مربع ناشناخته است و از قرار معلوم درهم است. فرض کنیم قرار است دنبالهٔ صریح را چنان مرتب کنیم که به ترتیب معمولی خود قرار گیرد، چنانکه مثلاً الفباها به صورت الفباهای به رمز درآوری باشند. در این صورت ستونهای داخل مربع باید مرتب شوند. و برای این کار تمام ستون باید یکجا انتقال یابد. بنابراین معادل صریح A_c در الفبای A، با معادل صریح B_c در الفبای B یکی است. همچنین B_c در الفبای A همان معادل صریحی را دارد که C_c در الفبای B داراست. به طور کلی، اگر دو حرف رمزی که در الفبای معمولی متوالی‌اند مفروض باشند، اولی همان معادل صریحی را در الفبای A دارد که دومی در الفبای B داراست. البته این معادل شناخته شده نیست، اما احتمال ظهور این دو حرف رمزی برابر است، زیرا هر دو نشاندهندهٔ یک حرف صریح‌اند. حال فرض کنید که هر حرف از الفبای B را به حرف ماقبل آن در الفبای معمولی تبدیل کنیم. چنین گامی معادل است با از رمز درآوردن هر حرف از الفبای B به وسیلهٔ الفبای جایگذاری زیر:

```
صریح  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
رمزی  B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
```

حروف رمزی جدید در الفبای B دارای معادلهای صریح یکسان با معادلهای صریح حروف رمزی در الفبای A خواهند بود. به بیان دیگر، الفبای B به الفبای A تبدیل خواهد شد. توزیعهای فراوانی این دو الفبای رمزی باید با یکدیگر مطابقت کنند، زیرا هردو متناظر با یک مجموعه از فراوانیهای حروف زبان معمولی‌اند.

حال تأثیری که این تحویل (الفبای رمز B به الفبای رمز A) در توزیع B دارد، انتقال نشانخطهای فراوانیِ زیر حروف رمزی الفبای B به اندازهٔ یک مکان به سمت چپ است. برای مثال، اگر توزیع واقعی B به قرار زیر بوده باشد:

$$\underline{\underline{A}}\ B\ C\ \underline{\underline{D}}\ E\ F\ \underline{G}\ H\ I\ J\ K\ L\ \underline{\underline{M}}\ N\ O\ \underline{\not\equiv P}\ Q\ \underline{R}\ \underline{\underline{S}}\ \underline{T}\ \underline{U}\ V\ W\ \underline{\underline{X}}\ Y\ \underline{Z}$$

با انتقال مذکور یک توزیع جدید B حاصل می‌شود که عبارت است از:

$$A\ B\ \underline{\underline{C}}\ D\ E\ \underline{F}\ G\ H\ I\ J\ K\ \underline{\underline{L}}\ M\ N\ \underline{\not\equiv O}\ P\ \underline{Q}\ \underline{\underline{R}}\ \underline{\underline{S}}\ \underline{T}\ U\ V\ \underline{\underline{W}}\ X\ \underline{Y}\ \underline{\underline{Z}}$$

با این تغییر، توزیع جدید B با توزیع اولیهٔ A مطابقت می‌کند.

این استدلال را برای هر دو الفبای متوالی از مربع ویژنر می‌توان به کار برد. اگر توزیع الفبای متناظر با دومین حرف کلمهٔ کلیدی به اندازهٔ یک مکان به چپ انتقال داده شود، توزیع حاصل معرف همان جایگذاری تک‌الفبایی است که از الفبای متناظر با اولین حرف کلمهٔ کلیدی به دست می‌آید.

به علاوه، این استدلال را می‌توان تعمیم داد. اگر فاصلهٔ بین دو سطر از مربع ویژنر n باشد، در آن صورت از انتقال توزیع متناظر با سطر پایینی به اندازهٔ n مکان به سمت چپ، همان تک‌الفبایی به دست می‌آید که توزیع الفبای بالایی معرف آن است.

اما فرض کنید فاصلهٔ بین دو سطر نامعلوم باشد. در این صورت نمی‌دانیم انتقال به اندازهٔ چند مکان باید باشد. با این حال، اندازهٔ صحیح انتقال این توزیع، از بین همهٔ اندازه‌های ممکن انتقال، با تطبیق مناسب این توزیع و توزیع سطر مفروض، قابل تشخیص است. اگر دو توزیع مطابقت یابند، در آن صورت آن دو نتیجهٔ به رمز درآوردن به وسیلهٔ یک تک‌الفبا بوده‌اند. از این موضوع باید نتیجه گرفت که مجموعهٔ حروفِ هر دو توزیع متناظر با یک تک‌الفباست. بنابراین اگر توزیع جدیدی بسازیم، به این ترتیب که فراوانی هر حرف

را مجموع فراوانیهای آن حرف در دو توزیع اصلی بگیریم، نتیجه یک توزیع تک‌الفبایی خواهد بود.

بنابراین روش تعیین اندازهٔ انتقال دو توزیع نسبت به هم، جستجوی وضعیتی است که در آن دو توزیع با یکدیگر مطابقت کنند. اگر پیام طولانی باشد و توزیعها تعداد زیادی از حروف را در برداشته باشند، ممکن است با جستجو به چنین تطابقی دست یابیم. انجام دادن این کار در واقع عبارت از آن است که توزیعها را چنان مقابل هم قرار دهیم که مکانهای متناظر دارای فراوانیهای مشابه باشند، یعنی فراوانیهای زیاد با فراوانیهای زیاد مطابقت کنند و فراوانیهای کم با فراوانیهای کم مطابق شوند، و الی آخر، به همان نحو که در مورد تطبیق الفباهای متعارف مستقیم در فصل ۱ شرح داده شد. با ممارست و تجربه، فرد می‌آموزد که چگونه در این جستجو تطابق صحیح را با چشم تشخیص دهد. در صورت فقدان چنین تجربه‌ای، یا در صورتی که تعداد حروف توزیع کم باشند، رمزگشا باید یک وسیلهٔ آماری برای کمک به تصمیم‌گیری خود بیابد.

اگر استدلال فوق منطقی بوده باشد، باید یکی از نحوه‌های ممکن قراردادن دو توزیع در مقابل یکدیگر درست باشد. در این وضعیت، اگر دو توزیع را با جمع‌کردن فراوانیهای متناظر ترکیب کنیم، توزیع مرکب باید با یک تک‌الفبا متناظر شود. در هر وضعیت دیگر، توزیع مرکب معرف توزیع دوالفبایی خواهد بود. می‌دانیم که شاخص انطباق مورد انتظار برای توزیع دوالفبایی ۰٫۰۵۲ است، در حالیکه شاخص انطباق توزیع تک‌الفبایی ۰٫۰۶۶ است. بنابراین انتظار می‌رود در حالت تطابق صحیح بیشترین شاخص انطباق از ۲۶ حالت ممکن را داشته باشیم.

به این ترتیب روش کار معلوم می‌شود. برای تطبیق دو تا از توزیعها، آنها را در هر یک از ۲۶ وضعیت ممکن مقابل هم قرار می‌دهیم. برای هر وضعیت فراوانیهای متناظر را ترکیب کرده و شاخص انطباق را تعیین می‌کنیم. قاعدتاً بزرگترین شاخص انطباق نشاندهندهٔ وضعیت صحیح است.

برای هر وضعیت، محاسبه‌ای که باید انجام شود به قرار زیر است. فرض کنید f_i نشاندهندهٔ فراوانی i امین حرف در یکی از دو توزیع باشد و تعداد کل حروف آن توزیع N باشد. فرض کنید f'_i فراوانی i امین حرف در توزیع دوّم باشد و تعداد کل حروف آن N' باشد. در توزیع مرکب، $f_i + f'_i$ فراوانی i امین حرف است، و تعداد کل حروف $N + N'$

است. طبق فرمول شاخص انطباق، داریم:

$$\text{I.C.} = \frac{\sum_{i=A}^{i=Z}(f_i + f'_i)(f_i + f'_i - ۱)}{(N+N')(N+N'-۱)}.$$

این عدد باید برای تمام ۲۶ وضعیت دو توزیع در مقابل یکدیگر محاسبه شود.

از آنجا که مخرج کسر عددی ثابت است، برای مقایسه کافی است تنها صورت کسر محاسبه شود. با بسط صورت کسر خواهیم داشت:

$$\sum_{i=A}^{i=Z}(f_i^۲ + f_i'^۲ + ۲f_if'_i - f_i - f'_i)$$

$$= \sum_{i=A}^{i=Z} f_i^۲ + \sum_{i=A}^{i=Z} f_i'^۲ + ۲\sum_{i=A}^{i=Z} f_if'_i - \sum_{i=A}^{i=Z} f_i - \sum_{i=A}^{i=Z} f'_i$$

تمام جملات عبارت فوق به استثنای سومی، تنها به یک توزیع وابسته‌اند. در نتیجه مقدار عددی چنین جملاتی مستقل از شیوهٔ قرارگرفتن دو توزیع در مقابل یکدیگر است. بنابراین در مقایسهٔ وضعیتهای متفاوتِ دو توزیع در مقابل یکدیگر، برای دریافتن آنکه درکدام وضعیت، شاخص انطباق بزرگترین مقدار را دارد، کافی است تنها یک جملهٔ $\sum_A^Z f_if'_i$ را محاسبه کنیم. (واضح است که این کار به میزان زیادی تعداد عملیات محاسبه را کاهش می‌دهد.)

حال این روش را برای پیامی که برای گشودن آن می‌کوشیم به کار می‌بریم، و جزئیات کار را برای ستونهای ۱ و ۲ شرح می‌دهیم. ابتدا، توزیع ستون ۱ را به طورکامل می‌نویسیم ـبهتر است آن را برکاغذ شطرنجی بنویسیمـ و از آنجا که قصد داریم محاسبات زیادی با فراوانی حروف انجام دهیم، استفاده از اعداد مناسبتر از نشانخط است. (شکل ۷ صفحهٔ بعد را نگاه کنید.) سپس روی یک ورق کاغذ دیگر، توزیع ستون ۲ را می‌نویسیم. این توزیع را در یک سطر دوبار پشت سرهم می‌نویسیم تا امکان لغزاندن توزیع ستون ۲ را در مقابل ستون ۱ فراهم کنیم (شکل۸، صفحهٔ بعد).

حال دو الفبا را چنان در زیر یکدیگر قرار می‌دهیم که Aها در یک ردیف قرار بگیرند (شکل ۹، صفحهٔ بعد)، فراوانیهای متناظر را ضرب می‌کنیم و همهٔ حاصلضربها را جمع می‌کنیم:

$$\sum_{i=A}^{i=Z} f_if'_i = ۳(۲) + ۴(۲) + ۵(۱) + \cdots + ۰(۲) + ۵(۶)$$

ستون ۱

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
3 4 5 1 3 2 1 0 2 0 0 0 5 4 0 4 1 1 6 1 3 6 0 4 0 5

شکل۷

ستون ۲

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
2 2 1 1 2 1 0 0 0 1 0 0 0 4 1 5 6 1 1 4 0 4 1 5 2 2 6 2 2 1 1 2 1 0 0 0 1 0 0 0 4 1 5 6 1 1 4 0 4 1 5 2 2 6

شکل۸

ستون ۱

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
3 4 5 1 3 2 1 0 2 0 0 0 5 4 0 4 1 1 6 1 3 6 0 4 0 5

ستون ۲

A B C D E F G H I J́ K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
2 2 1 1 2 1 0 0 0 1 0 0 0 4 1 5 6 1 1 4 0 4 1 5 2 2 6 2 2 1 1 2 1 0 0 0 1 0 0 0 4 1 5 6 1 1 4 0 4 1 5 2 2 6

شکل۹

ستون ۱

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
3 4 5 1 3 2 1 0 2 0 0 0 5 4 0 4 1 1 6 1 3 6 0 4 0 5

ستون ۲

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
2 1 1 2 1 0 0 0 1 0 0 0 4 1 5 6 1 1 4 0 4 1 5 2 2 6 2 2 1 1 2 1 0 0 0 1 0 0 0 4 1 5 6 1 1 4 0 4 1 5 2 2 6 2

شکل۱۰

نتیجه ۱۵۸ خواهد بود.

بعد الفبای دوّم را یک مکان به سمت چپ انتقال می‌دهیم چنانکه حرف B از آن در زیر حرف A از الفبای اول قرار گیرد (شکل ۱۰، صفحهٔ قبل) و همان محاسبات را انجام می‌دهیم. نتیجه ۱۲۹ خواهد بود.

مجدداً الفبای دوّم را به اندازهٔ یک مکان به چپ انتقال می‌دهیم و $\sum_{A}^{Z} f_i f'_i$ را محاسبه می‌کنیم. این فرایند را تا جایی ادامه می‌دهیم که محاسبه را برای هر ۲۶ وضعیت دو الفبا در مقابل یکدیگر انجام داده باشیم. مجموعهٔ نتایج مربوط به هر یک از وضعیتهای الفبای دوّم در مقابل الفبای اول در زیر داده شده است:

$\sum_{i=A}^{i=Z} f_i f'_i$ به‌ازای وضعیتهایی که در آنها حرف A از الفبای ۱ درمقابل حروف زیر از الفبای ۲ قرار گیرد.

A ۱۵۸	N ۱۳۸
B ۱۲۹	O ۱۶۱
C ۱۶۱	P ۱۳۸
D ۱۲۲	Q ۱۰۷
E ۱۳۹	R ۱۷۲
F ۱۳۶	S ۱۲۹
G ۱۰۰	T ۱۲۲
H ۱۶۹	U ۱۸۵
I ۱۲۸	V ۱۳۶
J ۱۲۴	W ۱۴۹
K ۱۸۷	X ۲۳۴
L ۸۷	Y ۹۷
M ۱۶۱	Z ۱۵۲

نتیجهٔ مربوط به وضعیتی که در آن حرف X از الفبای دوّم در زیر حرف A از الفبای اول قرارگرفته بزرگتر از سایر نتایج است. در این وضعیت الفبای ۲، به اندازهٔ ۲۳ مکان به سمت چپ انتقال یافته است.

حال این کار را برای مقابله و تطبیق توزیع ستون ۲ و ستون ۳، و سپس ستونهای ۳ و ۴، و بالاخره ستونهای ۴ و ۵ انجام می‌دهیم. نتایج در فهرست زیر آمده‌اند:

	تقابلهای ۲ و ۳	تقابلهای ۳ و ۴	تقابلهای ۴ و ۵
A	190	187	142
B	152	86	125
C	146	148	149
D	140	164	127
E	111	165	105
F	172	117	224
G	94	82	72
H	174	231	118
I	172	122	191
J	108	110	170
K	157	143	122
L	141	109	87
M	91	150	172
N	267	229	123
O	117	53	171
P	111	180	116
Q	180	146	119
R	104	103	146
S	174	204	161
T	110	108	74
U	101	126	177
V	133	190	138
W	165	114	148
X	142	124	152
Y	158	145	71
Z	111	124	200

در مورد تقابلهای ۲ و ۳ و نیز تقابلهای ۴ و ۵، جواب صحیح آشکار است، زیرا بزرگترین مقدار $\sum f_i f'_i$ به مقدار زیادی از تمام مقادیر دیگر بزرگتر است. اما در مورد

تقابلهای ۳ و ۴ دو عدد ۲۳۱ و ۲۲۹ را داریم که آنقدر به هم نزدیک‌اند که نمی‌توان یکی از آنها را با قاطعیت انتخاب کرد.

پیش آمدن چنین ابهامی چندان غیر منتظره نیست. نتایجی که می‌خواهیم از محاسباتی که هم اکنون انجام دادیم بگیریم مبتنی بر استدلالات آماری است. ۲۵ وضعیت نادرست یک الفبا در مقابل دوّمی، به نتایجی منجر می‌شود که (طبق قوانین آماری) میانگین آنها حول و حوش شاخص انطباق ۰٫۰۵۲ (I.C.ی دو الفباییها) است. اگر پیام به قدری طولانی باشد که بتوان از آن استنتاجات آماری کرد، یعنی اگر در هر توزیع تعداد حروف کافی باشد، جواب صحیح که متناظر با شاخص ۰٫۰۶۶ است، از بزرگترین جواب غلط بزرگتر خواهد بود. به عبارت دیگر، اگر پیام رمزی به اندازهٔ کافی طولانی باشد، جواب صحیح که بیشترین مقدار از ۲۶ مقدارِ محاسبه شده است و فاصله‌اش با سایر مقادیر زیاد است، همواره به سادگی قابل تشخیص خواهد بود. اگر پیام آن‌قدر طولانی نباشد که چنین تمایزی بین جواب صحیح و بزرگترین جواب نادرست موجود باشد، ممکن است با ابهاماتی نظیر ابهام کنونی مواجه شویم. حتّی در بعضی موارد ممکن است در یک تقابل نادرست، عدد $\sum f_i f'_i$ بزرگتر از مقدار صحیح باشد.

چگونه می‌توان تعیین کرد که کدام یک از دو تقابل مناسب الفباهای ۴ و ۳، تقابل صحیح است؟ توجه کنید که تا اینجا توزیع متناظر با هر یک از ستونها را فقط در مقابل توزیع ستون مجاور آن قرار داده‌ایم. نه سعی در تطبیق ۱ و ۴ کرده‌ایم، و نه ۲ و ۴، اگر چه، ممکن بود در چنان تطبیقهایی با ابهامی نظیر ابهام کنونی مواجه نشویم. در واقع، لزومی ندارد که همهٔ این تطبیقها را انجام دهیم، زیرا نیازی نیست که تقابل صحیح را از بین ۲۶ تقابل انتخاب کنیم، بلکه کافی است از بین ۲ تقابل انتخاب کنیم. برای این منظور از تقابل صحیح الفبای ۱ نسبت به الفبای ۲ و الفبای ۳ نسبت به الفبای ۲ که قبلاً تعیین کرده‌ایم استفاده می‌کنیم و به این ترتیب تطابق بین الفباهای ۱ و ۳ را، که از روی سطرهای اول و سوم جدول زیر معین می‌شود، به دست می‌آوریم:

1:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2:	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
3:	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
(i) 4:	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
(ii) 4:	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

حال تنها از دو تقابل مناسب استفاده می‌کنیم:

A(i) در ۳ متناظر با H در ۴ است،

A(ii) در ۳ متناظر با N در ۴ است،

دو سطر آخر جدول فوق را نگاه کنید و نتیجهٔ تقابل الفبای ۴ نسبت به الفبای ۱ را (در این دو حالت) در نظر گیرید:

A(i) در ۱ متناظر با R در ۴ است،

A(ii) در ۱ متناظر با X در ۴ است،

همچنین دو تقابل الفبای ۴ نسبت به الفبای ۲ را در نظر گیرید:

A(i) در ۲ متناظر با U در ۴ است،

A(ii) در ۲ متناظر با A در ۴ است.

از محاسبهٔ $\sum f_i f'_i$ برای الفباهای ۱ و ۴، در تقابل (i) عدد ۲۲۵ و در تقابل (ii) عدد ۱۶۹ به دست می‌آید؛ و برای الفباهای ۲ و ۴ نتیجهٔ بی‌فایدهٔ ۲۲۸ در تقابل (i) و ۲۲۸ در تقابل (ii) به دست می‌آید.

اگر هنوز متقاعد نشده باشیم که تقابل صحیح الفبای ۴ و ۳ از (i) به دست می‌آید، می‌توانیم با استفاده از اطلاعات خود دربارهٔ تقابل صحیح ۴ و ۵، دو تقابل ۳ را با ۵ در حالتهای (i) و (ii) معین کنیم. از این دو تقابل به ترتیب مقادیر ۲۶۹ و ۱۵۶ برای $\sum f_i f'_i$ به دست می‌آید، که نتیجه‌گیری قبلی ما را که (i) صحیح است تأیید می‌کند. حال تمام تقابلهای صحیح را برای تطابق پنج توزیع خود داریم.

جالب است بدانیم که برای به دست آوردن این تطابقها می‌توانستیم از ابتدا الفبای ۱ را به ترتیب با الفباهای ۲، ۳، ۴، ۵ تطبیق دهیم. اگر خواننده محاسبات مربوطه را انجام دهد، درخواهد یافت که در این موارد تمام تقابلهای صحیح بدون‌هیچ ابهامی قابل تعیین هستند. چنین وضعی، یعنی عدم ابهام، همان چیزی است که معمولاً باید انتظار داشت، مشروط بر اینکه پیام به قدری طولانی باشد که استنتاجات محکم آماری میسر باشد.

اگر در مورد بعضی از جوابها شکی وجود داشته باشد، آنگاه همان‌طورکه دیدیم ممکن است لازم باشد تقابل بعضی از الفباها را با بیش از یک الفبای دیگر بررسی کنیم.

نیاز به چنین تطبیقهای دیگری، باعث مطرح شدن راه حل کلی‌تری می‌شود. به جای اینکه سعی کنیم الفباها را متوالیاً با هم تطبیق دهیم، اصولی‌تر آن است که تمام تقابلهای ممکن هر الفبا را با تمام الفباهای دیگر بررسی کنیم. اگر پنج الفبا موجود باشند، باید ده دسته محاسبه انجام داد. از این محاسبات، تقابلهایی را که معرف بهترین تطبیق هر الفبا در

مقابل چهار الفبای دیگر هستند انتخاب می‌کنیم، به این ترتیب تقابلهای صحیح هر پنج الفبا را نسبت به هم می‌توانیم معین کنیم.

اگر راه حل فوق را به طریق زیر اصلاح کنیم، نتیجه خیلی بهتر خواهد بود. فرض کنیم از ده دسته تقابل تحت بررسی، آن دسته‌ای را انتخاب کنیم که تشخیص تقابل صحیح در آن قطعی به نظر می‌رسد ـ یعنی دسته‌ای که در آن بزرگترین مقدار $\sum f_i f'_i$ به مقدار زیادی از سایر مقادیر $\sum f_i f'_i$ بیشتر است. در مثال مورد بحث، می‌توانیم دستهٔ ۲ در مقابل ۳ را انتخاب کنیم، زیرا مقدار ۲۶۸ برای الفبای N تقریباً ۱٫۵ برابر دومین مقدار بزرگ $\sum f_i f'_i$ است.

سپس توزیعهای ۲ و ۳ را با مقابل هم قرار دادن آنها در وضعیتی که هم اکنون انتخاب شد ترکیب می‌کنیم:

```
2:  A B C D E F G H I  J  K L M N O P Q R S T U V W X Y Z
    2 2 1 1 2 1 0 0 0 10 0 0 4 1 5 6 1 1 4 0 4 1 5 2 2 6

3:  N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
    1 6 0 3 2 0 0 0 1 11 3 0 6 1 3 3 0 2 5 0 3 0 2 5 0 4
```

و فراوانیهای متناظر را جمع می‌کنیم. نتیجه، توزیع جدیدی است که آن را ۳ + ۲ می‌نامیم. این توزیع جدید دارای فراوانیهای زیر است:

```
2+3:  A B C D E F G H I  J  K L  M N O P Q R S T U V W X Y  Z
      3 8 1 4 4 1 0 0 1 21 3 0 10 2 8 9 1 3 9 0 7 1 7 7 2 10
```

حال این توزیع مرکب را به ترتیب با ۱، ۴، ۵ تطبیق می‌دهیم، و تقابلی را که به وضوح صحیح به نظر می‌رسد انتخاب می‌کنیم. مشاهده می‌شود که این تقابل عبارت است از تقابل توزیع ۵ و توزیع ۳ + ۲ وقتی که Z از اولی در مقابل A از دومی قرار گیرد. حال فراوانیهای توزیع ۵ را با فراوانیهای توزیع ۳ + ۲ جمع می‌کنیم تا توزیع مرکب ۵ + ۳ + ۲ به دست آید. اگر کار را به این طریق ادامه دهیم، می‌توانیم تقابلهای صحیح تمام الفباها را تعیین کنیم. فایدهٔ این کار آن است که در این ترکیبات متوالی، توزیعها بزرگتر و بزرگتر می‌شوند و لذا نتایج آماری قطعی‌تری از آنها به دست می‌آید.

ما جزئیات این محاسبات را ارائه نمی‌کنیم، بلکه آنها را به عنوان تمرین به خواننده واگذار می‌کنیم. توصیه می‌کنیم که خواننده برای اینکه تا حدی با چگونگی به دست آوردن نتایج آشنا شود، تمام این کارها را انجام دهد. بدیهی است که کارهای مذکور، مستلزم مقدار

زیادی کار محاسباتی است که بیشترِ آن را می‌توان کسل‌کننده دانست، اما به هر حال باید انجام شود. خوشبختانه می‌توان با کمک ماشینهای محاسبه یا کامپیوترهای سریع العمل این محاسبات را به سهولت انجام داد.

البته ممکن است پیام تحت مطالعه آن‌قدر کوتاه باشد که با هیچ یک از این روشها نتوان الفباها را با یکدیگر تطبیق داد. در چنین موردی، اگر با استفاده از اطلاعاتی دربارهٔ موضوع پیام، یا از طریقی دیگر، امکان دریافتن قسمتی از متن صریح وجود نداشته باشد، ترکیب و تطبیق الفباها ممکن نخواهد بود.

کاری که تا به حال برای گشودن پیام مورد بحث انجام داده‌ایم از این قرار است: ۵ الفبای پیام اصلی خود را در مقابل یکدیگر چنان قرار داده‌ایم که توزیعهای آنها مطابقت کنند. البته، این تطابق مبتنی بر این فرض بوده که دنباله‌های رمزی در مربع ویژنر دنباله‌های معمولی باشند. اما چگونه می‌توان مطمئن بود که این فرض، فرض درستی است؟ آیا از این نتایج می‌توانیم شواهد دیگری دال بر صحت این فرض به‌دست آوریم؟

از قرار معلوم از محاسباتی که هم اکنون به پایان رساندیم شاهدی به دست می‌آید، یعنی از روش استفاده از مقداری که به وضوح بزرگترین مقدار از مقادیر $\sum f_i f'_i$ است، شاهدی دال بر صحت این فرض به دست می‌آید. اگر حقیقتاً توزیعها در هیچ وضعیتی با یکدیگر مطابقت نداشتند، چنین نتایج سازگاری به دست نمی‌آمد، یعنی بزرگترین مقدار $\sum f_i f'_i$ در تمام موارد واضح نبود. اما آزمون مهم دیگری نیز وجود دارد. اگر توزیعها را در وضعیتهای تطبیقی که به کمک این محاسبات تعیین کرده‌ایم زیر هم قرار دهیم و تمام فراوانیهای متناظر را جمع کنیم، توزیع حاصل باید تک‌الفبایی باشد. حال این آزمون را انجام می‌دهیم.

تطابق نهایی الفباها با فراوانی حروف آنها در **شکل ۱۱ نشان داده شده است.**

اتفاقاً کلمهٔ ROBIN را در یک ستون از این **شکل** مشاهده می‌کنیم؛ احتمالاً این کلمه، کلید پیامی است که برای گشودن آن تلاش می‌کنیم.

باترکیب فراوانیهای تمام حروفِ هر ستون و قراردان نتایج در زیر الفبای ۱، خواهیم‌داشت:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
20	11	21	7	19	6	7	4	14	0	0	3	40	9	0	23	5	13	25	2	8	29	0	20	1	16

```
1: A B C D E F G H I J K L  M N O P Q R S T U V W X Y Z
   3 4 5 1 3 2 1 0 2 0 0 0  5 4 0 4 1 1 6 1 3 6 0 4 0 5

2: X Y Z A B C D E F G H I  J  K L M N O P Q R S T U V W
   2 2 6 2 2 1 1 2 1 0 0 0 10 0 0 4 1 5 6 1 1 4 0 4 1 5

3: K L M N O P Q R S T U V  W  X Y Z A B C D E F G H I J
   5 0 4 1 6 0 3 2 0 0 0 1 11 3 0 6 1 3 3 0 2 5 0 3 0 2

4: R S T U V W X Y Z A B C  D E F G H I J K L M N O P Q
   7 2 1 1 3 3 1 0 7 0 0 2  7 1 0 2 1 1 8 0 0 5 0 7 0 1

5: W X Y Z A B C D E F G H  I J K L M N O P Q R S T U V
   3 3 5 2 5 0 1 0 4 0 0 0  7 1 0 7 1 3 2 0 2 9 0 2 0 3
```

شکل۱۱

تعداد کل حروف در این توزیعِ مرکّب ۳۰۳ است. با خشنودی ملاحظه می‌کنیم که فراوانی مشخصهٔ حرفی که زیادترین فراوانی (۴۰) را دارد تقریباً همان ۱۳٪ است.[۱] دیگر اینکه ۴ حرف رمزی وجود دارند که اصلاً ظاهر نشده‌اند. وجود این جاهای خالی امید بخش است.[۲] اما مهمتر از همه تعیین شاخص انطباق این توزیع مرکب است، که شاهد دیگری خواهد بود بر **تک الفبایی بودن آن. مشاهده می‌شود که .I.C.ای آن مساوی ۰٫۰۶۵، در مقابل مقدار مورد** انتظار ۰٫۰۶۶، است. حال می‌توانیم احساس اطمینان کنیم که در مسیر درستی قرار داریم.

تمرین

۴۸. بهترین وضعیت تطابق دو توزیع زیر را در مقابل یکدیگر بیابید:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
1 4 2 7 4 1 6 5 0 4 2 0 1 2 0 0 1 2 3 2 0 3 0 0 0 0

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 3 1 2 4 3 0 0 2 0 4 0 0 4 0 0 0 0 0 0 2 9 5 0 2 9
```

---

۱. توجه کنید که بالاترین فراوانی مشخصه، یعنی فراوانی مشخصهٔ E، ۱۳٪ است. (م.)

۲. به صفحهٔ ۱۹ نگاه کنید. (م.)

ثابت کنید که الفبای مرکّبی که از وضعیت تطابق نتیجه می‌شود دارای شاخص انطباق تک الفبایی است.

۴۹. توزیعهای زیر را تطبیق دهید و ثابت کنید الفبای مرکبِ حاصل، تک‌الفبایی است:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	1	4	3	0	1	1	1	2	5	0	0	1	1	4	0	0	1	0	2	0	0	1	9	1	10

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	4	0	1	1	1	1	7	0	0	4	0	2	1	0	5	1	0	0	0	0	6	3	4	3	1

۵۰. آیا توزیعهای مسائل ۴۸ و ۴۹، هر دو از یک مربع ویژنر به‌دست آمده‌اند؟

۷.۳ تبدیل رمز چندالفبایی به رمز تک‌الفبایی

تا به حال چند نتیجهٔ مهم دربارهٔ پیام خود به‌دست آورده‌ایم، امّا هنوز اطلاعی از متن آن نداریم. حال چگونه آن را بگشاییم؟

شکل ۱۱ از صفحهٔ قبل را که در آن چگونگی تقابل پنج الفبا نسبت به‌هم نشان داده شده است در نظر بگیرید. این دنباله‌ها با سطرهایی از مربع ویژنر که برای به رمز درآوردن به‌کار رفته‌اند متناظرند. آنچه هنوز ناشناخته است، دنبالهٔ صریح است. این دنباله هر چه باشد، می‌دانیم که حروفِ هر ستون از شکل ۱۱، همگی دارای یک معادل صریح‌اند. این موضوع را به طریق دیگری نیز می‌توان مطرح کرد، اگر به جای هر حرف از الفبای ۲ حرف بالای آن از الفبای ۱ را بگذاریم، حرف جدید از الفبای ۲ و همان حرف از الفبای ۱ دارای یک معادل صریح خواهند بود. بنابراین برای "از رمز درآوردن" حروف الفبای ۲ از الفبای جایگذاری زیر استفاده می‌کنیم:

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

یعنی به جای هر حرف از ستون دومِ پیام رمزی، حرف بالای آن از الفبای جایگذاری فوق را قرار می‌دهیم. با انجام دادن این کار، ستون ۲ به رمزی مبتنی بر همان تک الفبای ستون ۱ تبدیل خواهد شد.

به همین نحو، به جای حروف ستون سوم پیام، حروف بالای آنها از الفبای جایگذاری زیر را قرار می‌دهیم:

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

و به این ترتیب ستون ۳ نیز به رمزی مبتنی بر همان تک‌الفبای ستون ۱ تبدیل خواهد شد. با ادامهٔ این فرایند، کلّ پیام چندالفبایی اولیه به رمزی تک‌الفبایی تبدیل می‌شود.

توجه کنید که این کار را به طریق زیر نیز می‌توان انجام داد: فرض کنید دنبالهٔ صریح مربع ویژنر همان خط ۱ از شکل ۱۱ باشد. سپس پیام اصلی را به عنوان یک رمز پنج الفبایی، با استفاده از پنج سطر شکل ۱۱ به عنوان دنباله‌های رمزی، "از رمز درآورید". نتیجه به صورت زیر خواهد بود:

SZMSV GSHMR FPMSI XHMPV ZMGMR VMPAZ SCNXN VZMAS VEXAQ
MRVMP ISQGZ ECMDX CCEIE ATGSP USAID XXCSE PFPXI BDMIV
ZBAIM PRVXP URSAI NBAAM CDCXB IREAV ZMAXP VZMSR VSAIE
AIELE MCEVV CMPMC EMNNP XUVZM ZMSVE RMLFM DVMIB AVECV
BMRIS QSNVM PGZED ZAXPU SCVMU FMPSV BPMRG ECCFP MHSEC
VZPXB TZXBV UXRVX NVZMA SVEXA CXDSC VMUFM PSVBP MRGEC
CYMAM SPCQA XPUSC NXPVZ MAMLV NEHMI SQR

دنباله‌های تکراری طولانی از حروف، در این پیام تبدیل شده وجود دارند. وجود این دنباله‌ها که با خطی در زیرشان نمایش داده شده‌اند، شاهد جالب توجهی است بر تک الفبایی بودن این پیام.

گشودن این پیام تک‌الفبایی که بالغ بر ۳۰۰ حرف دارد به سهولت انجام می‌شود. از فراوانیهای تک حرفی به‌نظر آشکار می‌رسد که $M_c = E_p$ و $V_c = T_p$. سه حرفی رمزی VZM که به کرات ظاهر شده، باید THE باشد. چهار حرفی رمزی تکراری ZMSV، در آغاز پیام به الگوهای SZMSV و VZMZMSV متعلق است و $S_c = A_p$ را تداعی می‌کند. با یافتن این مدخلها برای گشودن پیام، بقیهٔ کار آسان است. متن صریحی که حاصل می‌شود عبارت است از:

A HEAT WAVE SPREAD OVER THE WESTERN HALF OF THE NATION YESTERDAY WHILE COLLIDING WARM AND COOL AIR PRODUCED THUNDER STORMS AND FUNNEL CLOUDS IN THE NORTHEAST AND DIXIE LITTLE RELIEF FROM THE HEAT IS EXPECTED UNTIL TUESDAY AFTER WHICH NORMAL TEMPERATURES WILL PREVAIL THROUGHOUT MOST OF THE NATION LOCAL TEMPERATURES WILL BE NEARLY NORMAL FOR THE NEXT FIVE DAYS

[دیروز یک موج گرما برفراز نیمهٔ غربی مملکت منتشر شد. از برخورد هوای گرم و سرد، در شمال شرقی و در ایالات جنوبی رعد و برق و گردباد ایجاد شد. طی روزهای آینده تا سه‌شنبه اندکی از میزان گرما کاسته می‌شود و پس از آن دمای اغلب نقاط مملکت عادی خواهد شد. دمای مناطق گوناگون در پنج روز پس از آن تقریباً عادی خواهد بود.]

با گشودن این رمز تک‌الفبایی، در می‌یابیم که دنبالهٔ صریح بالای مربع ویژنر یک دنبالهٔ درهم انتقالی مبتنی بر کلمهٔ کلیدی است که بر کلمهٔ SOLVE بنا شده است، و کلمهٔ کلیدی در به رمز درآوردن پیام ROBIN بوده است.

۸.۳ رمز چندالفبایی با دنبالهٔ رمزی درهم‌ریخته

حال ببینیم ضعفِ سیستم قبل چه بود که بااستفاده از آن گشودن پیام ممکن می‌شد. برای مثال، چه چیز بود که تطبیق الفباها را مقدور می‌ساخت؟ پاسخ این سؤال، معمولی بودن دنبالهٔ رمزی است. در صورت همین معمولی بودن دنبالهٔ رمزی است که اگر دو سطر از مربع ویژنر به فاصلهٔ n از یکدیگر باشند، آنگاه فاصلهٔ الفبایی بین هر دو حرف از آنها که نمایندهٔ یک حرف صریح باشند نیز n خواهد بود. اگر یکی از این توزیعها را در مقابل دیگری انتقال دهیم تا با یکدیگر مطابقت کنند، مقدار انتقال همان عدد n است.

در واقع، برای اینکه بتوان از روشهای مذکور در بخش قبل استفاده کرد، لزومی ندارد که دنبالهٔ رمزی معمولی باشد. در صورتی که رمزگشا ترتیب دنبالهٔ رمزی را دریافته باشد، می‌تواند از روشهای مذکور استفاده کند، خواه دنبالهٔ رمزی معمولی باشد، خواه نباشد. تغییری که در عملیات گشودن پیام باید داد این است که توزیع هر الفبا را باید به ترتیب دنبالهٔ رمزی نوشت.

اما فرض کنید دنبالهٔ رمزی ناشناخته باشد. آنگاه دیگر تطبیق دادن توزیعها ممکن نخواهد بود. بنابراین رمزگشا از آن خاصیت اساسی که به او امکان می‌داد پیام را به طریقی که شرح دادیم بگشاید، محروم خواهد بود.

اگر رمزگشا با پیامی چندالفبایی مواجه شود که مربع ویژنر به‌کار رفته برای آن مبتنی بر دنبالهٔ رمزی درهم‌ریختهٔ ناشناخته‌ای باشد، چه باید بکند؟ چندالفبایی بودن پیام را همچون گذشته می‌تواند استنتاج کند، و تعداد الفباهای به‌کار رفته را می‌تواند تعیین کند. در این‌صورت او می‌داند که تمام حروفِ هر کدام از ستونها در یک الفبا هستند، و می‌تواند برای به دست

آوردن متن صریح سعی کند که معادلهای صریح حروف در هر تک‌الفبا را با استفاده از روشهای شرح داده شده در بخش ۶.۳ تعیین کند. روشن است که در چنین وضعیتی برای اینکه بتوان نتیجه‌ای به دست آورد، باید متن نسبتاً بزرگی در اختیار داشت. یک پیام کوتاهِ منفرد، در سیستمی چندالفبایی از این نوع، از ایمنی زیادی برخوردار است.

اما، فرض کنید که پیامهای زیادی فقط با استفاده از یک سیستم کلی به رمز درآمده باشند، یعنی در همهٔ آنها از یک مربع ویژنر با یک دنبالهٔ رمزی درهم‌ریخته استفاده شده باشد. به علاوه فرض کنید که در هر پیام انتخاب الفباهای به رمز درآوری بر اساس کلمهٔ کلیدیی مخصوصِ آن پیام صورت گرفته باشد. در این صورت رمزگشا می‌تواند توزیعهای تک‌الفبایی الفباهای همهٔ پیامها را تشکیل دهد. هرگاه حرفی از کلمهٔ کلیدی یک پیام در آن پیام تکرار شود یا حرفی از کلمات کلیدی چند پیام یکسان باشد، توزیعهای الفباهای رمزی متناظر با آن حرف تکراری معرف تک‌الفبای واحدی هستند. بنابراین حرفهای کلیدی تکراری را با استفاده از این نکته می‌توان تعیین کرد که توزیع الفباهای آنها بدون هیچ انتقالی با یکدیگر مطابقت دارند.

اگر تعداد پیامهایی که در دسترس است برای بررسی و نتیجه‌گیری کافی باشد، رمزگشا می‌تواند تعداد زیادی حروف رمزی را از یک الفبا جمع‌آوری کند، آن‌قدر که به تشخیص صحیح معادل تعدادی از حروف رمزی، با استفاده از فراوانی آنها، امیدوار باشد. داخل کردن این معادلهای صریح در تمام مکانهایی که آن حروف رمزی ظاهر شده‌اند ممکن است به معلوم‌شدن قسمتی از متنی منجر شود که شاید بتوان آن قسمت را توسعه داد و به اتکای آن رمزگشایی را با موفقیت انجام داد.

به‌نظر می‌رسد که در بهترین حالتها نیز این‌کار دشوار باشد، و چنین نیز هست. با این حال، گاهی وضعیتهای خاصی وجود دارند که رمزگشا می‌تواند از آنها استفاده کند. اکنون یکی از این وضعیتها را با ذکر نکات خاص مفید آن شرح می‌دهیم. این وضعیت خاص به قرار زیر است:

فرض کنید که یک پیام باید به دوگیرنده ارسال شود که دو کلید متفاوت به آنها داده شده است. برای شرح مفصل شیوه‌های رمزگشایی در چنین مورد خاصی، مثالی می‌زنیم و در حین گشودن رمز آن نشان می‌دهیم که چگونه می‌توان از چنین وضعیتی استفاده کرد.

فرض می‌کنیم که رمزگشا دو پیام زیر را که از یک مکان و تقریباً در یک زمان به دو نشانی متفاوت ارسال شده‌اند در دست دارد:

1. WCOAK TJYVT VXBQC ZIVBL AUJNY BBTMT JGOEV GUGAT KDPKV
   GDXHE WGSFD XLTMI NKNLF XMGOG SZRUA LAQNV IXDXW EJTKI
   YAOSH NTLCI VQMJQ FYYPB CZOPZ VOGWZ KQZAY DNTSF WGOVI
   IKGXE GTRXL YOIP

2. TXHHV JXVNO MXHSC EEYFG EEYAQ DYHRK EHHIN OPKRO ZDVFV
   TQSIC SIMJK ZIHRL CQIBK EZKFL OZDPA OJHMF LVHRL UKHNL
   OVHTE HBNHG MQBXQ ZIAGS UXEYR XQJYC AIYHL ZVMQV QGUKI
   QDMAC QQBRB SQNI

به وسیلهٔ شیوه‌هایی که قبلاً دربارهٔ بررسی دنباله‌های تکراری حروف و .I.C ای توزیعهای ستونی شرح داده شد، می‌توان نشان داد که هر یک از این پیامها چند الفبایی است، در اولی از شش الفبا و در دومی از پنج الفبا استفاده شده است.

به این نکتهٔ خیلی مفید توجه کنید که در اینجا طول هر دو پیام یکسان است. آنها را در زیر یکدیگر می‌نویسیم:

```
     5    10    15    20    25    30    35    40    45    50
WCOAK TJYVT VXBQC ZIVBL AUJNY BBTMT JGOEV GUGAT KDPKV GDXHE
TXHHV JXVNO MXHSC EEYFG EEYAQ DYHRK EHHIN OPKRO ZDVFV TQSIC

    55    60    65    70    75    80    85    90    95   100
WGSFD XLTMI NKNLF XMGOG SZRUA LAQNV IXDXW EJTKI YAOSH NTLCI
SIMJK ZIHRL CQIBK EZKFL OZDPA OJHMF LVHRL UKHNL OVHTE HBNHG

   105   110   115   120   125   130   135   140   145   149
VQMJQ FYYPB CZOPZ VOGWZ KQZAY DNTSF WGOVI IKGXE GTRXL YOIP
MQBXQ ZIAGS UXEYR XQJYC AIYHL ZVMQV QGUKI QDMAC QQBRB SQNI
```

در مکانهایی از دو پیام، حروف یکسانی را می‌یابیم. حال اعدادی را که نشاندهندهٔ مکان این حروف یکسان در متن هستند می‌نویسیم:

X	C	D	V	Z	A	Q	Q	G	I
12	15	42	45	72	75	102	105	132	135

این اعداد دو الگوی آشکار را نشان می‌دهند. بعضی از این حروف در مکان دوازدهم و تمام مکانهایی پس از آن آمده‌اند که فواصل میان آنها سی حرف است. باقی این حروف در مکان پانزدهم و تمام مکانهایی پس از آن آمده‌اند که فواصل میان آنها سی‌حرف است.

از این موضوع چه نتیجه‌ای می‌توان گرفت؟ توجه کنید که یک پیام دارای شش الفبا و دیگری دارای پنج الفباست، و ۳۰ کوچکترین مضرب مشترک ۶ و ۵ است. فرض کنید

هر دو پیام دارای یک متن صریح باشند (که فرضی معقول است، نظر به اینکه آنها به یک اندازه بوده و تقریباً در یک زمان ارسال شده‌اند). به علاوه فرض کنید که دو حرف یکی از کلمات کلیدی در کلمهٔ کلیدی دیگر نیز آمده باشد. از آنجا که مکان دوازدهم در هر دو پیام دارای حروف یکسانی است و با توجه به اینکه

$$۱۲ \equiv ۲ \text{ (پیمانهٔ۵)} \quad , \quad ۱۲ \equiv ۶ \text{ (پیمانهٔ۶)}$$

به این فکر می‌رسیم که

الفبای ۶ از پیام اوّل = الفبای ۲ از پیام دوّم

همچنین، از آنجا که

$$۱۵ \equiv ۵ \text{ (پیمانهٔ۵)} \quad , \quad ۱۵ \equiv ۳ \text{ (پیمانهٔ۶)}$$

احتمال می‌دهیم که

الفبای ۳ از پیام اوّل = الفبای ۵ از پیام دوّم

از $۳۰ = ۶ \times ۵$ نتیجه می‌شود که به ازای $n = ۰, ۱, ۲, \ldots$ ،

$$۱۵ + ۳۰n \equiv \begin{cases} ۳ & \text{(پیمانهٔ۶)} \\ ۵ & \text{(پیمانهٔ۵)} \end{cases} \quad \text{و} \quad ۱۲ + ۳۰n \equiv \begin{cases} ۶ & \text{(پیمانهٔ۶)} \\ ۲ & \text{(پیمانهٔ۵)} \end{cases}$$

که دلیل بر یکسان بودن حروف در مکانهای مذکور است.

چگونه می‌توانیم دربارهٔ صحّت این استنتاجات تحقیق کنیم؟ راه آن این است که ببینیم آیا الفباهای متناظر با یکدیگر مطابقت می‌کنند یا نه. توزیعها را تشکیل می‌دهیم:

الفبای ۶ پیام ۱: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

الفبای ۲ پیام ۲: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

اگر توزیعها را ترکیب کنیم و I.C. ی الفبای مرکب را محاسبه کنیم، مقدار ۰٫۰۷۵ را به‌دست خواهیم آورد.

برای دو الفبای دیگر به‌دست می‌آوریم:

الفبای ۳ پیام ۱ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

الفبای ۵ پیام ۲ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

در این مورد، I.C. ی الفبای مرکب مساوی ۰٫۰۶۶ است.

این مقادیر نشان می‌دهند که الفباهای مرکب قاعدتاً تک‌الفبا هستند. این مقادیر را می‌توان مؤید استنتاجات زیر دانست:

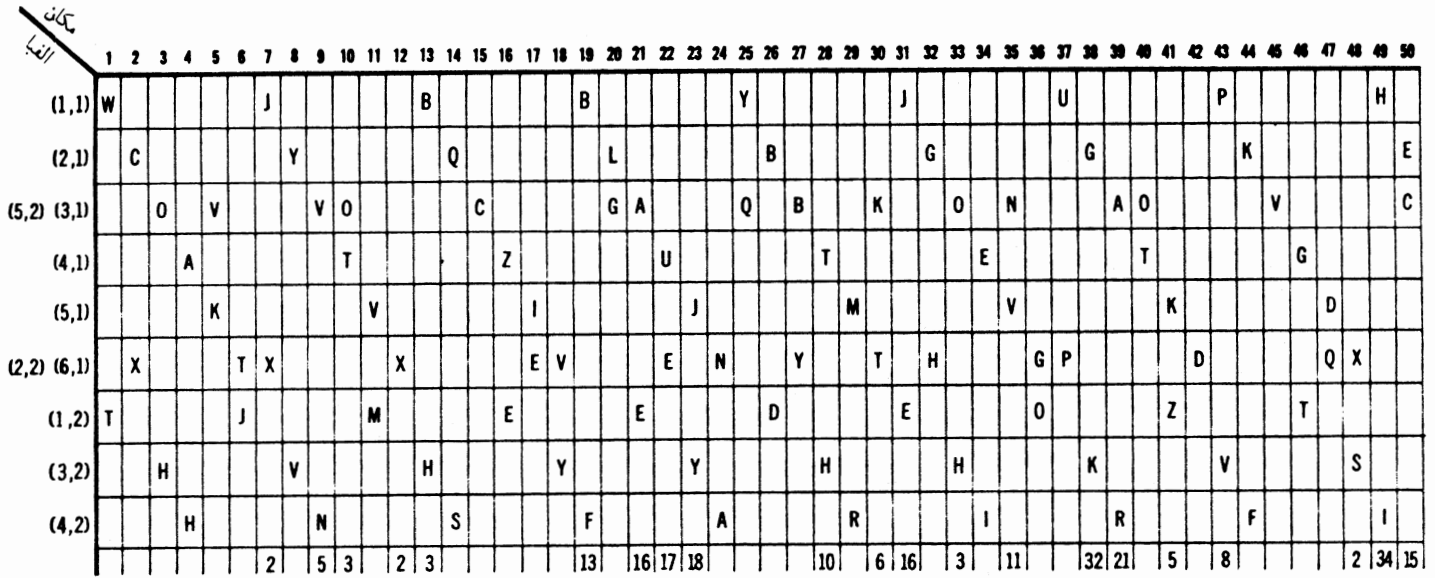
(الف) متن صریح هر دو پیام یکی است،

(ب) الفبای ۶ از پیام ۱ = الفبای ۲ از پیام ۲،

(ج) الفبای ۳ از پیام ۱ = الفبای ۵ از پیام ۲.

چون به نظر می‌رسد که متن صریح هر دو پیام یکی باشد، با نگاه‌کردن به حروف اوّل دو پیام می‌توانیم بگوییم که W_c در الفبای ۱ از پیام ۱ همان معادل صریحی را دارد که T_c در الفبای ۱ از پیام ۲ دارد. همچنین، C_c در الفبای ۲ از پیام ۱ همان‌معادل صریحی را دارد که X_c در الفبای ۲ از پیام ۲ دارد. اگر به این طریق ادامه دهیم خواهیم توانست برای هر مکان از دو پیام، معادلهای دو حرف رمزی را که یکی در پیام ۱ و دیگری در پیام ۲ است، مساوی قرار دهیم: حال اطلاعات را به طریق منظم زیر یادداشت می‌کنیم. (شکل ۱۲ صفحهٔ بعد را مشاهده کنید). برای نشان دادن نُه الفبای متفاوت، جدولی نُه سطری ایجاد می‌کنیم. (تنها نُه الفبا وجود دارند زیرا دو الفبا از پیام ۲ به پیام ۱ نیز متعلق‌اند.) سپس در ستون ۱، W و T را مطابق شکل در سطرهای مناسب می‌نویسیم تا نشاندهندهٔ این باشد که W_c در (۱, ۱) (یعنی الفبای ۱ از پیام ۱) معادل T_c در (۱, ۲)است. از معادلهای صریح آنها اطلاعی نداریم، اما می‌دانیم که این معادلها برای هر دو حرف یکسان‌اند. در ستون ۲، C و X را مطابق شکل می‌نویسیم تا نشاندهندهٔ این باشد که C_c در (۱, ۲) با X_c در (۲, ۲) معادل است. به همین طریق ادامه می‌دهیم و تمام زوجهای حروف رمزی را در سطرهای مناسب می‌نویسیم، البته به خاطر داریم که پیام ۱ دارای ۶ الفباست و پیام ۲، ۵ الفبا دارد.

یک حرف از پیام ۱ در صورتی در سطر $(r, ۱)$ قرار خواهد گرفت که عدد مکان آن به شکل $6k + r$ باشد، و یک حرف از پیام ۲ در صورتی در سطر $(s$و۲$)$ قرار خواهد گرفت که عدد مکان آن به شکل $5k + s$ باشد. شکل ۱۲ جدولِ مربوط به ۵۰ حرف اول را نشان



شکل۱۲

می‌دهد؛ به علاوه نشان می‌دهد در حالت $r = ۳$ و $s = ۵$ یک سطر برای نشان‌دادن الفباهای یکسان (۱ ,۳) و (۲ ,۵) به‌کار می‌رود؛ و همین‌طور در مورد $r = ۶$ و $s = ۲$.

حال می‌توانیم بعضی از ستونهای این جدول را به طریق زیر ترکیب کنیم. از آنجا که حروف رمزی در هر یک از سطرها همه از یک الفبا هستند، حرف تکراری در یک سطر باید متناظر با یک حرف صریح تکراری باشد. بنابراین، معادل صریح حروف ستون ۷ که دارای X در (۲ ,۲) است باید همان معادل صریح حروف ستون ۲ باشد که آن هم دارای X در (۲ ,۲) است. در نتیجهٔ یکی‌بودن این معادلهای صریح، این دو ستون را می‌توان در یک ستون که شامل سه حرف J، C، و X در سطرهای (۱ ,۱)، (۱ ,۲) و (۲ ,۲) است ترکیب کرد.

به همین طریق ستون ۹ را می‌توان با ستون ۵ ترکیب کرد، زیرا در سطر سوم هر دو ستون V آمده است و بنابراین هر دو ستون معرف یک حرف صریح‌اند. برای اینکه این کار را در تمام جدول انجام دهیم، ستونهای هم‌ارز، یعنی ستونهایی را که معرف یک حرف صریح‌اند، با شماره‌گذاری در زیر آنها مطابق شکل معین می‌کنیم. سپس این ستونهای هم‌ارز را ترکیب می‌کنیم. با این کار تعداد ستونها کاهش می‌یابد و در عین حال، تعداد درایه‌ها در بعضی از ستونها افزایش می‌یابد. به‌عنوان مثال، از ترکیب ستونهای ۳، ۱۰، ۱۳، ۱۹ ستون زیر حاصل می‌شود:

(1,1)	B
(2,1)	
(3,1)	O
(4,1)	T
(5,1)	
(6,1)	
(1,2)	
(3,2)	H
(4,2)	F

ستون ۳۳ که O و H در آن آمده‌اند مؤید صحت اطلاعات فوق است.

البته فرایند فهرست کردن ستونها و ترکیب آنها را می‌توان تاانتهای دو پیام رمزی ادامه داد. تکمیل این‌کار را به خواننده واگذار می‌کنیم. نتیجهٔ نهایی، بعد از انجام‌دادن تمام ترکیبات

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7
(1,1)	W	J	B		D	P		M		N	U	X		L		H	Y		R								T			Z	K	O	
(2,1)	Q	C	K	X		Y		E		A	L		B		G		T			U		V						J				
(3,1)	L	A	O	V	K	W	N	C		Z	G		S	B			Q					F	I	J		E			R			
(4,1)	G	Z	T	F				A	U	X	I					E	L								S							
(5,1)	Y	M	D	K	F		V	R	I	J	W						S				A					H		O				P
(6,1)	I	X	Q	D	T			Z	E	V	P	N		Y	H		G	F			J		K				B					
(1,2)	T	E		Z	J	S	M	U		C	Q	H	D				O					X	L							A		
(3,2)	J	S	H			V	I	B		Y	N			A	K		M		D										E		U	
(4,2)	S	R	F	N		G		H		M	Y	A	Q				B	J		P		K			T			X				I

شکل۱۳

ممکن، در شکل ۱۳ نمایش داده شده است.

سودمندی این جدول آشکار است. تمام حروف هر یک از ستونها، معرف یک حرف صریح‌اند. اگر معادلهای دلخواهی در بالای هر ستون بنویسیم، و پیام را با آن معادلها "از رمز درآوریم" پیام به پیامی تقریباً تک‌الفبایی تبدیل خواهد شد. ناچاریم بگوییم "تقریباً" زیرا در جدول خود، ۳۳ ستون داریم و در نتیجه در پیام تبدیل یافته ۳۳ حرف خواهیم داشت.

اگر ۳۳ ستون جدول را همان‌طورکه‌در شکل ۱۳ نشان‌داده شده است به‌ترتیب با A، . . . ، Z، ۱، ۲، . . . ، ۷ نامگذاری کنیم، حاصل "از رمز درآوردن" پیام به‌صورت زیر خواهدبود:

ABCHD EBFDC GBCAH BIJCK BIJLQ MNCBE BOC7G QKOBC DDFCD
ACB7H FAQRE DACBA JCGQE BHOCA QHSTB QUCJV WJCBA HXCDA
QJCYZ L1KHK GCH2Q DANFM HB3K4 VCAKH 5AJHA DJQMD KQ6VO
KDQLH KCHBN FCK7

بعضی از این ۳۳ علامت هم‌ارزند (یعنی معرف یک حرف‌اند). متن پیام اصلی آن‌قدر طولانی نبود که تمام ستونهای هم‌ارز مشخص شوند، و بنابراین، در واقع از جایگذاریی استفاده کرده‌ایم که آن را جایگذاری تک‌الفبایی با هم‌ارزها می‌گویند. به عبارت دیگر، بعضی از ستونهای شکل ۱۳ باید یکی شوند. اما این یکی‌کردن نباید به تناقض منجر شود. می‌توانیم بگوییم که ستونهای A، B، C، H، J، K، Q با هیچ ستونی هم‌ارز نیستند، زیرا اگر هر یک

از آنها با ستون دیگری ترکیب شوند، دو حرف متفاوت باید یک محل را اشغال کنند. تنها هم‌ارزهای احتمالیِ ستونِ D، ستونهای S و ۶ هستند، زیرا دو ستون اخیر تنها ستونهایی هستند که درایه‌های آنها فقط در سطرهایی قرار دارند که ستون D در آن سطرها دارای جای خالی است، یعنی سطرهای (۱, ۱) و (۲, ۳). چند استنتاج مشابه دیگر دربارهٔ هم‌ارزهای ممکن می‌توان کرد که در تلاش برای گشودن این پیام تک‌الفبایی مفید خواهند بود.

به خواننده توصیه می‌کنیم که رمز تبدیل یافتهٔ مزبور را بگشاید. این‌کار را در اینجا انجام نخواهیم داد، زیرا از طرق دیگری نیز می‌توان اطلاعاتی دربارهٔ ستونهای هم‌ارز باقیمانده به دست آورد و لذا ستونهای دیگری از جدول را ترکیب کرد. هنوز از این موضوع که پیام احتمالاً با استفاده از مربع ویژنر به رمز درآمده، استفادهٔ کامل نکرده‌ایم. حال فرض می‌کنیم که پیام با استفاده از مربع ویژنر به رمز درآمده باشد، و چگونگی استفاده از چنین فرضی را بررسی می‌کنیم.

کاری که می‌خواهیم انجام دهیم، به دست آوردن بعضی از خواص کلی مربع ویژنر است. کلی‌ترین حالت یک مربع ویژنر را در نظر بگیرید، یعنی مربعی که هم دنبالهٔ رمزی آن درهم است، هم دنبالهٔ صریح آن. من باب مثال، فرض کنید دنبالهٔ صریح مربع، دنبالهٔ درهم مبتنی بر کلمهٔ کلیدی با کلید NEW YORK CITY است و دنبالهٔ رمزی مربع، دنبالهٔ درهم انتقالی مبتنی بر کلمهٔ کلیدی با کلید CHICAGO است. مربع ویژنر مربوطه در شکل ۱۴ نشان داده شده است. چنانکه می‌دانیم در مربع ویژنر می‌توان هر سطر را از سطر دیگر با انتقال آن سطر به اندازهٔ مناسب به دست آورد.

حال الفباهای جایگذاری را چنان مرتب می‌کنیم که به صورت الفباهای به رمز درآوری درآیند. برای انجام دادن این کار باید دنبالهٔ صریح را به صورت معمولی درآوریم. بنابراین ستونی را که A در بالای آن است در جای ستون اول قرار می‌دهیم، ستونی را که B در بالای آن است در جای ستون دوّم قرار می‌دهیم، و الی آخر. به این ترتیب مربع به شکلی که در شکل ۱۵ نشان داده شده است درخواهد آمد.

بیست و شش الفبایی که در این مربع ایجاد شده همان الفباهای مربع اصلی‌اند. اما دیگر رابطهٔ بین دو سطر مربع آشکار نیست. دیگر نمی‌توان دنبالهٔ رمزی اصلی را در سطرهای مربع مشاهده کرد. اما این دنباله را در ستونهای مربع می‌توان مشاهده کرد؛ زیرا برای مرتب کردن مجدد دنباله‌ها به طوری که در مربع جدید دنبالهٔ صریح به صورت معمولی باشد، لازم بود که هر ستون را یکجا انتقال دهیم.

صریح	N	E	W	Y	O	R	K	C	I	T	A	B	D	F	G	H	J	L	M	P	Q	S	U	V	X	Z
	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X
	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C
	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B
	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L
	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S
	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y
	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H
	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D
	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M
	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T
	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z
رمزی	E	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I
	N	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E
	U	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N
	A	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U
	F	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A
	P	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F
	V	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P
	G	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V
	J	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G
	Q	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J
	W	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q
	O	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W
	K	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O
	R	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K
	X	C	B	L	S	Y	H	D	M	T	Z	I	E	N	U	A	F	P	V	G	J	Q	W	O	K	R

شکل۱۴

حال دو سطر را از مربع شکل ۱۵ انتخاب می‌کنیم، مثلاً سطرهای اول و چهارم را.

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی	I	E	M	N	B	U	A	F	T	P	D	V	G	C	Y	J	Q	H	W	Z	O	K	L	R	S	X
	U	A	I	F	Y	P	V	G	E	J	Z	Q	W	S	M	O	K	T	R	N	X	C	H	B	D	L

چون این سطرها در مربع شکل ۱۵ سه سطر با یکدیگر فاصله دارند، نتیجه می‌گیریم که دو حرفِ هر یک از ستونهای فوق، در دنبالهٔ رمزی اصلی، سه حرف فاصله دارند. و این به معنی آن است که این زوجهای ستونی، در طرح چند در میان دنبالهٔ رمزی اصلی با فاصلهٔ ۳، حروفی متوالی‌اند. بنابراین می‌توانیم به طریق زیر طرح چند در میان دنبالهٔ رمزی اصلی را با فاصلهٔ ۳ به

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	I	E	M	N	B	U	A	F	T	P	D	V	G	C	Y	J	Q	H	W	Z	O	K	L	R	S	X
	E	N	T	U	L	A	F	P	Z	V	M	G	J	B	H	Q	W	D	O	I	K	R	S	X	Y	C
	N	U	Z	A	S	F	P	V	I	G	T	J	Q	L	D	W	O	M	K	E	R	X	Y	C	H	B
	U	A	I	F	Y	P	V	G	E	J	Z	Q	W	S	M	O	K	T	R	N	X	C	H	B	D	L
	A	F	E	P	H	V	G	J	N	Q	I	W	O	Y	T	K	R	Z	X	U	C	B	D	L	M	S
	F	P	N	V	D	G	J	Q	U	W	E	O	K	H	Z	R	X	I	C	A	B	L	M	S	T	Y
	P	V	U	G	M	J	Q	W	A	O	N	K	R	D	I	X	C	E	B	F	L	S	T	Y	Z	H
	V	G	A	J	T	Q	W	O	F	K	U	R	X	M	E	C	B	N	L	P	S	Y	Z	H	I	D
	G	J	F	Q	Z	W	O	K	P	R	A	X	C	T	N	B	L	U	S	V	Y	H	I	D	E	M
	J	Q	P	W	I	O	K	R	V	X	F	C	B	Z	U	L	S	A	Y	G	H	D	E	M	N	T
	Q	W	V	O	E	K	R	X	G	C	P	B	L	I	A	S	Y	F	H	J	D	M	N	T	U	Z
رمزی	W	O	G	K	N	R	X	C	J	B	V	L	S	E	F	Y	H	P	D	Q	M	T	U	Z	A	I
	O	K	J	R	U	X	C	B	Q	L	G	S	Y	N	P	H	D	V	M	W	T	Z	A	I	F	E
	K	R	Q	X	A	C	B	L	W	S	J	Y	H	U	V	D	M	G	T	O	Z	I	F	E	P	N
	R	X	W	C	F	B	L	S	O	Y	Q	H	D	A	G	M	T	J	Z	K	I	E	P	N	V	U
	X	C	O	B	P	L	S	Y	K	H	W	D	M	F	J	T	Z	Q	I	R	E	N	V	U	G	A
	C	B	K	L	V	S	Y	H	R	D	O	M	T	P	Q	Z	I	W	E	X	N	U	G	A	J	F
	B	L	R	S	G	Y	H	D	X	M	K	T	Z	V	W	I	E	O	N	C	U	A	J	F	Q	P
	L	S	X	Y	J	H	D	M	C	T	R	Z	I	G	O	E	N	K	U	B	A	F	Q	P	W	V
	S	Y	C	H	Q	D	M	T	B	Z	X	I	E	J	K	N	U	R	A	L	F	P	W	V	O	G
	Y	H	B	D	W	M	T	Z	L	I	C	E	N	Q	R	U	A	X	F	S	P	V	O	G	K	J
	H	D	L	M	O	T	Z	I	S	E	B	N	U	W	X	A	F	C	P	Y	V	G	K	J	R	Q
	D	M	S	T	K	Z	I	E	Y	N	L	U	A	O	C	F	P	B	V	H	G	J	R	Q	X	W
	M	T	Y	Z	R	I	E	N	H	U	S	A	F	K	B	P	V	L	G	D	J	Q	X	W	C	O
	T	Z	H	I	X	E	N	U	D	A	Y	F	P	R	L	V	G	S	J	M	Q	W	C	O	B	K
	Z	I	D	E	C	N	U	A	M	F	H	P	V	X	S	G	J	Y	Q	T	W	O	B	K	L	R

شکل۱۵

دست آوریم. با حرف I آغاز می‌کنیم و پس از آن حرف U را (که حرف زیر I در ستون A است) می‌نویسیم. سپس U را در سطر بالایی یافته و حرف زیر آن را که P است پس از آن می‌نویسیم؛ محل P را در سطر بالایی تعیین کرده و حرف زیر آن را که J است پس از آن می‌نویسیم، و الی آخر. این فرایند «زنجیره‌ای» را ادامه می‌دهیم و دنبالهٔ ۲۶ حرفی الفبا را ایجاد می‌کنیم:

I U P J O X L H T E A V Q K C S D Z N F G W R B Y M

به سهولت مشاهده می‌شود که این دنباله طرح چند در میان دنبالهٔ رمزی اصلی با فاصلهٔ ۳ است.

اگر دو سطری که با آنها آغاز کردیم n سطر فاصله می‌داشتند، از فرایند زنجیره‌ای، طرح

چند در میان دنبالهٔ اصلی با فاصلهٔ n به دست می‌آمد، البته مشروط برآنکه n نسبت به ۲۶ اوّل باشد. اگر n زوج باشد، نتیجه دو دنبالهٔ ۱۳ حرفی خواهد بود. اگر n عدد ۱۳ باشد، نتیجه ۱۳ زوج از حروف خواهد بود. در این دو حالت اخیر اطلاعات حاصل مفید است، امّا برای آنکه دنبالهٔ ۲۶ حرفی به دست آید باید فاصلهٔ طرح چند در میان نسبت به ۲۶ اوّل باشد.

اگر در مربع ویژنر اصلی ترتیب دنباله‌ها طوری تغییر داده شود که دنبالهٔ صریح دلخواهی به دست آید، بازهم از همین روش برای به دست آوردن دنبالهٔ رمزی با طرح چند در میان می‌توان استفاده کرد. در تمام مواردی که ستونها یکجا انتقال یابند، از دو سطر مربع، با استفاده از فرایند زنجیره‌ای، دنبالهٔ رمزی اصلی با طرح چند درمیان به دست می‌آید.

خاصیت مهمّی که دنبالهٔ با طرح چند درمیان دارد آن است که مربع ویژنرِ حاصل از این دنباله از جهت خاصّی معادل مربع اصلی است.

برای روشن‌شدن موضوع، مربع ویژنری را که با یکی از دنباله‌های با طرح چند در میان ساخته شده بررسی می‌کنیم. به عنوان مثال از دنباله‌ای که دارای فاصلهٔ ۳ است استفاده می‌کنیم. مربع در شکل ۱۶ نشان داده شده است.

اگر دنبالهٔ صریح مناسبی را در بالای این مربع قرار دهیم، همان ۲۶ الفبای حاصل از مربع ویژنر اصلی را خواهیم داشت. یک راه برای ساختن چنین دنباله‌ای آن است که اوّلین الفبای این مربع جدید را با اولین الفبای جایگذاری مربع اصلی یکی کنیم. یعنی، دنبالهٔ زیر را به عنوان دنبالهٔ رمزی انتخاب کنیم:

I U P J O X L H T E A V Q K C S D Z N F G W R B Y M

و دنبالهٔ صریحی را بیابیم که الفبای زیر از آن حاصل شود:

صریح	**A B C D E F G H I J K L M N O P Q R S T U V W X Y Z**
رمزی	**I E M N B U A F T P D V G C Y J Q H W Z O K L R S X**

دنبالهٔ صریح مطلوب عبارت است از:

A F J P U Z W R I B G L Q V N Y K T D H M S X E O C

وقتی دنباله‌ای را که اکنون به دست آوردیم در بالای مربع ویژنرِ مبتنی بر دنبالهٔ رمزی

I U P J O X L H T E A V Q K C S D Z N F G W R B Y M

صریح

I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M
U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I
P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U
J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P
O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J
X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O
L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X
H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L
T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H
E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T
A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E
V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A
Q	K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V
K	C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q
C	S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K
S	D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C
D	Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S
Z	N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D
N	F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z
F	G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N
G	W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F
W	R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G
R	B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W
B	Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R
Y	M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B
M	I	U	P	J	O	X	L	H	T	E	A	V	Q	K	C	S	D	Z	N	F	G	W	R	B	Y

رمزی

شکل ۱۶

قرار دهیم، ۲۶ الفبای حاصل همان ۲۶ الفبای اصلی خواهند بود. ولی، ترتیب این دو دسته الفبا یکی نخواهد بود. اگر الفباهای متوالی که از مربع اصلی حاصل می‌شوند ۱، ۲، ۳، ... ، ۲۶ باشند، این الفباها در مربع با طرح چند درمیان به ترتیب زیر ظاهر می‌شوند:

$$۱, ۴, ۷, ۱۰, \ldots, ۲۵, ۲, ۵, \ldots, ۲۳, ۲۶, ۳, ۶, \ldots, ۲۱, ۲۴.$$

بنابراین، ۲۶ الفبای حاصل از یک مربع مبتنی بر دنبالهٔ با طرح چند درمیان، صرف‌نظر از ترتیبشان، همانهایی هستند که از مربع اصلی حاصل می‌شوند.

اگر پیامی r الفبایی با استفاده از مربع اصلی به رمز درآمده باشد ـ که در آن از r سطر

مربع، که با کلمهٔ کلیدی معین می‌شوند، استفاده شده باشد ـ مجموعهٔ مناسبی از r سطر مربعِ با طرح چند درمیان دقیقاً همان رمز را تولید خواهد کرد.

حال فرض کنید به طریقی این سطرهای مربعِ با طرح چند درمیان را به درستی تعیین کرده‌ایم، اما دنبالهٔ صریح را نمی‌دانیم. در این صورت یک دنبالهٔ "صریح" انتخاب می‌کنیم و پیام را با استفاده از آن "از رمز درمی‌آوریم". این‌کار در واقع یک رمزنگاری تک‌الفبایی از متن صریح اصلی خواهد بود، زیرا فقط "اسامی "حروف قرارگرفته در بالای ستونهای مربع ویژنر تغییر یافته‌اند. بنابراین با استفاده از روشهای فوق در مربعِ با طرح چند درمیان نتایجی حاصل می‌شود که معادلهای تک‌الفبایی متن صریح‌اند.

حال به پیام رمزی خود که آن را مبتنی بر مربع ویژنر می‌دانیم برمی‌گردیم. بجز بعضی جاهای خالی و بعضی ستونهای هم‌ارز، سطرهای صحیح مورد نیاز برای از رمز درآوردن پیام را بازسازی کرده‌ایم. اگر دو سطر کامل در دست داشتیم، می‌توانستیم با استفاده از فرایند زنجیره‌ای، یک طرح چند درمیان دنبالهٔ رمزی اصلی را به دست آوریم. اکنون دو سطر کامل در دست نداریم. امّا می‌توانیم قسمتهایی از یک دنبالهٔ با طرح چند درمیان را به دست آوریم. برای مثال، اگر با سطرهای (۳, ۲) و (۴, ۲) آغاز کنیم، می‌توانیم نتیجه بگیریم که دو حرفِ هر یک از زوجهای JS، SR، HF، VG، BH، YM، NY، MB در یک طرح چند درمیانِ دنبالهٔ رمزی اصلی متوالی‌اند. با پهلوی هم قراردادن زوجهایی که دارای یک حرف مشترک هستند، درخواهیم یافت که دنباله‌های حروف زیر

J S R
N Y M B H F
V G

در آن طرح چند درمیان قرارگرفته‌اند. دربارهٔ اینکه فاصلهٔ این طرح چنددرمیان چه ممکن است باشد چیزی نمی‌دانیم. فرض کنید این فاصله k باشد.

کاری که می‌خواهیم انجام دهیم این است که این دنباله‌های حروف را با استفاده از اطلاعات دیگری از جدول گسترش دهیم. برای مثال، فاصلهٔ طرح چند درمیانی که از دو سطر (۱, ۱)و (۳, ۲) به دست می‌آید باید k باشد. زیرا آن دو سطر نیز شامل زوجهای JS، BH، MB، NY و YM هستند که به طور عمودی قرارگرفته‌اند. بنابراین زوجهای WJ، PV، UN، LA، RD، OV را نیز می‌توان متعلق به همان طرح چند درمیان دانست و با

استفاده از دنباله‌هایی که قبلاً به دست آمده‌اند، دنباله‌های زیر را به دست آورد:

W J S R D
O U N Y M B H F
P V G
L A

حال به ترتیب به سطرهای (۱,۲)و (۱,۱) نگاه کنید. از آنجا که آنها شامل زوجهای JD، VM، OY هستند، فاصلهٔ طرح چند درمیان حاصل از آنها باید $3k$ باشد. هر زوج از حروفِ سطرهای (۱,۲)و (۱,۱)، که حرف اول آن از سطر (۱,۲) و حرف دوم از سطر (۱,۱) باشد، در دنبالهٔ با طرح چند درمیان با فاصلهٔ k ، باید به فاصلهٔ ۳ از یکدیگر باشند. بنابراین، در چنین دنباله‌ای، خواهیم داشت:

T..W, E..J, S..P, C..N, Q..U, H..X, A..K

در دنبالهٔ حروف W J S R D، حروف T را سه مکان قبل از W قرار داده، E را سه محل قبل از J، و P را سه محل بعد از S قرار می‌دهیم، در نتیجه به‌دست می‌آوریم:

T E . W J S R D P

دنبالهٔ P V G را قبلاً به دست آورده‌ایم و می‌توانیم آن را با دنبالهٔ فوق که به‌P خاتمه یافته ترکیب کنیم:

T E . W J S R D P V G

همچنین می‌توانیم C، Q و X را به دنبالهٔ آغاز شده با OU که قبلاً به دست آورده‌ایم اضافه کنیم و به دست آوریم:

Q C O U N Y M B H F . X

و از ترکیب A..K با LA به دست آوریم:

L A . . K

حال به سطرهای (۱,۱) و (۴,۱) توجه کنید. دنباله‌های WG و NX باید متعلق به طرح چند درمیان با فاصلهٔ $7k$ باشند، زیرا حروف هر یک از آنها در طرح چند درمیان با فاصلهٔ k، به فاصلهٔ ۷ از یکدیگر قرار دارند. بنابراین JZ، BT، MA، UI، HE، YL باید در طرح

چند درمیان با فاصلهٔ k، به فاصلهٔ ۷ از یکدیگر باشند. از ترکیب این زوجها و دنباله‌های جزئی که تا اینجا به دست آمده‌اند، دنبالهٔ زیر به دست می‌آید:

T E K W J S R D P V G Z Q C O U N Y M B H F I X L A

که دنبالهٔ کامل با طرح چند درمیان با فاصلهٔ k است.

حال که این دنباله معلوم شده، پرکردن جاهای خالی جدول، که ستونهای آن از مربع ویژنر هستند، امکانپذیر است. از دو سطر اول، یعنی (۱ ,۱) و (۲ ,۱) آغاز می‌کنیم. توجه کنید که W و Q از ستون ۱، در دنبالهٔ فوق، به فاصلهٔ ۹ از یکدیگر قرار دارند. بنابراین دو درایهٔ هر ستون از آن دو سطر باید به فاصلهٔ ۹ از یکدیگر باشند. پس حرف بالای X از سطر دوّم باید O باشد؛ حرفی که در سطر ۲ در زیر D از سطر اوّل واقع است باید N باشد؛ حرف زیر X از سطر اوّل باید R باشد، و الی آخر. در هر ستون از سطرهای ۱ و ۲ که یک حرف از آن شناخته شده باشد، حرف دوم را می‌توان با استفاده از دنبالهٔ با طرح چند درمیان شناخته شده، نوشت. وقتی این‌کار انجام شد، ستون چهارم را می‌توان با ستون ماقبل آخر یکی کرد، و نیز دو ستونی را که در سطر (۱ ,۱) از آنها R آمده می‌توان یکی کرد، همچنین دوستونی را که در سطر (۱ ,۱) از آنها T آمده می‌توان یکی کرد (جدول زیر را مشاهده کنید).

(1,1)	W	J	B	O	D	P		M		N	U	X	G	L	E	H	Y		R	R		T					T	F		Z	K	O	
(2,1)	Q	C	K	X	N	Y		E		A	L	R	B	D	G	W	T		U	U		V					V	J		H	Z	X	
(3,1)	L	A	O	V	K	W	N	C		Z	G		S	B			Q					F	I	J		E				R			
(4,1)	G	Z	T	F				A	U	X	I					E	L								S								
(5,1)	Y	M	D	K	F		V	R	I	J	W						S				A					H			O			P	
(6,1)	I	X	Q	D	T			Z	E	V	P	N		Y	H		G	F			J			K			B						
(1,2)	T	E		Z	J	S	M	U		C	Q	H	D				O					X	L								A		
(3,2)	J	S	H			V	I	B		Y	N			A	K		M		D										E			U	
(4,2)	S	R	F	N		G		H		M	Y	A	Q				B	J		P		K			T			X					I

حال مشاهده می‌کنیم که حروف زوجهای هر ستون از سطرهای (۱ ,۲) و (۱ ,۳) در دنبالهٔ فوق به فاصلهٔ ۱۲ از یکدیگر قرار دارند. با استفاده از این اطلاعات می‌توانیم در هر ستونی که یک حرف از آن دو سطر معلوم است، حرف دیگر را معلوم کنیم.

با ادامهٔ این کار می‌توان تمام جدول را پر کرد. در نتیجه ستونهای جدول به ۲۱ ستون کاهش پیدا می‌کند. اگر در بالای این ستونها ۲۱ حرف به دلخواه قرار دهیم، آنگاه می‌توانیم پیام اصلی را با این ۲۱ حرف "از رمز در آوریم"، و نتیجه یک پیام رمزی تک‌الفبایی از متن صریح اصلی خواهد بود. می‌توانیم نتیجه بگیریم که متن صریح تنها شامل ۲۱ حرف متمایز است. پیام تک‌الفبایی به قرار زیر خواهد بود:

```
ABCHD EBFDC GBCAH BFJCK BFJLQ MNCBE BOC7G QKOBC
DDFCD ACB7H FAQRE DACBA JCGQE BHOCA QHSSB QUCJV
OJCBA HXCDA QJCNS LVKHK GCHGQ DANFM HBVKU VCAKH
RAJHA DJQMD KQDVO KDQLH KCHBN FCK7
```

گشودن این متن دشوار نیست. متن صریح با TREASURY SECRETARY آغاز می‌شود.

توجه کنید که دنبالهٔ درهم بازسازی شده در صفحهٔ قبل ممکن نیست دنبالهٔ رمزی اصلی در مربع ویژنر بوده باشد. با این حال، این دنباله طرحی چند درمیان از دنبالهٔ اصلی است و، به این دلیل، می‌توان از آن به جای دنبالهٔ رمزی اصلی برای از رمز درآوردن استفاده کرد.

اگر تعیین دنبالهٔ اصلی مورد نظر بود، لازم بود که تمام طرحهای چند درمیانِ دنبالهٔ فوق را با فاصله‌های فرد بنویسیم (به استثنای فاصلهٔ ۱۳) و ببینیم که درکدام یک از آنها شواهدی دال بر اینکه به درستی ساخته شده دیده می‌شود. اگر چنین دنباله‌ای به دست آید، همان دنبالهٔ اصلی خواهد بود. آنگاه چون مربع ویژنر را با این دنبالهٔ رمزی اصلی بسازیم، دنبالهٔ صریح اصلی در بالای مربع ظاهر می‌شود.

۹.۳ تذکرات کلی دربارهٔ رمزهای چندالفبایی

در این فصل از روشهایی بحث می‌کنیم که با استفاده از آنها رمزهای چندالفبایی ممکن است شناخته و گشوده شوند. در این روشها تعداد الفباهای به کار رفته تعیین می‌شود و سپس الفباها به طور مجزا گشوده می‌شوند یا با استفاده از روابط بین الفباها رمز اصلی به رمزی تک‌الفبایی تبدیل می‌شود. ضعف لاینفک سیستمهای چندالفبایی در این واقعیت نهفته است که الفباهایی که برای به رمز درآوردن به کار می‌روند به تناوب تکرار می‌شوند.

برای رفع این ضعف، لازم می‌شود که از چندالفبا به طور غیر تکراری یا غیر تناوبی استفاده شود. بررسی رمزهای غیر تناوبی خارج از حوزهٔ این کتاب است.

تمرین

۵۱. در مسألهٔ پیامهای هم‌طول، در صفحهٔ ۱۰۶ ، وجود الفباهای مشترک بین دو پیام از آنجا معلوم شد که در مکانهای یکسانی از دو پیام حروف یکسانی آمده بود. فرض کنید هیچ حرف کلیدی تکراری وجود نداشته باشد. در این صورت چگونه می‌توان به وجود الفباهای مشترک بین دو پیام پی‌برد؟

۵۲. از دنبالهٔ صفحهٔ ۱۱۹ ، که به جای دنبالهٔ رمزی اصلی برای از رمز درآوردن پیام به کار رفت، دنبالهٔ رمزی اصلی مربع ویژنری را که برای به رمز درآوردن پیامهای یکسان صفحهٔ ۱۰۶ به کار رفته است، تعیین کنید. سپس دنبالهٔ صریح اصلی را تعیین کنید. این دنباله‌ها مبتنی بر چه کلمات کلیدیی هستند؟

رمزهای زیر رابگشایید:

۵۳.
```
UYSMS ZNZGC MBOVF YJVOK SBRNM ISFIA VVGKM QDFAZ YGFIG
KVRNR YSRTU RLZEL FIGWS EFYCX IFUSI DEGUY SCEZF KWWIZ
JCZSS ATFTN SYMRF CEEFS SSRTS VHEVA FUHYE ZFIWM EAURL
ZELFI GNYRU FASWG BBSCG BSISM XRESM DLRNR QRMAF J
```

۵۴.
```
IHLNO CJBZA ELTGX KGVOA RNRYR WSUTF USWII MDIAL KYMZI
SQIXK VLVRX ZGNMA LTZGN FBRXZ GNUAG EILVH YRGRE WIYLG
VAHPR VIREL XBIJK ALCAQ IIVVL RRJKA LWVWC RGKNB WECVB
LSHAI XTUVQ WZGLZ SHGKK LJBUX JHMMA LTZGN UAGPF HACAJ
LROLY OEIU
```

۵۵.
```
ICRGD JAVSQ ISXWJ SIRKD BVVIB QYEHW PIDBP ZUCIS YRRFX
KTUVT WRWIA BVENX ZERRM QSSGV FVJDT XMTUN ICABY MTDZN
QZGAI SDRUV KQKFD VDXJS XAVSM EINMS SDYBC LXFBA JNDQO
TISMV FMDIJ FMBCA ZQGSZ VDIKK EPMIQ GMAQM LJGCM FOREI
UOICR QGCDS GLRAE ELFHS QDDZL SBDNH QLRUG NVHYN D
```

۵۶.
```
FWPAY FEALS NVXLO ETAYS XIRHQ XSAHQ OIZES AYVHR GYZWR
AJNHR NCRYQ BYIHG DYHHC DIRHQ XSAHQ TJJEZ EGKMV LYRHA
HJVKY ZMXLA NJNHC DIHGS BEFVK XBPHH BYVHR AKPUB IWREA
EHMWQ NPNHC DCJMO DVEBU OVPSS BEMWQ NVRSA DADWK DDQTN
PYDSR NIFVK XBPTB MVPKO PPNQY DEYKQ ASQIV FWVAB XSDLO
AAAIS NSAFY FEALY DMPVD OWUMO AYNIS
```

۵۷. با فرض اینکه سیستمی که پیام زیر در آن به رمز درآمده سیستمی مبتنی بر مربع ویژنر باشد که دنبالهٔ رمزی آن معمولی و دنبالهٔ صریح آن دنبالهٔ درهم مبتنی بر کلمهٔ کلیدی (امانه انتقالی) با کلمهٔ کلیدی EARTHQUAKES باشد، پیام زیر را بگشایید:

```
IPKNE DUSOL SPZVP HAETP WPMYK FKYKP PKNZW SEEZI OLYQC
QETPL LPUBM CASPJ BCIBF FVPWE BLFSL HOGFL ABKAH MOWJS
QDBGV HQAVJ QYPBN VWBNP XLMLT PEXOL ADVLN DCOSE WSNSU
KMEWJ NAZKR VTVDA ZXNAZ JZTOO QFUPZ MXBFX MVQFY QICKT
BBDBW EKMFM VQNDW JDBLP QFTHE WFSRV WSWVP HAEPA VMUBW
WLGED XHEFW QUEPY MSLHH BFTNA DTWWA YQWLG WWZ
```

۵۸.

```
XTDVM IQEUP ZJJZZ OUACA QEUMZ XSEHD RUWXF VLOZK KZBUF
GCGZN LIWGI KKBDL GYMSS EUJHQ ZOUAC AQEGE UPDTV LOZKK
ZBUFL GAQSD AONGQ BDVZJ BLQNO ONDRQ NKTMZ PQKRT MKQHJ
XKNXZ BPEZH EWQLM VAHXK LIWKG KZYOZ XUMED VFJUH BZUBU
MXGJE FMWMH DKGVR WKXDV ASWXT DVMUM GJRFH ZESSD OPKQR
JXOGG PRJJF LKKWB VUMSX VAXBJ PFHPK VCGRP KDLPK QXTDV
AMWBK PONDR VXUOY TFWHK EVTVQ APBUU OVLFZ XDZBU FMUUO
EUMUX BWBRO W
```

۵۹.

```
CYLOF XNMNO VVNUN XNIDZ LUOPL XLCCU VXJVG ATRRH ZMSMZ
RRHZM DXDSB SVBFC ICHPO IEACR HAGIH ZLEML CMAZI FRBBN
OZBUF AQQLA TBVQD BHCCH LFVYS MZRRH ZMTGP ZKQOU HZIUW
HMSVK FNORA MQQDO CMNOV VNUZU NQDQI EQFZU RCIUD BNIHF
NJHEY ASGAJ ORQXT SXBZT KUDZL UODQZ ZOPRH FCYLV UBKIQ
YGLIB DXYEO QIEDX OIDHM ORAUU DKKSF RBUZS IVCEU NTONM
RCJIL SYRRA GILVG PKECY LVBYO LDEOC BYHAU ZHVNU VTYQP
ZBCZT KUWZX CZHDE QVYUZ FJUHC FBDHL XWCYC HPUUL LUBBH
JCLKC EKTKU WZXCW VJEAS XMHPQ RFAOC VYCEE CPZKK QXBZT
NDHLQ TMNTH TKUIC PNUXG BH
```

۶۰. در سیستمی که پیام زیر در آن به رمز درآمده، کلمهٔ کلیدی UNDERWATER برای دنبالهٔ صریح و کلمهٔ کلیدی HYDROGRAPHY برای دنبالهٔ رمزی به کار رفته است؛ هر دو دنباله دنباله‌های درهم انتقالی مبتنی بر کلمهٔ کلیدی‌اند.

```
AOWNJ ATLXP QMLKV YDDBD IDZBB AJXML OWYSO GJHML BLABT
JJGMB IWEXJ RDUPV NNXBH RVHPM UFLSD RVUAO STGHU QPTPB
IWFUP PBHPB IDMAN JQGGL PDWNO YWHKI MWMAN PXAUY FXXLI
AHGMV YMGOI YRXBQ RZWUQ RXHCI MWINB IWLPB ONZAP PLPUJ
LNQIV UZLUD UWXNN RAGSB UDQGQ JJGMO OLQOL PRDAP PDXBO
YZHSL BLABT JJHRP PLRZQ AJLMO ERGSP QOJLB APXAJ BGRXB
PTGII Y
```

۶۱. دو پیام رمزی زیر را که از یک محل و حدوداً در یک زمان به دو نشانی متفاوت ارسال شده‌اند بگشایید. (راهنمایی: اگر محتمل باشد که متن یک پیام با قسمتی از دیگری یکسان باشد، دو آزمون زیر را انجام دهید: یک‌بار دو پیام را از ابتدا حرف به حرف مقابل هم‌قرار دهید و آنها را یکی بگیرید، و یک بار از انتها).

پیام شمارهٔ۱:

ZSRDQ XHPCZ BYMHS KWHHD HRTQS JTRHH KVOUA JANOK TWOPD
JCGVL GEOGD UHTIF XUBVG ZSRVH ZVAAG ZEPAG XBPAF ZWASP
AXFVS TQOAZ BYLEO UXYUS JMOMG BGTPL JQOUS JCTOA REQSF
HKCTF IQOID HRDBZ PANUX JKRUD HXCTR GVJVW XEPAM JHLBR
KJPJF QTROL JQOUR UVQUQ RVLGM GCRAM ZSRVR MQAOF BOYHS
ZSRDB BNBBS JXLSA RKRHE JEOUP JQAMZ XHYEH UXHEW PWOID
HKFPB TKRAL YHRDA ZAEEH PQEUR JQCVH GTNLZ BVQL

پیام شمارهٔ ۲:

XFFST MZYDG YCOVU YXITY XUGCH OKTQV RCTKQ VEWIZ PVQTS
IZKDU DVOJA HWDAJ MUUYT DSXFZ UGAAD UWVQD OXCUQ QQCNT
HYPAA RKXCG FTQPF FOQNE OFFIR JNOGZ SKTBA HWDAZ CYIXK
DTKCT ZJFNE MCZOR FOXYZ DLSDH XCPPC TZCUV QNKFX CGFTI
OQVTP IOXDQ YWSMK QVEQM ESVTF GZEAW YGFNJ FFZJA YMAHV
QBFNX HWTZN DBWIO HTXH

۴

سیستمهای چندحرفی

۱.۴ رمزهای دوحرفی مبتنی بر تبدیلهای خطی یا ماتریسها

در فصول قبل مشاهده کردیم که رمزگشا با استفاده از شیوه‌های گوناگون و فراوانی هر حرف و ترکیبات حروف می‌تواند از عهدهٔ گشودن انواع مختلف رمزهای جایگذاری برآید. محتملاً این موضوع در مورد شیوه‌های پیچیده‌تر رمزنگاری نیز درصورتی که واحد رمزنگاری یک حرف باشد، صادق است. شاید چارهٔ رمزنگار برای ممانعت از موفقیت رمزگشا در استفاده از فراوانی حروف، این باشد که واحد رمزنگاری را به‌جای یک حرف، گروهی از حروف قرار دهد. هر سیستم رمزنگاری که در آن، واحد رمزنگاری به‌جای یک حرف یک گروه nحرفی صریح باشد که به‌جای آن یک گروه nحرفی رمزی گذاشته می‌شود، سیستم چندحرفی خوانده می‌شود.

در ساده‌ترین حالت، یعنی $n = ۲$، سیستم را دوحرفی می‌نامند. به‌جای هر زوج از حروف متن صریح یک دوحرفی رمزی می‌گذارند.

شیوه‌های گوناگون زیادی برای برقرار کردن روابط بین رمز و معادل صریح آن در سیستم دوحرفی وجود دارد. برای مثال می‌توان مربعی ۲۶×۲۶ با همهٔ دوحرفیهای ممکن ساخت، یعنی $۶۷۶ = ۲۶^۲$ دوحرفی را به تصادف در خانه‌های مربع قرار داد. حروف الفباهای معمولی در بالای مربع، از چپ به راست، و در سمت چپ مربع، از بالا به پایین، به‌عنوان اجزای دوحرفیهای صریح به‌کار می‌روند. معادل رمزی دوحرفی صریح $P_۱P_۲$

در خانه‌ای از مربع که در سطر P_1 و ستون P_2 واقع است یافت می‌شود. یک قسمت از چنان مربعی در همین صفحه نشان داده شده است؛ معادلهای رمزی دوحرفیهای AC، BE، CD عبارت‌اند از RA، AS، YE.

	A	B	C	D	E	F	.	.
A	QX	FN	RA	PD	CO	..	..	..
B	LU	TD	BN	EZ	AS	..	..	..
C	MG	OP	HJ	YE	LB	..	..	..

استفاده از این مربع برای از رمز درآوردن پیام دشوار است. اگر معکوس مربع فوق (جدولی که در آن دوحرفیهای صریحِ معادل دوحرفیهای رمزی فوق آمده باشند) فایده‌ای بیش از این مربع داشت، ساختن آن مطلوب بود.

دانشمند انگلیسی پلیفر[1] سیستمی دوحرفی ارائه کرده، که از نظر تاریخی تاحدی جالب است. در این سیستم، دنباله‌ای درهم از ۲۵ حرف الفبا (یک حرف، معمولاً J، حذف می‌شود) در یک مربع ۵ × ۵ نوشته می‌شود، شکل ۱۷ را مشاهده کنید.

قواعد به رمز درآوردن عبارت‌اند از:

۱. اگر P_1 و P_2 در این مربع دوگوشهٔ یک مستطیل باشند، آنگاه C_1 و C_2 دوگوشهٔ دیگر مستطیل‌اند و C_1 در همان سطری قرار دارد که P_1 قرار دارد. مثال: RE به‌صورت

D	B	M	W	I
C	O	X	G	E
Q	Y	R	F	S
Z	A	K	T	P
L	U	H	M	V

شکل۱۷

1. Playfair

SX به رمز درمی‌آید.

۲. اگر P_1 و P_2 در یک سطر باشند، C_1 و C_2 به‌ترتیب حروف مجاور سمت راست P_1 و P_2 هستند. (اوّلین ستون، سمت راست آخرین ستون در نظر گرفته می‌شود.) مثال: GE به‌صورت EC به رمز درمی‌آید.

۳. اگر P_1 و P_2 در یک ستون باشند، C_1 و C_2 درست در زیر P_1 و P_2، بدون فاصله با آنها، قرار دارند. (بالاترین سطر زیر پایینترین سطر در نظر گرفته می‌شود.) مثال: IS به‌صورت EP به رمز درمی‌آید.

۴. برای به رمز درآوردن یک دوحرفی با دو حرف یکسان قاعده وضع نمی‌کنیم؛ اگر با چنین دوحرفی مواجه شویم، به‌جای حرف دوم حرفی بی‌معنی (معمولاً X) قرار می‌دهیم تا مشکل برطرف شود.

قواعد از رمز درآوردن را به‌سادگی به‌صورت معکوس قواعد به رمز درآوردن می‌توان بیان کرد.

از لحاظ ریاضی، یک نوع بسیار جالب سیستم رمزنگاری، سیستمی است که نخستین بار لستر هیل[1] در مجلهٔ ریاضی مانتلی[2] (مارس ۱۹۳۱) ارائه کرد. در این فصل صورت ساده‌ای از سیستم هیل را ارائه می‌کنیم.

اساس کار در این سیستم، استفاده از تبدیل خطی با n متغیر است. برای ساده کردن بحث n را برابر ۲ انتخاب می‌کنیم تا سیستم ما دوحرفی باشد. (از مقادیر بزرگتر n بعداً بحث خواهیم کرد.)

از آنجا که شیوه‌های به‌کار رفته مبتنی بر اعداد هستند، از یک تناظر بین اعداد و حروف استفاده می‌کنیم تا این امکان را داشته باشیم که به‌جای هر حرف یک عدد بگذاریم. برای مثال، می‌توانیم به هر حرف عدد متناظر با مکان آن را در الفبای معمولی نسبت دهیم (صفحه ۷ را مشاهده کنید).

در این روشِ رمزنگاری، حروف متوالی متن صریح را دوتا دوتا اختیار کرده و آنها را (یعنی معادلهای عددی آنها، مثلاً P_1 و P_2، را) در یک زوج معادلهٔ همنهشتی (به پیمانهٔ

1. Lester. S. Hill 2. American Mathematical Monthly

۲۶) به‌صورت زیر قرار می‌دهیم:

$$\begin{aligned} C_1 &\equiv aP_1 + bP_2 \ (\text{پیمانهٔ } ۲۶) \\ C_2 &\equiv cP_1 + dP_2 \ (\text{پیمانهٔ } ۲۶) \end{aligned} \tag{۱.۴}$$

در نتیجه C_1C_2، یعنی معادل رمزی دوحرفی صریح معین می‌شود. این کار را دوحرف دوحرف ادامه می‌دهیم تا تمام پیام به رمز درآید. این روش را در زیر شرح می‌دهیم.

چهار عدد a، b، c، d که معادلات همنهشتی فوق با آنها شکل گرفته‌اند کلید ویژه را تشکیل می‌دهند. آنها را معمولاً در یک آرایهٔ مربعی، داخل پرانتز بزرگی می‌نویسند. چنین آرایه‌ای را ماتریس می‌نامند:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

برای شرح روش به رمز درآوردن، از مثالی استفاده می‌کنیم، مثلاً ماتریس به رمز درآوری زیر را انتخاب می‌کنیم:

$$\begin{pmatrix} ۷ & ۹ \\ ۳ & ۱۲ \end{pmatrix}$$

در این‌صورت همنهشتیها عبارت‌اند از:

$$C_1 \equiv ۷P_1 + ۹P_2 \ (\text{پیمانهٔ } ۲۶)\ ,$$
$$C_2 \equiv ۳P_1 + ۱۲P_2 \ (\text{پیمانهٔ } ۲۶)\ .$$

فرض کنید پیامی که باید به رمز درآید به‌قرار زیر باشد:

PREPARE TO EVACUATE AT ONCE

در این‌صورت اولین دوحرفی که باید به رمز درآید PR است،

$$P_1 = ۱۶, \qquad P_2 = ۱۸,$$

$$C_1 \equiv ۷(۱۶) + ۹(۱۸) \equiv ۲۷۴ \equiv ۱۴ = \text{N},$$
$$C_2 \equiv ۳(۱۶) + ۱۲(۱۸) \equiv ۲۶۴ \equiv ۴ = \text{D}.$$

دوّمین دوحرفی که باید به رمز درآید EP است،

$$P_۱ = ۵, \quad P_۲ = ۱۶,$$
$$C_۱ \equiv ۷(۵) + ۹(۱۶) \equiv ۱۷۹ \equiv ۲۳ = \mathrm{W},$$
$$C_۲ \equiv ۳(۵) + ۱۲(۱۶) \equiv ۲۰۷ \equiv ۲۵ = \mathrm{Y}.$$

با ادامهٔ این روش، به رمز درآورنده دوحرفیهای زیر را به دست می‌آورد:

pr ep ar et oe va cu at ea to nc e
ND WY MK GU TA GZ BA EI RA OF UZ

از آنجا که تعداد حروف پیام فرد است و در نتیجه یک حرفِ تنها در آخر باقی می‌ماند، به رمز درآورنده یک حرف ساختگی اضافه می‌کند تا دو حرفی آخر را بسازد. بنابراین اگر حرف X را انتخاب کند، دوحرفی رمزی آخر QQ خواهد بود. سرانجام برای ارسال پیام، آن را در دسته‌های پنج‌حرفی می‌نویسد:

NDWYM KGUTA GZBAE IRAOF UZQQ

روشن است که دوحرفی رمزی تابعی است از هر دو حرف دوحرفی صریح. اگر دو دوحرفی از متن صریح یک حرف مشترک داشته باشند، این موضوع به هیچ طریقی در معادلهای رمزی آنها قابل تشخیص نیست، همچنین اگر دو دوحرفی رمزی یک حرف مشترک داشته باشند، این موضوع هیچ چیزی را در مورد دوحرفیهای متن صریح آشکار نمی‌سازد. بنابراین فراوانیهای تک‌حرفی به‌کلّی پنهانند.

از آنجا که این روشِ به رمز درآوردن متضمن محاسبات بسیاری است، به رمز درآوردن پیامی طولانی ممکن است کار سنگینی باشد. به‌علاوه، باید دقت کرد که اشتباهی رخ ندهد. شخصی که چنین کاری را انجام می‌دهد، خیلی زود این سؤال برایش مطرح می‌شود که آیا می‌توان این فرایند را تسهیل کرد.

روشی را برای تسهیل کار شرح می‌دهیم. قدم اوّل تهیهٔ جدولی با دو ردیف برای $P_۱$ است که ردیف اوّلِ آن متناظر با ضریب $P_۱$ در عبارت $C_۱$ (یعنی همنهشتی مربوط به $C_۱$) باشد ـ این ضریب در مثال ما ۷ است. در زیرِ حروف الفبای معمولی، مضارب متوالی ۷ را که به پیمانهٔ ۲۶ تحویل شده‌اند می‌نویسیم. یک روش ساده برای انجام دادن این کار این است که هفت‌تا هفت‌تا بشماریم و هرجا که لازم بود مضارب ۲۶ را کم کنیم.

P_1:	A	B	C	D	E	F	G	H	I	J	K	L	M
aP_1:	7	14	21	2	9	16	23	4	11	18	25	6	13
cP_1:	3	6	9	12	15	18	21	24	1	4	7	10	13
P_1:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
aP_1:	20	1	8	15	22	3	10	17	24	5	12	19	26
cP_1:	16	19	22	25	2	5	8	11	14	17	20	23	26
P_2:	A	B	C	D	E	F	G	H	I	J	K	L	M
bP_2:	9	18	1	10	19	2	11	20	3	12	21	4	13
dP_2:	12	24	10	22	8	20	6	18	4	16	2	14	26
P_2:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
bP_2:	22	5	14	23	6	15	24	7	16	25	8	17	26
dP_2:	12	24	10	22	8	20	6	18	4	16	2	14	26

شکل۱۸

به‌عبارت دیگر فرایند شمارش عبارت است از ۷، ۱۴، ۲۱، ۲، ۹، و الی آخر (شکل ۱۸ را نگاه کنید)، که البته همان طرح چند در میان با فاصلهٔ ۷ است. به همین ترتیب دومین ردیف این جدول، طرح چند در میان با فاصلهٔ ۳ خواهد بود، که ۳ ضریب P_1 در عبارت C_2 (همنهشتی مربوط به C_2) است.

در جدول P_2 طرحهای چند در میانِ با فواصل ۹ و ۱۲ متناظر با ضریبهای P_2 در عبارات C_1 و C_2 می‌آید. توجه کنید که در مورد مضارب ۱۲ سیزده عدد زوج را، هرکدام دو مرتبه، به‌دست می‌آوریم.

برای به رمز درآوردن دوحرفیی چون P_1P_2 به‌وسیلهٔ این جدولها، C_1 را از جمع‌کردن اوّلین عدد زیر P_1 با اوّلین عدد زیر P_2 و تحویل این مجموع به پیمانهٔ ۲۶ (یعنی یافتن عدد همنهشت با آن در مجموعهٔ $\{1, \ldots, 26\}$) به‌دست می‌آوریم و C_2 را از جمع‌کردن دو عدد دوم زیر P_1 و P_2 و تحویل این مجموع به پیمانهٔ ۲۶ به‌دست می‌آوریم.

بنابراین، در به رمز درآوردن PR، داریم:

$$C_1 \equiv 8 + 6 \equiv 14 = \mathrm{N}$$

$$C_2 \equiv 22 + 8 \equiv 30 \equiv 4 = \mathrm{D}.$$

اگر این جدولها را در کاغذهای مجزا بنویسیم، چنانکه بتوان آنها را در مقابل یکدیگر لغزاند

تا $P_۲$ در زیر $P_۱$ قرار گیرد، کار جستجوی این اعداد تسهیل می‌شود.

طبعاً سیستم رمزنگاری باید متضمن راهی برای از رمز درآوردن باشد. این راه آن است که تبدیلی که وارون تبدیل رمزنگاری است در اختیار از رمز درآورنده قرار داده شود.*

در این مورد خاص، تبدیل از رمز درآوری تبدیلی است مبتنی بر ماتریس زیر:

$$\begin{pmatrix} ۱۸ & ۱۹ \\ ۱۵ & ۱۷ \end{pmatrix}.$$

برای استفاده از این تبدیل، از رمز درآورنده با پیام رمزی چنان رفتار می‌کند که گویی متن صریح است. نتیجه‌ای که او از محاسباتش به‌دست می‌آورد پیام اصلی است. توصیه می‌کنیم خواننده با از رمز درآوردن بعضی از دوحرفیهای رمزی، درستی تبدیل از رمز درآوری را بیازماید.

ماتریسهایی را که در این محاسبات با آنها سروکار داریم، ماتریسهای ۲×۲ می‌گوییم، زیرا دارای دو سطر و دو ستون‌اند. برای نشان دادن عناصر (یا درایه‌های) ماتریس، از دو اندیس استفاده می‌کنیم، اوّلی نشاندهندهٔ سطر، و دوّمی نشاندهندهٔ ستونی است که عنصر در آن قرار گرفته است. بنابراین درایه‌ای که در سطر iام و ستون jام آمده، به‌صورت m_{ij} نشان داده می‌شود. در حالت کلی ماتریس ۲×۲ را به‌صورت زیر نشان می‌دهند:

$$\begin{pmatrix} m_{۱۱} & m_{۱۲} \\ m_{۲۱} & m_{۲۲} \end{pmatrix}.$$

از آنجا که محاسبات ما به پیمانهٔ ۲۶ صورت می‌گیرد و به‌جای هر عددی عدد همنهشت با آن از مجموعهٔ $\{۱, ۲, \ldots, ۲۶\}$ را اختیار می‌کنیم، چهار عنصر ماتریس ما همیشه از مجموعهٔ $\{۱, ۲, \ldots, ۲۶\}$ هستند.

اگر دو ماتریس با هم تفاوت داشته باشند، نتیجهٔ عمل به رمز درآوردن با آنها یکسان نخواهد بود. بنابراین گوییم دو ماتریس برابرند اگر و فقط اگر تمام عناصر متناظر آنها برابر باشند. بنابراین

$$\begin{pmatrix} a_{۱۱} & a_{۱۲} \\ a_{۲۱} & a_{۲۲} \end{pmatrix} = \begin{pmatrix} b_{۱۱} & b_{۱۲} \\ b_{۲۱} & b_{۲۲} \end{pmatrix}$$

---

* نحوهٔ به‌دست آوردن ماتریسِ «از رمز درآوری» از ماتریس «به رمز درآوری» به‌زودی شرح داده خواهد شد.

اگر و فقط اگر $a_{۱۱} = b_{۱۱}$، $a_{۱۲} = b_{۱۲}$، $a_{۲۱} = b_{۲۱}$، $a_{۲۲} = b_{۲۲}$.

چگونه تبدیلِ از رمز درآوری از تبدیلِ به رمز درآوریِ مفروضی به‌دست می‌آید؟ این تبدیل اساساً از حل همنهشتیهای زیر و تعیین $P_۱$ و $P_۲$ برحسب $C_۱$ و $C_۲$ به‌دست می‌آید،

$$C_۱ \equiv ۷P_۱ + ۹P_۲$$

$$C_۲ \equiv ۳P_۱ + ۱۲P_۲$$

برای این منظور، اگر همنهشتی اوّل را در ۴، و همنهشتی دوم را در ۳ ضرب کنیم، ضرایب $P_۲$ در هر دو همنهشتی برابر می‌شود:

$$۴C_۱ \equiv ۲۸P_۱ + ۳۶P_۲$$

$$۳C_۲ \equiv ۹P_۱ + ۳۶P_۲ .$$

با کم کردن همنهشتی پایینی از بالایی، به‌دست می‌آوریم:

$$۴C_۱ - ۳C_۲ \equiv ۱۹P_۱ \equiv ۴C_۱ + ۲۳C_۲ .$$

حال برای اینکه $P_۱$ را از همنهشتی فوق به‌دست آوریم، باید طرفین این همنهشتی را بر ۱۹ تقسیم کنیم، یا در معکوس ۱۹ (به پیمانهٔ ۲۶) ضرب کنیم. چنین معکوسی موجود است، زیرا ۱۹ نسبت به ۲۶ اول است (صفحهٔ ۲۸ را ملاحظه کنید). این معکوس جواب همنهشتی زیر است:

$$۱۹x \equiv ۱ \text{ (پیمانهٔ ۲۶)}.$$

قبلاً دیده‌ایم (صفحهٔ ۲۸) که جواب این همنهشتی $x = ۱۱$ است. حال دو طرف همنهشتی زیر را

$$۱۹P_۱ \equiv ۴C_۱ + ۲۳C_۲$$

در ۱۱ ضرب کرده، به‌دست می‌آوریم:

$$۲۰۹P_۱ \equiv ۴۴C_۱ + ۲۳۵C_۲$$

که معادل است با:

$$P_۱ \equiv ۱۸C_۱ + ۱۹C_۲ .$$

در همنهشتی اصلی مربوط به $C_۱$، به‌جای $P_۱$ مقدار فوق را قرار می‌دهیم:

$$\begin{aligned} C_۱ &\equiv ۷P_۱ + ۹P_۲ \\ &\equiv ۷(۱۸C_۱ + ۱۹C_۲) + ۹P_۲ \\ &\equiv ۱۲۶C_۱ + ۱۳۳C_۲ + ۹P_۲, \\ ۹P_۲ &\equiv ۵C_۱ + ۲۳C_۲ \ . \end{aligned}$$

حال برای تقسیم طرفین این همنهشتی بر ۹، آن را در ۳ (یعنی معکوس ۹ به پیمانهٔ ۲۶) ضرب می‌کنیم که در نتیجه، همنهشتی زیر به‌دست می‌آید:

$$P_۲ \equiv ۱۵C_۱ + ۱۷C_۲ \ .$$

بنابراین تبدیل خطیِ از رمز درآوری عبارت است از:

$$\begin{aligned} P_۱ &\equiv ۱۸C_۱ + ۱۹C_۲ \\ P_۲ &\equiv ۱۵C_۱ + ۱۷C_۲, \end{aligned}$$

و ماتریس آن عبارت است از:

$$\begin{pmatrix} ۱۸ & ۱۹ \\ ۱۵ & ۱۷ \end{pmatrix}$$

همان‌طورکه قبلاً دیدیم، با استفاده از این تبدیل پیامی که به رمز درآمده بود از رمز درمی‌آید.

ماتریسی که به‌دست آوردیم، یعنی ماتریس

$$\begin{pmatrix} ۱۸ & ۱۹ \\ ۱۵ & ۱۷ \end{pmatrix}$$

وارون ماتریس زیر به پیمانهٔ ۲۶ خوانده می‌شود

$$\begin{pmatrix} ۷ & ۹ \\ ۳ & ۱۲ \end{pmatrix}$$

زیرا تبدیل متناظر با ماتریس اوّلی پیامی را که با ماتریس دومی به رمز درآمده از رمز درمی‌آورد.

در اینجا خواننده باید توجه کند که در محاسبهٔ ماتریس وارون، برای به‌دست آوردن $P_۱$ با لزوم تقسیم بر ۱۹ مواجه شدیم، و برای به‌دست آوردن $P_۲$ با لزوم تقسیم بر ۹؛ هر

دو تقسیم ممکن بود، زیرا ۱۹ و ۹ هر دو نسبت به ۲۶ اوّلند و در نتیجه به پیمانهٔ ۲۶ دارای معکوس‌اند. اما فرض کنید لزوم تقسیم بر عددی پیش می‌آمد که به پیمانهٔ ۲۶ دارای معکوس نیست، برای مثال، هر عدد زوج. در آن‌صورت حل معادلات نسبت به P_1 و P_2 مقدور نمی‌بود. در چنان موردی، فرایند به رمز درآوردن، فاقد فرایند متناظر از رمز درآوردن می‌بود، و تبدیل به رمز درآوری قابل‌قبول نمی‌بود. از اینجا نتیجه می‌گیریم که نمی‌توانیم ماتریس به رمز درآوری خود را به تصادف انتخاب کنیم. این ماتریس باید چنان انتخاب شود که دارای وارون باشد. در بخش بعد به تفصیل به این موضوع می‌پردازیم.

تمرین

۶۲. پیام زیر را با استفاده از ماتریس از رمز درآوری $\begin{pmatrix} ۱ & ۵ \\ ۷ & ۲ \end{pmatrix}$ از رمز درآورید.

YITJP GWJOW FAQTQ XCSMA ETSQU SQAPU SQGKC PQTYJ

۶۳. پیام زیر را با استفاده از ماتریس از رمز درآوری $\begin{pmatrix} ۲ & ۲۳ \\ ۲۱ & ۷ \end{pmatrix}$ از رمز درآورید.

MWALO LIAIW WTGBH JNTAK QZJKA ADAWS SKQKU AYARN CSODN IIAES OQKJY B

۲.۴ ضرب ماتریسها و وارون آنها

حال ببینیم که چگونه می‌توان از وجود وارون مطمئن شد. برای این هدف ابتدا به پرسش زیر می‌نگریم. اگر پس از تبدیلی، تبدیل دیگری انجام دهیم، چه نتیجه‌ای به‌دست می‌آید؟ این سؤال معادل آن است که بپرسیم اگر پیامی با یک ماتریس به رمز درآید و سپس پیام حاصل با ماتریس دیگری به رمز درآید، چه نتیجه‌ای به‌دست خواهد آمد؟

تعیین این نتیجه مشکل نیست. اگر ماتریس اوّل به‌صورت زیر باشد:

$$A = \begin{pmatrix} a_{۱۱} & a_{۱۲} \\ a_{۲۱} & a_{۲۲} \end{pmatrix},$$

به‌جای زوج P_1P_2 از حروف صریح، برطبق همنهشتیهای زیر زوج C_1C_2 از حروف رمزی قرار می‌گیرد:

$$\begin{aligned} C_1 &\equiv a_{11}P_1 + a_{12}P_2 \\ C_2 &\equiv a_{21}P_1 + a_{22}P_2. \end{aligned} \qquad (۲.۴)$$

اگر ماتریس دوّم به‌صورت زیر باشد:

$$B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$$

با به‌کار بردن آن برای متن رمزی حاصل‌شده در بالا، نتیجه می‌گیریم:

$$\begin{aligned} C_1' &\equiv b_{11}C_1 + b_{12}C_2 \\ C_2' &\equiv b_{21}C_1 + b_{22}C_2. \end{aligned}$$

عبارات (۲.۴) را به‌جای C_1 و C_2 قرار می‌دهیم و به‌دست می‌آوریم:

$$\begin{aligned} C_1' &\equiv b_{11}(a_{11}P_1 + a_{12}P_2) + b_{12}(a_{21}P_1 + a_{22}P_2) \\ C_2' &\equiv b_{21}(a_{11}P_1 + a_{12}P_2) + b_{22}(a_{21}P_1 + a_{22}P_2). \end{aligned}$$

با ضرب و دسته‌بندی جملات مشابه، به‌دست می‌آوریم:

$$\begin{aligned} C_1' &\equiv (b_{11}a_{11} + b_{12}a_{21})P_1 + (b_{11}a_{12} + b_{12}a_{22})P_2 \\ C_2' &\equiv (b_{21}a_{11} + b_{22}a_{21})P_1 + (b_{21}a_{12} + b_{22}a_{22})P_2 \ . \end{aligned}$$

بنابراین به‌جای این دو عملِ به رمز درآوردن متوالی می‌توان یک عمل به‌وسیلهٔ ماتریس زیر انجام داد:

$$\begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix} = BA$$

که آن را حاصلضرب $B.A$ از ماتریسهای A و B می‌نامند. با کمی دقت راه به‌دست آوردن این ماتریس از دو ماتریس اصلی معلوم می‌شود. جملهٔ سطر iام و ستون jام از حاصلضرب، نتیجه‌ای است که از حرکت در طول سطر iام ماتریس B و ستون jام ماتریس A و ضرب جملات متناظر و جمع حاصلضربها به‌دست می‌آید.

مثال:
ماتریس $\begin{pmatrix} ۱ & ۲ \\ ۳ & ۵ \end{pmatrix}$ را در $\begin{pmatrix} ۵ & ۶ \\ ۷ & ۳ \end{pmatrix}$ ضرب کنید.
پاسخ:

$$\begin{pmatrix} ۱ & ۲ \\ ۳ & ۵ \end{pmatrix}\begin{pmatrix} ۵ & ۶ \\ ۷ & ۳ \end{pmatrix} = \begin{pmatrix} ۱(۵)+۲(۷) & ۱(۶)+۲(۳) \\ ۳(۵)+۵(۷) & ۳(۶)+۵(۳) \end{pmatrix}$$

$$\equiv \begin{pmatrix} ۱۹ & ۱۲ \\ ۲۴ & ۷ \end{pmatrix}$$ (پیمانهٔ ۲۶).

در اینجا متذکر می‌شویم که ترتیب ضرب‌کردن مهم است. اگر در مثال خود ترتیب ماتریسها را معکوس کرده و $\begin{pmatrix} ۵ & ۶ \\ ۷ & ۳ \end{pmatrix}$ را در $\begin{pmatrix} ۱ & ۲ \\ ۳ & ۵ \end{pmatrix}$ ضرب کنیم، نتیجه $\begin{pmatrix} ۲۳ & ۱۴ \\ ۱۶ & ۳ \end{pmatrix}$ خواهد بود که کاملاً با نتیجهٔ ضرب قبلی متفاوت است. این نوعی از عمل ضرب است که به‌طور کلی در آن

$$A.B \neq B.A$$

این نوع ضرب، غیرجابجایی خوانده می‌شود.

حال از این تعبیر که ضرب دو ماتریس همچون دو تبدیل پی‌درپی است، استفاده می‌کنیم تا ببینیم یک تبدیل تحت چه شرایطی دارای وارون است.

اگر ماتریس B وارون ماتریس مفروض A باشد، آنگاه تبدیل تحت B اثر تبدیل تحت A را خنثی خواهد کرد؛ یعنی بعد از انجام‌دادن تبدیل A، و به‌دنبال آن تبدیل B، باید با حروف صریح اولیه مواجه شویم، به‌عبارت دیگر باید داشته باشیم:

$$C'_۱ \equiv P_۱$$

$$C'_۲ \equiv P_۲$$

اگر این معادلات را به‌شکل زیر بنویسیم:

$$C'_۱ \equiv P_۱ + ۰ \cdot P_۲$$

$$C'_۲ \equiv ۰ \cdot P_۱ + P_۲,$$

مشاهده می‌کنیم که ماتریس متناظر عبارت است از:

$$\begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} = I.$$

از آنجا که با این ماتریس، رمزی حاصل می‌شود که در آن به‌جای هر زوج $P_۱P_۲$ خود آن زوج قرار می‌گیرد ($P_۱ \equiv C'_۱$ ، $P_۲ \equiv C'_۲$)، این ماتریس، ماتریس همانی خوانده می‌شود و با I نمایش داده می‌شود؛ تبدیل تحت این ماتریس همواره تبدیل همانی است که در آن هر زوج، صرف‌نظر از آنکه پیمانه چه عددی است، با خودش جایگزین می‌شود.

نشان دادن این مطلب دشوار نیست که اگر $B.A = I$، آنگاه $A.B = I$؛ به‌عبارت دیگر، در ضرب هر ماتریس در وارون آن ترتیب عوامل ضرب مهم نیست.

تا اینجا نشان داده‌ایم که اگر حاصلضرب دو ماتریس A و B ماتریس همانی باشد، این دو ماتریس وارون یکدیگرند. نتیجهٔ این موضوع برای کار ما این است که یک تبدیلِ به رمز درآوری مانند:

$$C_۱ \equiv a_{۱۱}P_۱ + a_{۱۲}P_۲$$

$$C_۲ \equiv a_{۲۱}P_۱ + a_{۲۲}P_۲$$

دارای تبدیلِ از رمز درآوری متناظر است اگر ماتریس

$$A = \begin{pmatrix} a_{۱۱} & a_{۱۲} \\ a_{۲۱} & a_{۲۲} \end{pmatrix}$$

دارای وارون باشد. برای آنکه این قاعده را در مثالی نشان دهیم، ماتریسهایی را که برای به رمز درآوردن و از رمز درآوردن پیام صفحهٔ ۱۲۷ به‌کار برده‌ایم درهم ضرب می‌کنیم:

$$\begin{pmatrix} ۷ & ۹ \\ ۳ & ۱۲ \end{pmatrix} \cdot \begin{pmatrix} ۱۸ & ۱۹ \\ ۱۵ & ۱۷ \end{pmatrix} = \begin{pmatrix} ۱۲۶ + ۱۳۵ & ۱۳۳ + ۱۵۳ \\ ۵۴ + ۱۸۰ & ۵۷ + ۲۰۴ \end{pmatrix} = \begin{pmatrix} ۲۶۱ & ۲۸۶ \\ ۲۳۴ & ۲۶۱ \end{pmatrix}$$

$$\equiv \begin{pmatrix} ۱ & ۰ \\ ۰ & ۱ \end{pmatrix} \text{ (پیمانهٔ ۲۶)}.$$

از عمل ضرب فوق معلوم می‌شود که چگونه می‌توان نشان داد یک ماتریس وارون ماتریس دیگر است.

حال شیوه‌ای برای محاسبهٔ وارون ماتریسها ارائه می‌کنیم. این کار مستلزم استفاده از مفهومی است که به دترمینان مشهور است و به طریق زیر تعریف می‌شود: دترمینان ماتریس ۲ × ۲ی زیر

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix},$$

که با خطوط راست به‌جای خطوط خمیده، به‌صورت زیر نشان داده می‌شود

$$|M| = \begin{vmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{vmatrix},$$

عدد زیر است:

$$d = m_{11}m_{22} - m_{12}m_{21}\ .$$

توجه کنید که ممکن است ماتریسهای متفاوت، دترمینانهای مساوی داشته باشند.
مثال:

$$\begin{vmatrix} ۱ & ۲ \\ ۲ & ۶ \end{vmatrix} = (۱)(۶) - (۲)(۲) = ۲,$$

$$\begin{vmatrix} ۸ & ۳ \\ ۲ & ۱ \end{vmatrix} = (۸)(۱) - (۳)(۲) = ۲,$$

$$\begin{vmatrix} ۱۴ & ۳ \\ ۴ & ۱ \end{vmatrix} = (۱۴)(۱) - (۳)(۴) = ۲\ .$$

حال ثابت می‌کنیم که وارون M، که آن را با M^{-1} نمایش می‌دهیم مساوی است با

$$M^{-1} = \begin{pmatrix} \dfrac{m_{22}}{d} & \dfrac{-m_{12}}{d} \\ \dfrac{-m_{21}}{d} & \dfrac{m_{11}}{d} \end{pmatrix} \qquad (۳.۴)$$

البته، برای آنکه اعدادی مانند m_{ij}/d در حساب همنهشتی ما وجود داشته باشند، باید d عدد فرد غیرقابل‌قسمت بر ۱۳ باشد. بالعکس، اگر d در این شرط صدق کند، تمام عناصر M^{-1} را می‌توان محاسبه کرد.

برای اثبات کافی است M^{-1} را در M ضرب کرده و نشان دهیم که حاصل I است.

$$\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \cdot \begin{pmatrix} \frac{m_{22}}{d} & \frac{-m_{12}}{d} \\ \frac{-m_{21}}{d} & \frac{m_{11}}{d} \end{pmatrix}$$

$$= \begin{pmatrix} \frac{m_{11}m_{22} - m_{12}m_{21}}{d} & \frac{-m_{11}m_{12} + m_{11}m_{12}}{d} \\ \frac{m_{21}m_{22} - m_{21}m_{22}}{d} & \frac{m_{11}m_{22} - m_{12}m_{21}}{d} \end{pmatrix}.$$

از آنجا که $d = m_{11}m_{22} - m_{12}m_{21}$، حاصلضرب فوق برابر می‌شود با:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.$$

خواننده می‌تواند به‌راحتی نشان دهد که تساوی $M = I$. M^{-1} نیز برقرار است، تا در این مورد صحت حکم قبلی ما را که حاصلضرب یک ماتریس در وارونش با هر ترتیبی I است مشاهده کند.

محاسبهٔ فوق نشان می‌دهد که شرط لازم و کافی برای اینکه ماتریس 2×2 وارون داشته باشد آن است که دترمینانش عددی فرد و غیر قابل‌قسمت بر ۱۳ باشد. با استفاده از این امر، به‌راحتی می‌توانیم کلید به رمز درآوردن را انتخاب کنیم. اگر ماتریس انتخاب‌شده برای تبدیل، دترمینانی داشته باشد که در شرایطی که هم‌اکنون به‌دست آمد صدق کند ـ یعنی نسبت به ۲۶ اوّل باشد ـ آنگاه ماتریس از رمز درآوری وجود دارد و قابل محاسبه است.

مشروط بودن مقدار دترمینان از این واقعیت ناشی می‌شود که ۲۶ بر ۲ و ۱۳ قابل‌قسمت است. اگر برحسب اتفاق تعداد حروف الفبای ما عدد اوّلی چون p بود، آنگاه هر عدد صحیح غیر قابل‌قسمت بر p می‌توانست مقدار دترمینان باشد. این موضوع سبب پیدایش برخی از سیستمهای رمزنگاری شده است که در آنها از p حرف استفاده شده و p را عمداً عدد اول انتخاب کرده‌اند. برای مثال، اگر سه حرف را از الفبای خود حذف کنیم به این ترتیب که C را برای خودش و K به‌کار بریم، I را برای خودش و J، U را برای خودش و V، آنگاه تنها ۲۳ حرف خواهیم داشت، و هر ماتریس که دترمینانش (به پیمانهٔ ۲۳) صفر نباشد، وارون خواهد داشت. همچنین اگر الفبای خود را با افزودن سه علامت، مانند نقطه،

ویرگول و علامت سؤال، به ۲۹ حرف افزایش دهیم، نتیجه‌ای مانند نتیجهٔ قبل خواهیم داشت، یعنی هر ماتریس که دترمینانش مضربی از عدد اوّل ۲۹ نباشد دارای وارون خواهد بود. چنین تغییراتی خیلی مهم‌اند، اما بیش از این آنها را مورد بحث قرار نخواهیم داد.

یکی از خاصیتهای دترمینان که اثبات آن را به‌عنوان تمرین به خواننده واگذار می‌کنیم از قرار زیر است: اگر ماتریسهای M، N، P چنان باشند که $M.N = P$، آنگاه

$$|M|.|N| = |P|.$$

یعنی، دترمینان حاصلضرب ماتریسها مساوی حاصلضرب دترمینانهای آنهاست.

تمرین

۶۴. ماتریسهای زیر را (به پیمانهٔ ۲۶) ضرب کنید:

الف) $M = \begin{pmatrix} ۲ & ۵ \\ ۷ & ۸ \end{pmatrix}$ در $N = \begin{pmatrix} ۴ & ۱ \\ ۳ & ۲ \end{pmatrix}$ ؛

ب) $A = \begin{pmatrix} ۵ & ۲ \\ ۶ & ۷ \end{pmatrix}$ در خودش.

۶۵. دترمینان ماتریسهای زیر را محاسبه کنید:

الف) $\begin{pmatrix} ۱ & ۶ \\ ۳ & ۲۳ \end{pmatrix}$ ب) $\begin{pmatrix} ۲ & ۳ \\ ۳ & ۵ \end{pmatrix}$ ج) $\begin{pmatrix} ۲۰ & ۲ \\ ۵ & ۴ \end{pmatrix}$ د) $\begin{pmatrix} ۵ & ۴ \\ ۴ & ۵ \end{pmatrix}$

۶۶. وارون ماتریسهای زیر را (به پیمانهٔ ۲۶) تعیین کنید:

الف) $\begin{pmatrix} ۵ & ۲ \\ ۷ & ۳ \end{pmatrix}$ ب) $\begin{pmatrix} ۲ & ۳ \\ ۱ & ۲۲ \end{pmatrix}$ ج) $\begin{pmatrix} ۴ & ۱۱ \\ ۱ & ۲۲ \end{pmatrix}$

۶۷. الف) اگر دترمینان یک ماتریس ۹ باشد، دترمینان وارون آن(به پیمانهٔ ۲۶)چه خواهدبود؟

ب) اگر دترمینان یک ماتریس ۱۰ باشد، دترمینان وارون آن به پیمانه‌های زیر چه خواهد بود؟

(۱) پیمانهٔ ۲۶ (۲) پیمانهٔ ۲۳ (۳) پیمانهٔ ۲۹

۳.۴ تبدیل برگشتی

اگر در یک سیستم دوحرفیِ مبتنی بر تبدیل خطی، ماتریس به رمز درآوری چنان انتخاب شود که وارون خود باشد، آنگاه در به‌کار بردن آن سیستم از تسهیلاتی برخوردار خواهیم بود. این مطلب معادل آن است که بگوییم ماتریس M را که برای به رمز درآوردن پیام به‌کار رفته می‌توان برای از رمز درآوردن آن نیز به‌کار برد. اگر با M دو تبدیل پی‌درپی انجام شود، نتیجه تبدیل همانی است. با استفاده از ضرب ماتریسها می‌توان گفت:

$$M.M \equiv I \quad \text{یا} \quad M^{۲} \equiv I \text{؛} \quad \text{همچنین} \quad M \equiv M^{-۱}$$

دورهٔ تناوب هر ماتریس را کوچکترین توان مثبتی تعریف می‌کنند که اگر ماتریس به آن توان برسد، حاصل ماتریس همانی باشد (اگر چنین توانی وجود داشته باشد). اگر $M^{۲} = I$، اما $M \neq I$، دورهٔ تناوب M، ۲ خواهد بود. ماتریس با دورهٔ تناوب ۲، برگشتی خوانده می‌شود. از آنجا که دترمینان ماتریس همانی مساوی است با

$$|I| = \begin{vmatrix} ۱ & ۰ \\ ۰ & ۱ \end{vmatrix} = ۱(۱) - ۰(۰) = ۱ ,$$

دترمینان ماتریس برگشتی عددی است که مربع آن ۱ است. بنابراین با ۱ یا ۲۵ (به پیمانهٔ ۲۶) همنهشت است. این شرط لازم است، امّا کافی نیست، یعنی ممکن است ماتریسی دترمینان همنهشت با ۱ یا ۲۵ داشته باشد اما برگشتی نباشد.

مثال: ماتریس زیر

$$M = \begin{pmatrix} ۲ & ۳ \\ ۲۵ & ۲۴ \end{pmatrix}$$

یک ماتریس برگشتی است. دترمینان آن با ۲۵ همنهشت است و این ماتریس وارون خود است: $M^{۲} \equiv I$.

$N = \begin{pmatrix} ۱ & ۲ \\ ۲ & ۵ \end{pmatrix}$ دارای دترمینان ۱ است، اما مربع آن $\begin{pmatrix} ۵ & ۱۲ \\ ۱۲ & ۳ \end{pmatrix}$ است. بنابراین N برگشتی نیست.

تنها ۷ نمونه از ماتریسهای برگشتی با دترمینان ۱ وجود دارند، و این ماتریسها در رمزنگاری استفادهٔ محدودی دارند. به‌عنوان تمرین پیشنهاد می‌کنیم که خواننده این ماتریسها و جایگذاریهای دوحرفیی را که آنها معین می‌کنند به‌دست آورد. (راهنمایی: ابتدا نشان

دهید که اگر $d = 1$ و $M = M^{-1}$، آنگاه $m_{11} \equiv m_{22}$ و $2m_{12} \equiv 2m_{21} \equiv 0$.)

اگر دترمینان ماتریسی چون M با -1 همنهشت باشد (یعنی با ۲۵)، آنگاه M برگشتی است اگر و فقط اگر $m_{11} + m_{22} \equiv 0$ (یعنی همنهشت با ۲۶ باشد). اثبات به‌قرار زیر است:

فرض کنیم دترمینان ماتریس $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ همنهشت با -1 باشد، یعنی $d \equiv -1$؛ معکوس آن M^{-1} مساوی است با

$$\begin{pmatrix} \frac{m_{22}}{d} & \frac{-m_{12}}{d} \\ \frac{-m_{21}}{d} & \frac{m_{11}}{d} \end{pmatrix}$$

از آنجا که $d \equiv -1$، داریم:

$$M^{-1} \equiv \begin{pmatrix} -m_{22} & m_{12} \\ m_{21} & -m_{11} \end{pmatrix}.$$

بنابراین

$$M^{-1} \equiv \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} = M$$

اگر و فقط اگر $m_{11} \equiv -m_{22}$ و $m_{22} \equiv -m_{11}$، یعنی، اگر و فقط اگر

$$m_{11} + m_{22} \equiv 0$$

از آنجا که در چنین صورتی M معکوس خود است، برگشتی است.

ساختن ماتریسهای برگشتی با اطلاع از آنکه $d \equiv -1$ و $m_{11} + m_{22} \equiv 0$، نسبتاً ساده است.

مثال: فرض کنید $m_{11} = 2$. در این‌صورت $m_{22} = 24$، و

$$d \equiv 48 - m_{12}m_{21} \equiv 25,$$

لذا $m_{12}m_{21} \equiv 23$. بنابراین هر جفت عددی را که حاصلضرب آنها با ۲۳ همنهشت باشد، می‌توان به عنوان m_{12} و m_{21} اختیار کرد. این اعداد یا ۲۳ و ۱، یا ۷ و ۷، یا ۳ و ۲۵، یا ۱۵ و ۵، و الی آخر هستند.

تمرین

۶۸. دورهٔ تناوب ماتریسهای زیر را تعیین کنید، یعنی عددی چون n تعیین کنید، چنانکه $M^n \equiv I$ (پیمانهٔ ۲۶)،

الف) $\begin{pmatrix} ۳ & ۰ \\ ۰ & ۱ \end{pmatrix}$ ؛ ب) $\begin{pmatrix} ۳ & ۴ \\ ۴ & ۲۳ \end{pmatrix}$.

۶۹. مقدار a را چنان تعیین کنید که ماتریسهای زیر برگشتی باشند:

الف) $\begin{pmatrix} ۲ & ۷ \\ ۷ & a \end{pmatrix}$، ب) $\begin{pmatrix} ۳ & ۴ \\ a & ۲۳ \end{pmatrix}$، ج) $\begin{pmatrix} ۵ & a \\ ۱۰ & ۲۱ \end{pmatrix}$.

۷۰. فرض کنید یک تبدیل برگشتی دوحرفی صریح DE را به‌صورت CI به رمز درمی‌آورد. این تبدیل کلمهٔ DECIDE را به چه صورت به رمز درمی‌آورد؟

۴.۴ شناسایی رمزهای دوحرفی

حال خود را به‌جای رمزگشا قرار می‌دهیم و این مسأله را بررسی می‌کنیم که چگونه می‌توان به گشودن پیامی اقدام کرد که با تبدیلی خطی به‌صورت دوحرف دوحرف به رمز درآمده است. من‌باب مثال، می‌خواهیم پیام رمزی زیر را بگشاییم:

```
IXXZK YRVGP JTCMM GIYGE YQMXZ DANSG HERUQ JCZBQ
ZQXAP CQCSG RUIPB CDAXZ ANMIO DTFIB AJKLS GASMX
SYWGO UQUFF CPSGA YCMMC SXKMR INAXA FNESE FHTYS
IJGEQ AHEYN LQOQD CIQXZ QAXZE ZQCOD FACVY QGTES
YXYSZ SOZWA CKLAR SESBL YQLQX ALAZW UOGLJ YYYXZ
ANQPK PWNVU EMIVF OCKBC BMLED IAEHE ZSSGY QEMXZ
UJSRC BHUSG QWMKZ WCKZQ RFSOY QGLZI SLTOP PQAEJ
DNZQZ WGYGW UDHJT EWNDA VGBGZ QZWQJ JUPXB CDAMX
XZQAX ZANKQ KNTSZ QXAZQ ZBHEW HHTQA XZEUO HHESG
TOXAX VUBBR QPXVG WHEMQ OUWGS GQAAN TCVPM NQNUW
FMXKW HXJEF WHCMS GXZAN KQKNT SILRI UAUEC MMJTS
YRRRQ CTAXQ TOKY
```

اوّلین کار رمزگشا به‌دست آوردن اطلاعاتی دربارهٔ سیستم رمزنگاریی است که برای به رمز درآوردن به‌کار رفته است. این کار با یک جدول فراوانی سه‌حرفی و جستجو برای یافتن دنباله‌های تکراری حروف در رمز آغاز می‌شود.

از این توزیع فراوانی، که در اینجا آن را ارائه نمی‌کنیم، روشن می‌شود که پیام احتمالاً تک‌الفبایی نیست. توزیع تک‌حرفی نسبتاً هموار است، و شاخص انطباق آن ۰٫۰۴۱ است.

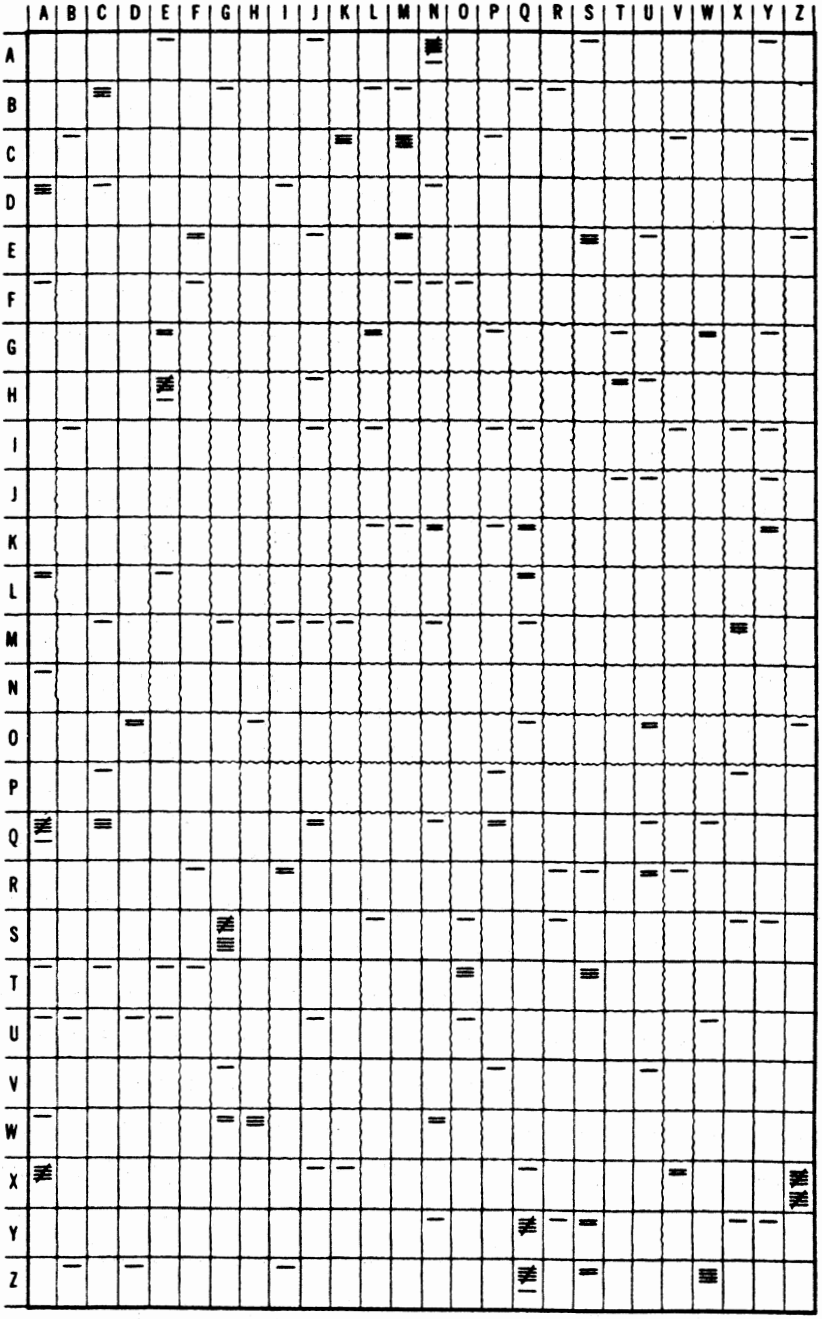
آیا احتمال دارد که پیام چندالفبایی باشد؟ دنباله‌های تکراری زیادی وجود دارند. تمام دنباله‌هایی را که حداقل چهار حرف دارند، به‌ترتیب اندازه‌شان، در زیر می‌آوریم:

دنباله‌های تکراری	مکان اولین حرف		فاصله	مقسوم‌علیه‌ها
XZANKQKNTS	325	417	92	2,2,23
XZQAXZ	139	321	182	2,7,13
ZQXA	41	335	294	2,3,7,7
BCDA	55	315	260	2,2,5,13
AXZE	142	350	208	2,2,2,2,13
XZAN	199	325	126	2,3,3,7
ZQZW	283	305	22	2,11
QAXZ	323	349	26	2,13

بسیار بعید به‌نظر می‌رسد که هم تکرار دنبالهٔ ده‌حرفی و هم تکرار دنبالهٔ شش‌حرفی تصادفی باشد. تنها مقسوم‌علیه مشترکی که فاصله‌های مربوط به آنها دارند ۲ است. از آنجا که ۲ مقسوم‌علیه مشترک تمام فواصل فوق است، امکان آن را که پیام ۲ الفبایی باشد بررسی می‌کنیم. شاخصهای انطباقی که به‌دست می‌آیند مساوی ۰٫۰۴۲ و ۰٫۰۴۵ هستند. این اعداد آن‌قدر کوچک‌اند که غیر قابل‌قبول‌اند.

از آنجا که پیام چندالفبایی نیست اما ۲ مقسوم‌علیه مشترک تمام فواصل تکرار است، قاعدتاً سؤال بعدی باید این باشد که آیا سیستم دوحرفی است. برای پاسخ دادن به این سؤال یک جدول فراوانی دوحرفی تشکیل می‌دهیم. پیام را به دوحرفیها تقسیم می‌کنیم و برای نشان دادن فراوانی آنها از نشانخط استفاده می‌کنیم. جدول حاصل در شکل ۱۹ نمایش داده شده است.

فرض کنیم این سیستمِ دوحرفی سیستمی است که در آن هر دوحرفی متن صریح، هرجا که ظاهر می‌شود، همواره با یک دوحرفی رمزی جایگزین بشود. آنگاه می‌توانیم فرض



شکل۱۹

کنیم این سیستم سیستمی تک‌الفبایی با الفبایی متشکل از ۶۷۶ = ۲۶ × ۲۶ علامت است. هریک از این علامتها (دوحرفیها) در زبان صریح دارای یک فراوانی مشخصه است. استدلالی که در فصل ۳ برای شاخص انطباق ارائه کردیم، در اینجا نیز قابل‌استفاده است. اگر حاصلجمع مربعات فراوانیهای مشخصهٔ این ۶۷۶ دوحرفی را محاسبه کنیم، عدد ۰٫۰۰۶۹ را به‌دست خواهیم آورد، که می‌توانیم آن را به‌عنوان شاخص ناهمواری سیستم (تک‌الفبایی) دوحرفی به‌کار بریم. برای یک توزیع کاملاً هموار دوحرفی، .M.R مساوی ۰٫۰۰۱۵ ≈ ۱/۶۷۶ است.

شاخص انطباق را بااستفاده از جدول فراوانی دوحرفیهای خود، طبق فرمول زیر محاسبه می‌کنیم:

$$\frac{\sum_{i=AA}^{i=ZZ} f_i(f_i - ۱)}{N(N-۱)},$$

که N تعداد دوحرفیهاست، یعنی نصف طول پیام، و f_iها فراوانی دوحرفیهای رمزی هستند. با انجام دادن محاسبات، ۰٫۰۰۸۴ را به‌دست می‌آوریم. بنابراین می‌توانیم محقق بدانیم که سیستم مورد بحث دوحرفی است و دوحرفیهای رمزی تکراری، هرجا که آمده باشند، همواره یک معادل صریح دارند. هرچند هنوز شاهدی دال بر اینکه سیستم چه نوع سیستم دوحرفی است نداریم.

۵.۴ گشودن تبدیل خطی

تعداد انواع متفاوت سیستمهای دوحرفی زیاد است. سیستم مبتنی بر تبدیل خطی که بررسی کرده‌ایم تنها یکی از این سیستمهاست. اگر دلیلی برای این حدس که در سیستم رمزنگاری از تبدیل خطی استفاده شده داشته باشیم، می‌توانیم این حدس را مدنظر قرار دهیم و آزمونهای خاص متناسب با آن را انجام دهیم. از این قرار، اگر بتوانیم معادل صریح دو یا تعداد بیشتری از دوحرفیهای رمزی را شناسایی کنیم، خواهیم توانست معادله‌هایی همنهشتی که مجهولات آنها عناصر ماتریس هستند تشکیل دهیم. از شناسایی معادل صریح دو دوحرفی رمزی چهار معادلهٔ همنهشتی به‌دست می‌آید که ممکن است برای تعیین هر چهار مجهول کافی باشد. اگر در جواب این همنهشتیها با ابهاماتی مواجه شویم، می‌توانیم برای تعیین جوابهای صحیح آنها را جداگانه در سایر قسمتهای متن امتحان کنیم. اگر بتوانیم بیش از دو دوحرفی

را شناسایی کنیم، احتمالاً معادله‌های همنهشتی اضافیِ حاصل موجب رفع شبهه در تعیین جوابهای یگانه می‌شوند. با این جوابها پیام از رمز درمی‌آید و متن صریح به‌دست می‌آید. البته، فرض بر این است که تناظر بین حروف و اعداد را که رمزنگار به‌کار برده می‌دانیم.

برای اقدام به گشودن سیستمهای دوحرفی از شیوه‌هایی مشابه شیوه‌هایی که درگشودن تک‌الفبایی‌ها به‌کار می‌روند می‌توان استفاده کرد. این شیوه‌ها اساساً عبارت‌اند از استفاده از اطلاعات مربوط به فراوانی و الگوهای تکرار برای یافتن بعضی از معادلهای صریح. این معادلها را باید در متن قرار داد، تا شاید ایده‌ای دربارهٔ نوع سیستم به‌دست آید. یک راه برای تعیین چنین معادلهای صریحی استفاده از روش کلمهٔ احتمالی است. اگر رمزگشا دلیلی در دست داشته باشد حاکی از وجود کلمات یا عبارات ویژه‌ای در پیام، می‌تواند برای دریافتن جای ممکن این کلمات یا عبارات در متن رمزی تلاش کند. مکانهای ممکن را می‌توان به‌وسیلهٔ فراوانی نسبی دوحرفیهای مربوطه و با اطلاعاتی که از الگوها به‌دست می‌آیند ـ اگر الگویی موجود باشد ـ بررسی کرد. برای مثال، اگر دلیلی وجود داشته باشد که ما را متقاعد کند که عبارت UNITED STATES در پیامی آمده است، از دوحرفی تکرارشدهٔ TE می‌توان برای آزمودن مکانهایی که ممکن است این عبارت در آنها آمده باشد استفاده کرد. به‌شرط آنکه مکان U زوج باشد. اگر مکان Uفرد باشد، راهی برای آزمودن مکانهای ممکن وجود نخواهد داشت.

اگر احتمال دهیم که بخشی از متن رمزی معادل با کلمه یا عبارت صریح خاصّی است، آنگاه معادلهای حاصل برای دوحرفیهای رمزی مربوطه را می‌توان هرجا که آن دوحرفیها آمده‌اند قرار داد. ممکن است این کار، در وضعیتهای خاصّی، باعث حدس قسمتهای دیگری از متن شود.

بدون‌شک خواننده فهمیده است که برای اینکه بتوان با استفاده از فراوانیها و الگوها متنی را در سیستمهای دوحرفی معین کرد، طول متن باید زیاد باشد، زیادتر از آنچه برای گشودن تک‌الفبایی‌ها موردنیاز است. به‌این دلیل است که پیامی که در حال بررسی آن هستیم، از پیامهایی که تا اینجا بررسی کرده‌ایم بسیار طولانیتر است.

در انگلیسی فراوانی TH بیش از سایر دوحرفیهاست. اگر پیام نسبتاً طویل باشد، این دوحرفی را غالباً می‌توان شناسایی کرد. پس از TH، دوحرفی HE بیشترین فراوانی را دارد، و فراوانی آن چندان کمتر از TH نیست، بعد از آن IN و ER قرار دارند، که فراوانی آنها تقریباً دوسوم فراوانی TH است. سپس دوحرفیهای زیادی قرار دارند که می‌توان فراوانی آنها را نسبتاً

زیاد دانست. در بین دوحرفیهای با فراوانی کم چند دوحرفی هستند که تقریباً هیچ‌گاه ظاهر نمی‌شوند. برای مثال، در متن معمولی انگلیسی هیچ‌گاه پس از Q حرفی غیر از U نمی‌آید.

در پیام ما دوحرفیی که بیشترین فراوانی را دارد XZ است. فرض می‌کنیم که این دوحرفی رمزی دوحرفی صریح TH باشد. این فرض با وجود دنبالهٔ تکراری XZQAXZ، یعنی الگویی که TH در آن زیاد ظاهر می‌شود، بسیار موجه می‌شود. بنابراین اگر XZQA یک کلمه باشد (و معقول است چنین باشد زیرا پیش از دنبالهٔ تکراری طولانی XZANKQKNTS می‌آید)، رمز XZQAXZ ممکن است THAT THE یا THAN THE یا THEN THE باشد. اگر XZQA یک کلمهٔ کامل نباشد آنگاه ممکن است XZQAXZ عبارتی مانند OTHER THAN یا RATHER THEN باشد. در هرصورت، تطابق دوحرفی رمزی XZ با دوحرفی صریح TH بسیار محتمل به‌نظر می‌رسد.

با تشخیص TH می‌توان از اطلاعات مربوط به فراوانی، استفاده‌های بیشتری کرد. قبلاً فراوانی بسیار زیاد THE را متذکر شده‌ایم (صفحهٔ ۵۴). از ۲۱۶۱ مورد ظهور TH، در ۱۷۱۷ مورد به‌دنبال TH حرف E آمده است. یعنی به‌طور متوسط، از هر پنج مورد، تقریباً در چهار مورد به‌دنبال آن E آمده است. اگر فرض کنیم که در هر مورد ظهور TH در مسألهٔ دوحرفی ما E به‌دنبال آن آمده، آنگاه گرچه ممکن است در بعضی موارد چنین فرضی درست نباشد، اما در اکثر موارد درست است. این فرض چه فایده‌ای دارد؟

تمام دوحرفیهایی راکه پس از دوحرفیهای رمزی XZ آمده‌اند می‌نویسیم. این دوحرفیها عبارت‌اند از:

KY, AN, QA, EZ, UJ, EU

تنها شش دوحرفی متفاوت وجود دارند، زیرا XZAN و XZQA چندبار تکرار شده‌اند (اولی چهاربار و دومی دوبار).

از این دوحرفیها چه استفاده‌ای می‌توان کرد؟ فرض کنیم که سیستم مبتنی بر تبدیل خطی باشد. در این‌صورت، می‌توانیم برای هریک از این دوحرفیهای رمزی یک همنهشتی بنویسیم که مبین آن باشد که اوّلین حرف از دوحرفی صریحی که این همنهشتی نشاندهندهٔ آن است، E است. بنابراین شش همنهشتی با تنها دو مجهول، به‌صورت زیر، خواهیم داشت:

$$b_{11}C_1 + b_{12}C_2 \equiv 5,$$

که b_{11} و b_{12} مجهول هستند. احتمال می‌دهیم که بیشتر این همنهشتیها صادق باشند.

اگر بتوانیم ثابت کنیم که سه همنهشتی، یا تعداد بیشتری از آنها، سازگارند، یعنی همه دارای یک جواب مشترک برای دو مجهول b_{11} و b_{12} هستند، آنگاه شاهدی داریم دال بر اینکه سیستم، مبتنی بر تبدیل خطی است.

برای اثبات چنین امری، دوتا از همنهشتیها را حل می‌کنیم و جوابها را در همنهشتیهای دیگر امتحان می‌کنیم تا ببینیم که آیا در همنهشتی دیگری نیز صدق می‌کنند یا نه. البته، دو معادله‌ای که حل می‌کنیم باید هر دو مربوط به دوحرفیهایی باشند که حرف اوّلِ آنها واقعاً معادل حرف صریح E است. بنابراین برای انتخاب دو همنهشتی مناسب، شاید لازم باشد بیش از یک زوج از همنهشتیها را بیازماییم، زیرا بعضی از دوحرفیها ممکن است معادل صریحی داشته باشند که حرف اوّلش E نیست.

یک راه مشابه، اما سریعتر، استفاده از این نکته است که عضو سمت راست هر یک از این همنهشتیها عدد یکسانی، معادل E، است. بنابراین تفریق یک همنهشتی از دیگری به یک همنهشتی همگن منجر خواهد شد، یعنی به یک همنهشتی به‌صورت $qb_{11}+rb_{12}\equiv ۰$.

حال معادلهای عددی حروف این شش دوحرفی را بررسی می‌کنیم:

$$\begin{aligned}
\mathbf{KY} &\rightarrow \mathbf{11, 25}\\
\mathbf{AN} &\rightarrow \mathbf{1, 14}\\
\mathbf{QA} &\rightarrow \mathbf{17, 1}\\
\mathbf{EZ} &\rightarrow \mathbf{5, 26}\\
\mathbf{UJ} &\rightarrow \mathbf{21, 10}\\
\mathbf{EU} &\rightarrow \mathbf{5, 21}
\end{aligned}$$

متوجه خاصیت جالبی می‌شویم. اگر دوحرفیهای AN، KY، UJ، EU را، به‌همین ترتیب، انتخاب کنیم، درمی‌یابیم که فاصلهٔ بین معادلهای عددی اعضای اول آنها، یعنی فاصلهٔ بین اعداد ۱، ۱۱، ۲۱، ۵، (به پیمانهٔ ۲۶)، ۱۰ است، و فاصلهٔ بین اعضای دوّم ۱۱ است. این نشان می‌دهد که همنهشتیهای این چهار دوحرفی سازگارند، زیرا اگر آنها را به‌صورت زیر بنویسیم:

$$\begin{aligned}
۱b_{11}+۱۴b_{12} &\equiv ۵\\
۱۱b_{11}+۲۵b_{12} &\equiv ۵\\
۲۱b_{11}+۱۰b_{12} &\equiv ۵\\
۵b_{11}+۲۱b_{12} &\equiv ۵,
\end{aligned}$$

و آنگاه هریک از این همنهشتیها را از همنهشتی زیر آن تفریق کنیم، به‌دست می‌آوریم: $۱۰b_{۱۱} + ۱۱b_{۱۲} \equiv ۰$. در نتیجه هر زوج از این همنهشتیها دارای جواب یکسانی برای $b_{۱۱}$ و $b_{۱۲}$ هستند. از آنجا که AN چهار مرتبه ظاهر می‌شود، از ده موردی که دوحرفی صریح TH ظاهر می‌شود، در هفت مورد به‌دنبال آن E می‌آید.

اگر دوتا از این همنهشتیها را حل کنیم، به‌دست می‌آوریم:

$$b_{۱۱} = ۳, \qquad b_{۱۲} = ۲,$$

و این مقادیر در دو همنهشتی دیگر هم صدق می‌کنند.

این مقادیر در همنهشتیهایی که بافرض E بودن حرف اول معادلهای QA و EZ تشکیل شده‌اند صدق نمی‌کنند. یعنی معادلهای صریح QA و EZ با حرفی غیر از E شروع می‌شوند. خوب است به گشودن رمز حرف اول آنها اقدام کنیم تا ببینیم چه‌چیزی به‌دست می‌آید. می‌توانیم این کار را به‌وسیلهٔ مقادیر $b_{۱۱}$ و $b_{۱۲}$ که اکنون شناخته شده‌اند انجام دهیم:

از QA به‌دست می‌آید: $۱۷(۳) + ۱(۲) \equiv ۵۳ \equiv ۱ \to \mathrm{A}$

از EZ به‌دست می‌آید: $۵(۳) + ۲۶(۲) \equiv ۱۵ \to \mathrm{O}$

هر دو حرف فوق سه‌حرفیهای خوبی با TH می‌سازند. به‌ویژه A_p این احتمال را که دنبالهٔ تکراری XZQAXZ نمایشدهندهٔ THAT THE یا THAN THE باشد تأیید می‌کند.

معادل دیگری هم داریم که هنوز از آن استفاده نکرده‌ایم. می‌دانیم که $\mathrm{XZ} \to \mathrm{TH}$. با جایگذاری ۳ به‌جای $b_{۱۱}$ و ۲ به‌جای $b_{۱۲}$، مقدار زیر را به‌دست می‌آوریم:

$$۲۴(۳) + ۲۶(۲) \equiv ۲۰$$

که معادل عددی T است. نتیجهٔ خوبی است، زیرا با نتیجهٔ قبلی مبنی بر اینکه TH معادل XZ است سازگار است.

حال می‌توانیم حرف دوّم این معادل را برای به‌دست آوردن اطّلاعاتی دربارهٔ عناصر باقیماندهٔ ماتریسِ از رمزدرآوری خود، یعنی $b_{۲۱}$ و $b_{۲۲}$، به‌کار بریم. در $C_۱b_{۲۱} + C_۲b_{۲۲} \equiv P_۲$ جایگذاری کرده و به‌دست می‌آوریم:

$$۲۴b_{۲۱} + ۲۶b_{۲۲} \equiv ۸$$

که معادل است با

$$۲۴b_{۲۱} \equiv ۸,$$

و دارای دو جواب است:

$$b_{۲۱} = ۹ \qquad \text{یا} \qquad b_{۲۱} = ۲۲ \ .$$

این اطّلاعات هم‌اکنون به‌کار نمی‌آیند، اما در آینده به‌کار خواهند آمد.

دو عنصر شناخته‌شدهٔ $b_{۱۱}$ و $b_{۱۲}$ از ماتریس از رمز درآوری، اولین همنهشتی از دو همنهشتی از رمز درآوری را تعیین می‌کنند. در نتیجه می‌توانیم برای هرکدام از دوحرفیهای رمزی حرف اول از معادل صریح آن را به‌دست آوریم. بنابراین می‌توانیم تمام حروف متن صریح اصلی را که در مکانهای با شمارهٔ فرد قرار دارند تعیین کنیم. نتیجهٔ از رمز درآوردن این حروف در مورد ده دسته حرف نخست پیام در زیر نشان داده شده است:

```
IXXZK YRVGP JTCMM GIYGE YQMXZ DANSG HERUQ JCZBQ ZQXAP CQCSG
w the ta ria ye ei h es hrs in hvb es
```

شاید برای خواننده جالب باشد که بداند تا چه‌اندازه می‌توان جاهای خالی متنی را که حروف فرد آن شناخته شده‌اند پرکرد. اگر خواننده من‌باب تمرین، این کار را برای پیام فوق انجام دهد، بدون‌شک درخواهد یافت که این کار به‌سادگی آنچه در وهلهٔ اوّل به‌نظر می‌رسد نیست.

اما ما مجبور نیستیم این‌کار را انجام دهیم. فقط کافی است معادل چند دوحرفی دیگر را تعیین کنیم. در این‌صورت قادر خواهیم بود دو مجهول $b_{۲۱}$ و $b_{۲۲}$ از ماتریس تبدیل را پیدا کنیم. بدین منظور، در پیام به‌دنبال محلی می‌گردیم که شاید بتوان کلمه یا عبارتی را در آنجا حدس زد. به‌نظر می‌رسد که دسته‌های ۹ و ۱۰ برای این منظور مناسب باشند:

```
ZQXAP CQCSG
h.v.b .e.s.
```

متن شبیه HAVE·BEEN به‌نظر می‌رسد.

از نمودار فراوانی خود مشاهده می‌کنیم دوحرفی ZQ، که به‌نظر می‌رسد معادل صریح آن HA باشد، شش‌بار در پیام ظاهر شده است، که دوبار آن در دنبالهٔ تکراری ZQXA است. وقتی در دسته‌های ۶۷ و ۶۸ دنبال ZQXA می‌گردیم الگوی زیر را پیدا می‌کنیم:

```
ZQXAZQZB
```

معادلهای ممکنِ ZQ و XA را می‌دانیم، و می‌توانیم حرف اول معادل ZB را نیز به‌دست

آوریم. نتیجه HAVE HAD خواهد بود. این نتیجه را می‌توان آزمون خوبی در تأیید نتایج قبلی دانست. بنابراین می‌توانیم کلمات HAVE BEEN را پذیرفته و بنویسیم:

$$\begin{aligned} \mathbf{ZQ} &\rightarrow \mathbf{HA} \\ \mathbf{XA} &\rightarrow \mathbf{VE} \\ \mathbf{PC} &\rightarrow \mathbf{BE} \\ \mathbf{QC} &\rightarrow \mathbf{EN} \end{aligned}$$

حال با این معادلها می‌توانیم دو مجهول $b_{۲۱}$ و $b_{۲۲}$ را در تبدیل از رمز درآوری خود تعیین کنیم، یعنی دو مجهولی را که متناظر با همنهشتی دوّم هستند.

از $\mathrm{ZQ} \rightarrow \mathrm{HA}$ به‌دست می‌آوریم:

$$\begin{aligned} ۲۶b_{۲۱} + ۱۷b_{۲۲} &\equiv ۱ \\ ۱۷b_{۲۲} &\equiv ۱ \\ b_{۲۲} &\equiv ۲۳ . \end{aligned}$$

برای به‌دست آوردن مقدار $b_{۲۱}$ ساده‌تر خواهد بود که از همنهشتی حاصل از $\mathrm{QC} \rightarrow \mathrm{EN}$ استفاده کنیم، یعنی

$$۱۷b_{۲۱} + ۳b_{۲۲} \equiv ۱۴,$$

زیرا ضریب مقدار مجهول $b_{۲۱}$ نسبت به ۲۶ اول است و در نتیجه این همنهشتی فقط یک جواب دارد:

$$\begin{aligned} ۱۷b_{۲۱} + ۳(۲۳) &\equiv ۱۴ \\ ۱۷b_{۲۱} &\equiv ۲۳ \\ b_{۲۱} &= ۹ . \end{aligned}$$

مقادیری که قبلاً برای $b_{۲۱}$ با استفاده از $\mathrm{XZ} \rightarrow \mathrm{TH}$ به‌دست آمد (صفحهٔ ۱۵۰) مؤید این مقدار $b_{۲۱}$ است.

بنابراین ماتریس از رمز درآوری کاملاً معین است:

$$\begin{pmatrix} ۳ & ۲ \\ ۹ & ۲۳ \end{pmatrix}$$

و می‌توان تمام پیام را از رمز درآورد. متن به این ترتیب آغاز می‌شود:

WITH EXTRAORDINARY FEVERISHNESS.

[با بی‌قراری فوق‌العاده]

تمرین

۷۱. وقتی احتمال می‌دهیم که کلمه یا عبارت مشخصی در متن باشد، درصورتی که این کلمه یا عبارت الگوی قابل تشخیصی داشته باشد، می‌توانیم از آن برای زخنه کردن در پیام استفاده کنیم. پیام زیر راکه شامل اسم GEORGE PAPANDREOU است بگشایید:

```
CMYPZ GTAYO EQBYQ JLAOW INELN NECNN UESZT YTFRU OWYXH
KYADM NJRUK CUFZP YPNNM XWSQQ OJMGO JZQZQ FLVAY XGIPR
OPUFJ WTSVA ATQU
```

۷۲. شواهدی در دست است که پیام زیر محتملاً به‌استفادهٔ وزارت دفاع از کامپیوتر در ترفیع کارمندان مربوط است. این پیام را بگشایید.

```
TWQZK XKBSD TWPOE QIAPS XMTSF HQNKB NOIAH NEPOW FYKGQ
ZVGKK OVKBG WYDYI IRYOH GNUHN UVAHY DRYQE KWDNB QBZHN
DAOVK BGWYD OOIIQ ANUYI IRYOH GTTLG GHQED NNKYD OZNUF
JOWYV TWARV YARFW NGSMY IAUCQ QEYII KARQN SSXEI NCCOM
SDJHN GIJDK YGCRT QEQUE ZGJUH EAQWK UFLBL QDVGE UVHNO
WLEWA YRHNU VAHYD RYQEK WDNBQ BZSBV GHRTQ NEKMF AXMZG
GUZOK XVKFK PJLGN QKOSA MPIAH EWPMW UYIGI KSBLO LZOWF
YKGQZ WV
```

۷۳. پیام زیر را بگشایید:

```
BPCNT QZVNS CWVWZ GBPRI IBYLA CULBP DEZSB PECLE UKGXQ
AGPCW FKIZX GOZCZ KWUUN TRWBP MBGHD IKGPH BEPDQ AGPPM
SUZPX WDSIU GQYTG MKJDS JOKOG MKGGX UHPMK MXAPH LSBIG
RQFOQ IZYLB QSUAG TMNYT GTUJO YSLSA YBUYL VVUUT GBPAT
IZYXC ZKWUU NTXJF QBPHY TQNVR IOPKK EIAGP MSUZP ALZSK
APIQK NNULB PBWGM GCONM BAOAG WBNMZ MONBP DEXGB PNSWB
ACYLJ ZQAKM ESNIZ PBPXG MSZPY LBQUL BPTQB QYLGM RVDEK
MRJQM KTBQB PRIAS TEULM WKWRG CDPMS UZPUH IBQDX GYQOQ
ULNMZ MGZGR MWKWW BBPAT CHYXQ QNNNG DEYLF JSNXG LBBAN
PPOEH XOONB QTXKV BIIUL OWFFM ONDBO ECRUU SUKMO NYNOV
```

۶.۴ چگونه می‌توان ایمنی سیستم هیل را بیشتر کرد

حال فرض کنید که رمزنگار از چگونگی گشوده‌شدن پیامی که با سیستم تبدیل خطی به رمز درآمده است آگاه شده باشد، و بخواهد با اصلاح نقایصی که رمزگشا با استفاده از آنها به گشودن پیام اقدام کرده، ایمنی سیستم را بیشتر کند.

تقریباً واضح است که او ابتدا توجه خود را معطوف به این امر خواهد کرد که تناظر حروف و اعداد برای رمزگشا قابل تشخیص بوده است و با استفاده از آن تناظر رمزگشا توانسته است معادلاتی را تشکیل دهد و عناصر ماتریس تبدیل را از آنها به دست آورد. بنابراین بهتر است رمزنگار آن تناظر را درکلید ویژه قرار دهد، یعنی قسمتی از کلید ویژه مشخص کنندهٔ این تناظر باشد.

برای مثال، یک کلمهٔ کلیدی مورد توافق را می‌توان برای ساختن دنباله‌ای درهم به‌کار برد. سپس حروف آن دنباله را از ۱ تا ۲۶ شماره‌گذاری کرد. به این ترتیب تناظر نامعلوم درهم ریخته‌ای از حروف و اعداد فراهم می‌شود. حال، حتی اگر رمزگشا از اینکه سیستم مبتنی بر تبدیل خطی است آگاه باشد، به تعیین ۳۰ مقدار ناشناخته نیاز دارد ـ چهار عنصر ماتریس و ۲۶ معادل عددی حروف الفبا. برای به دست‌آوردن این مقادیر به تشخیص صحیح تعداد زیادی از دوحرفیهای رمزی نیاز خواهد داشت، بنابراین بدون شک به متن بسیار طویلی احتیاج خواهد داشت.

برای ایمنی بیشتر می‌توانیم پس از اینکه اعداد متناظر با حروف صریح را با تناظری بین حروف و اعداد معین کردیم و اثر تبدیل به رمز درآوری را بر این اعداد به دست آوردیم، از تناظر دیگری برای قراردادن حروف رمزی به جای این اعدادِ به‌دست آمده، استفاده کنیم. با این کار بیست و شش مجهول به مجهولات قبلیِ رمزگشا اضافه می‌شود.

با این تغییرات به‌نظر می‌رسد که سیستم رمزنگاری جالبی به‌دست آید. اما هنوز این نکته به‌جای خود باقی است که درصورت طولانی بودن متن اطلاعاتی از فراوانی دوحرفیها و الگوها قابل استنتاج است. برای رفع این قابلیت، می‌توان به‌جای سیستم دوحرفی از سیستم سه‌حرفی استفاده کرد. یعنی، می‌توان از سه همنهشتی با سه مجهول استفاده کرد:

$$C_1 \equiv a_{11}P_1 + a_{12}P_2 + a_{13}P_3$$

$$C_2 \equiv a_{21}P_1 + a_{22}P_2 + a_{23}P_3$$

$$C_3 \equiv a_{31}P_1 + a_{32}P_2 + a_{33}P_3$$

با انتخاب ماتریسی که دارای وارون باشد، در این سیستم رمزنگاری، متن صریح سه‌حرف سه‌حرف به رمز درمی‌آید.

البته نیازی نیست که به واحد سه بسنده شود. سیستم می‌تواند چهارحرفی یا پنج‌حرفی باشد و هرچه این واحد بزرگتر باشد، ایمنی سیستم بیشتر است.

محدودیتها، محدودیتهای عملی هستند، به‌این معنی که با افزایش اندازهٔ ماتریسهای تبدیل مقدار محاسبات لازم به مقدار بسیار زیادی افزایش می‌یابد. به‌علاوه، احتمال اشتباه بسیار بیشتر می‌گردد، و از آنجا که اشتباه در یک حرف بر تمام حروف گروهی که با آن حرف به رمز درمی‌آیند تأثیر می‌گذارد، استفاده از یک واحد بزرگ احتمال این خطر را افزایش می‌دهد که تعداد کمی اشتباه در به رمز درآوردن یا در ارسال پیام سبب غلط‌شدن قسمت بزرگی از متن شود. در چنان مواردی ممکن است گیرنده نتواند پیامی را که دریافت کرده است بخواند. این نکته نکتهٔ مهمی در عدم‌استفاده از ماتریسهای بزرگ است.

۵

انتقال

۱.۵ انتقال ستونی

نوعی روش رمزنگاری که در اساس کاملاً با رمزهای جایگذاری، که تا به حال شرح داده‌ایم، متفاوت است، انتقال نام دارد. در چنین سیستمی هویت حروف پیام تغییر نمی‌کند، بلکه ترتیب مکانهای آنها تغییر می‌کند.

در اینجا چند مثال ساده از انتقالهایی را که برای به رمز درآوردن متن زیر به کار رفته‌اند می‌آوریم:

I CAME I SAW I CONQUERED

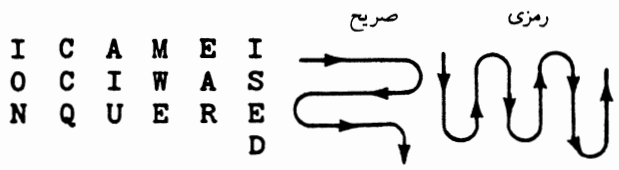
الف. متن را می‌توان وارونه نوشت:

DEREU QNOCI WASIE MACI

ب. رمزنگاری دو سطری. حروف متن یک درمیان در دو سطرِ جداگانه نوشته شده و آنگاه سطر به سطر خوانده می‌شود:

I A E S W C N U R D
C M I A I O Q E E

رمزی: **IAESW CNURD CMIAI OQEE**



شکل ۲۰

ج. در سیستمی که در اینجا مد نظر است، شکلی هندسی انتخاب می‌شود و پیام بر طبق مسیر یا جهتی در آن نوشته می‌شود، و سپس پیام بر طبق مسیر دیگری بازنویسی می‌شود، چنانکه به عنوان مثال در (شکل ۲۰) آمده است.

رمزی : **IONQC CAIUE WMEAR DESI**

بر اثر این نوع رمزنگاری ترتیب حروف پیام اصلی عوض می‌شود. این اثر را می‌توان به طریق ریاضی به وسیلهٔ مفهومی که جایگشت خوانده می‌شود نشان داد. برای روشن شدن مطلب، مثال وارونه‌نویسی الف را در پاراگراف قبل در نظر بگیرید. پیام دارای ۱۹ حرف است. آنها را با اعدادی که نشاندهندهٔ مکان آنها در پیام صریح هستند معین می‌کنیم، در این صورت پیام صریح از اعداد ۱ تا ۱۹ تشکیل می‌شود. با به کاربردن روش رمزنگاری مذکور برای متن صریح، پیام رمزی زیر تولید خواهد شد:

19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1

متن رمزی را در زیر متن صریح می‌نویسیم:

صریح	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
رمزی	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

در این شکل، جایگشت مکانی را که هر حرف در پیام اصلی اشغال می‌کند (در سطر بالایی) و مکان نهایی آن را در پیام رمزی (در سطر پایینی) نشان می‌دهد.

جایگشت نوعی قاعده است که تحت آن عناصر یک مجموعه به طریقی یک به یک با اعضای همان مجموعه جایگزین می‌شوند. به بیان دقیقتر: جایگشت تابعی یا نگاشتی یک به یک از یک مجموعه به روی خودش است. جایگشت مثال الف را می‌توان با تابع زیر نشان داد:

$$f : k \to ۲۰ - k, \qquad k = ۱, ۲, \ldots, ۱۹ .$$

با استفاده از فرایندی زنجیره‌ای مشابه با آنچه دربازسازی دنبالهٔ ویژنر به کار رفت (صفحهٔ ۱۱۴) می‌توان جایگشت را با یک سطر، به جای دو سطر فوق، نشان داد. با عدد ۱ شروع کرده، به دنبال آن عدد زیرین آن در سطر رمزی، یعنی ۱۹ را می‌آوریم. آنگاه، از آنجا که در زیر عدد ۱۹ از سطر صریح، عدد ۱ قرار دارد، به دنبال ۱۹ عدد ۱ را می‌آوریم. به این ترتیب یک چرخه حاصل می‌شود. بنابراین زوج اعداد (۱۹ ,۱) را در پرانتز می‌نویسیم تا نشان دهیم که ۱ به ۱۹ و ۱۹ به ۱ می‌رود. سپس زنجیره‌ای را با عدد ۲ آغاز می‌کنیم و (۱۸ ,۲) را به دست می‌آوریم. اگر به این طریق ادامه دهیم، درخواهیم یافت که جایگشت کامل، مرکب از چرخه‌هایی است که هرکدام از دو عدد تشکیل شده‌اند، به استثنای ۱۰ که با خودش جایگزین شده و چرخه‌ای از تنها یک عدد تشکیل می‌دهد:

(1,19) (2,18) (3,17) (4,16) (5,15) (6,14) (7,13) (8,12) (9,11) (10)

قرار می‌گذاریم که اعدادی مانند ۱۰ فوق را، که به تنهایی یک چرخه تشکیل می‌دهند، ننویسیم.

اگر کاری را که در بالا گفته شد برای رمز دوسطری (مثال ب) انجام دهیم، پیام رمزی زیر را به دست می‌آوریم:

M: 1 3 5 7 9 11 13 15 17 19 2 4 6 8 10 12 14 16 18

اگر این دنباله را در زیر دنبالهٔ صریح بنویسیم، خواهیم داشت:

```
1 2 3 4 5  6  7  8  9 10 11 12 13 14 15 16 17 18 19
1 3 5 7 9 11 13 15 17 19  2  4  6  8 10 12 14 16 18
```

حال با استفاده از فرایند زنجیره‌ای چرخه‌ای با ۱۸ عدد حاصل می‌شود:

N: (2, 3, 5, 9, 17, 14, 8, 15, 10, 19, 18, 16, 12, 4, 7, 13, 6, 11)

در اکثر رمزهای انتقالی، جایگشت حاصل متشکل از چند چرخه است که هیچ رابطهٔ مشخصی بین طولهای آنها (یعنی تعداد اعداد آنها) وجود ندارد. تعداد کل حروف نمایش داده شده در این چرخه‌ها از تعداد کل حروف پیام کمتر است، و تفاضل آنها به اندازهٔ تعداد حروفی است که مکانشان تغییر نمی‌یابد، یعنی حروفی که در چرخه‌های متشکل از تنها یک عدد قرار دارند.

فایدهٔ استفاده از مفهوم جایگشت برای انتقال عمدتاً از جنبهٔ نظری است. این موضوع را خواننده به طریق زیر به سهولت می‌تواند دریابد: دو پیام با طول متفاوت انتخاب کند و با یک سیستم انتقالی آنها را به رمز درآورد، ظاهر جایگشتهای حاصل معمولاً به‌کلی با یکدیگر متفاوت است. این به آن مفهوم است که جایگشتی که نتیجهٔ یک انتقال را نشان می‌دهد، نه تنها تابعی از نحوهٔ انتقال است، بلکه تابعی از طول پیام نیز هست. در نتیجه روش استفاده از جایگشت برای به رمز درآوردن و از رمز درآوردن پیامهایی به طولهای متفاوت، در واقع روش مفیدی نیست.

پرسشی که به کمک نماد جایگشت به سهولت می‌توان به آن پاسخ داد عبارت است از اینکه اگر یک فرایند انتقال را در مورد پیامی به دفعات به کار بریم، چه نتیجه‌ای حاصل می‌شود. برای بررسی این مطلب، شیوهٔ رمزنگاری دوسطری را به عنوان مثال در نظر گرفته وآن را دو بار به کار می‌بریم. بنابراین، پیام M در **صفحهٔ قبل** را با استفاده از انتقال به شیوهٔ دو سطری مجدداً به رمز درمی‌آوریم:

```
1  5  9   13   17   2  6  10   14   18
   3  7  11   15   19  4  8   12   16
```

رمز حاصل را در زیر پیام اصلی می‌نویسیم:

```
1 2 3  4  5  6 7  8  9  10 11 12 13 14 15 16 17 18 19
1 5 9 13 17 2 6 10 14 18  3  7 11 15 19  4  8 12 16
```

جایگشتی که با این انتقال متن اصلی متناظر است عبارت است از

$$(2,5,17,8,10,18,12,7,6)(3,9,14,15,19,16,4,13,11).$$

در مقایسهٔ آن با جایگشت حاصل از یک‌بار به کاربردن شیوهٔ رمزنگاری دوسطری (N **در صفحهٔ قبل**)، مشاهده می‌کنیم که جایگشتی که پس از مرحلهٔ دوم داریم طرح چند درمیان نتیجهٔ اوّل با فاصلهٔ ۲ است. به طور کلی، می‌توان نشان داد که از n بار به کار بردن انتقال، طرح چند درمیان جایگشت اصلی با فاصلهٔ n حاصل می‌شود.

حال این نتیجه به ما امکان می‌دهد که به سؤال زیر پاسخ دهیم: چند بار باید یک انتقال را به کار برد تا رمز با متن صریح اصلی یکی شود؟ یک چرخهٔ تنها از جایگشت اصلی را، مثلاً به طول x، در نظر بگیرید. طرح چند درمیانِ چنین چرخه‌ای تنها در صورتی متشکل از چرخه‌های تک حرفی خواهد بود که فاصلهٔ طرح مضربی از x باشد. به عبارت دیگر، اگر انتقال

به تعداد دفعاتی که مضربی از x است تکرار شود، تمام حروف آن چرخه به مکانهای اصلی خود برمی‌گردند. از آنجاکه چنین حکمی برای هر چرخه صادق است، تعداد دفعاتی که باید یک انتقال به‌کار رود تا پیام صریح اصلی حاصل شود، کوچکترین مضرب مشترک طول چرخه‌هایی است که انتقال شامل آنهاست. به عنوان یک مثال ساده، اگر شیوهٔ وارونه‌نویسی (مثال الف) دوبار به کار رود متن صریح حاصل خواهد شد، زیرا تمام چرخه‌های آن به طول ۲ هستند.

فرض کنید جایگشتی که نشاندهندهٔ نتیجهٔ فرایند انتقال است شامل چرخه‌های زیر باشد:

(1,14,9) (10,15,2,6) (5,16,3,11,4) (12,7,18,13,8,17).

در این صورت تعداد دفعاتی که لازم است این فرایند به کار رود تا رمز مزبور به متن صریح تبدیل شود، کوچکترین مضرب مشترک ۳، ۴، ۵ و ۶ است که ۶۰ است.

فرایندهای رایج انتقال فرایندهایی‌اند که در آنها پیام صریح به طور معمولی در مستطیلی که تعداد ستونهایش از قبل معین شده نوشته می‌شود و سپس به طور عمودی و ستونی بازنویسی می‌شود تا متن رمزی حاصل شود (این مستطیل را مستطیل انتقال می‌نامیم). قبلاً یک نوع از این شیوه را در انتقال ستونی دنباله‌های درهم مبتنی برکلمهٔ کلیدی دیده‌ایم (صفحهٔ ۴۳). در آنجا فرایند بازنویسی عبارت بود از نوشتن حروف ستونها به‌ترتیب از چپ به راست. ولی اگر حروف ستونها را به ترتیبی نامنظم بنویسند، سیستم به طرق متعددی قابل ساختن بوده و ایمنی آن بیشتر خواهد بود.

چنین سیستمی، سیستم انتقال ستونی خوانده می‌شود. کلید این سیستم دنباله‌ای است از اعدادی که از قبل معین شده و هم عرض مستطیل انتقال را تعیین می‌کند و هم ترتیب بازنویسی ستونها را.

برای کمک در به خاطر سپردن دنبالهٔ عددی، معمولاً قرار می‌گذارند که این دنباله ازکلمهٔ کلیدی قراردادی به طریق زیر ساخته شود: به حروف کلمهٔ کلیدی اعدادی را نسبت دهند که نشاندهندهٔ ترتیب الفبایی آنها نسبت به هم باشد. شیوهٔ انجام دادن این کار در مثال زیر شرح داده شده است: فرض کنید کلمهٔ کلیدی، SORCERY [سحر و جادو]باشد. آنگاه از آنجا که از نظر الفبایی C اوّلین حرف در این کلمه است، با ۱ شمارگذاری می‌شود. E با ۲ و O با ۳ شماره‌گذاری می‌شود. دو R از چپ به راست با ۴ و ۵ شماره‌گذاری شده و پس از آن S و Y به ترتیب با ۶ و ۷ شماره‌گذاری می‌شود. کلید عددی حاصل عبارت است از:

S O R C E R Y
6 3 4 1 2 5 7

می‌خواهیم پیام زیر را به رمز درآوریم:

LASER BEAMS CAN BE MODULATED TO CARRY MORE INTELLIGENCE THAN RADIO WAVES

[اشعهٔ لیزر را می‌توان چنان مدوله کرد که نسبت به امواج رادیویی اطّلاعات بیشتری را حمل کنند.]

پیام را در زیرِ دنبالهٔ عددی، به عرض ۷، می‌نویسیم:

S O R C E R Y
6 3 4 1 2 5 7

L A S E R B E
A M S C A N B
E M O D U L A
T E D T O C A
R R Y M O R E
I N T E L L I
G E N C E T H
A N R A D I O
W A V E S

از آنجا که طول پیام مضربی از ۷ نیست، در این طریقِ نوشتن سطر آخر مستطیل پر نمی‌شود. همان‌طور که به زودی خواهیم دید، اگر سطر آخر شامل خانه‌های خالی نباشد فرایند از رمز درآوردن ساده‌تر خواهد شد. بنابراین برای سیستم کلی مورد بحث قرار می‌گذاریم که مستطیل همیشه کاملاً پر باشد. اگر طول متن پیام صریح چنان نباشد که سطر آخر را پر کند، باید حروف بی‌معنی اضافه کرد تا این شرط محقق شود. از آنجا که دو جای خالی در سطر آخر وجود دارد، شکل را با افزودن دو حرف ساختگی، مثلاً Q و R، کامل می‌کنیم.

S O R C E R Y
6 3 4 1 2 5 7

L A S E R B E
A M S C A N B
E M O D U L A
T E D T O C A
R R Y M O R E
I N T E L L I
G E N C E T H
A N R A D I O
W A V E S Q R

حال فرایند به رمز درآوردن متشکل است از نوشتن متن فوق به طور ستونی به ترتیب ستونهای شماره‌گذاری شده. در ضمن می‌توان آن را در دسته‌های پنج حرفی یادداشت کرد.

ECDTM ECAER AUOOL EDSAM MERNE NASSO DYTNR VBNLC RLTIQ LAETR IGAWE BAAEI HOR

از رمز درآورنده به طریق زیر اقدام خواهد کرد: تعداد حروف پیام را می‌شمارد (۶۳). از آنجا که طول کلید ۷ است، ابعاد مستطیل انتقال ۹ × ۷ است. سطرها و ستونهای چنین مستطیلی را با رسم خطوطی مشخص می‌کند و کلید را در بالای آن قرار می‌دهد. سپس پیام رمزی را مطابق با ترتیب اعداد کلید در آن وارد می‌کند؛ ۹ حرف نخست پیام در ستون زیر ۱ قرار داده می‌شوند، سپس نه حرف بعدی در ستون زیر ۲، نه حرف بعدی در ستون زیر ۳، الی آخر.

6	3	4	1	2	5	7
	A		E	R		
	M		C	A		
	M		D	U		
	E		T	O		
	R		M	O		
	N		E	L		
	E		C	E		
	N		A	D		
	A		E	S		

وقتی تمام پیام در مستطیل قرار داده شود، متن صریح به طور معمولی در سطرهای مستطیل ظاهر خواهد شد.

تمرین

۷۴. پیام زیر را با کلید مبتنی بر کلمهٔ ROYALTY از رمز درآورید:

```
TNGTH CYIIL XHEIH PANCA AXHGR OUFOA EMITE LSOIP INDSR
ROEAR ERANX EEEFT ILMSE AEANS CESON EX
```

۷۵. پیام زیر را با کلید مبتنی بر کلمهٔ CREAMPUFF از رمز درآورید:

```
HDUCP IEATL EIEUU OENOI XMMCI TATDF DSSHC HSSVS ISTAO
TRNGO HRSSG OHASF EMBLH FPEEO EE
```

۲.۵ گشودن رمزهای انتقالی دارای مستطیل کاملاً پر

حال گشودن یک رمز انتقالی را بررسی می‌کنیم که در آن از مستطیلی کاملاً پر استفاده شده است. من باب مثال رمز زیر را در نظر می‌گیریم:

```
EOEYE GTRNP SECEH HETYH SNGND DDDET OCRAE RAEMH
TECSE USIAR WKDRI RNYAR ANUEY ICNTT CEIET US
```

البته مشکلی برای تشخیص آنکه در این رمز، از انتقال استفاده شده، نه از جایگذاری، وجود ندارد. توزیع تک حرفی چنین رمزی بدون هیچ انتقالی با توزیع معمولی مطابقت می‌کند؛ به عبارت دیگر این توزیع، توزیع معمولی است. این نشان می‌دهد که هویّتهای حروف اصلی تغییر نکرده‌اند، بنابراین باید ترتیب مکانهای آنها تغییر کرده باشد.

بدین ترتیب معلوم می‌شود که رمز فوق رمزی انتقالی است. فرض می‌کنیم که در آن از انتقال ستونی با مستطیلی کاملاً پراستفاده شده است. (بعداً در این فصل مشاهده خواهیم کرد که چگونه می‌توان رمز انتقالی را بدون فرض آنکه مستطیل کاملاً پر است گشود.)

عرض مستطیل کاملاً پر باید مقسوم‌علیهی از طول پیام باشد؛ از آنجا که پیام دارای ۷۷ حرف است، مستطیل باید به عرض ۷ یا ۱۱ حرف باشد. (برای پیامهایی با طولهای

دیگر، ممکن است تعداد عرضهای ممکنی که باید در نظر گرفته شوند از این بیشتر باشد. زیرا ممکن است طول پیام مقسوم‌علیه‌های بیشتری داشته باشد. در آن صورت کار بیشتری باید انجام داد، اما در راه حل کلی تفاوتی وجود ندارد.) پیام رمزی را به صورت عمودی در داخل مستطیلهایی با عرضهای ممکن می‌نویسیم؛ دو نتیجهٔ حاصله در زیر نشان داده شده‌اند:

1	2	3	4	5	6	7	8	9	10	11
E	R	H	N	E	R	C	R	N	E	C
O	N	H	G	T	A	S	W	Y	Y	E
E	P	E	N	O	E	E	K	A	I	I
Y	S	T	D	C	M	U	D	R	C	E
E	E	Y	D	R	H	S	R	A	N	T
G	C	H	D	A	T	I	I	N	T	U
T	E	S	D	E	E	A	R	U	T	S

1	2	3	4	5	6	7
E	E	G	A	E	R	C
O	C	N	E	U	N	N
E	E	D	R	S	Y	T
Y	H	D	A	I	A	T
E	H	D	E	A	R	C
G	E	D	M	R	A	E
T	T	E	H	W	N	I
R	Y	T	T	K	U	E
N	H	O	E	D	E	T
P	S	C	C	R	Y	U
S	N	R	S	I	I	S

اگر فرض پر بودن مستطیل درست باشد، آنگاه برای گشودن رمز ستونها را به قسمی جابه‌جا می‌کنیم که متن صریح حاصل شود (در این کار تمام حروف یک‌ستون را یکجا حرکت می‌دهیم). فرایند مرتب کردن مجدد مجموعهٔ نامرتبی از حروف به ترتیب اصلیشان مقلوب‌سازی نامیده می‌شود. کار ما مقلوب‌سازی این ستونها برای تشکیل متن صریح است.

از آنجا که سطر اوّل حروف نشاندهندهٔ آغاز پیام است، می‌توانیم کار را با اقدام به بازسازی کلمهٔ اوّل آغاز کنیم. بابررسی مستطیل به عرض ۱۱، متوجه می‌شویم که ۱۱ حرف نخست تنها شامل ۳ حرف صدا دارند، که توزیع نامحتملی از حروف صدادار و بی‌صداست. سطر چهارم نیز دارای تنها ۳ حرف صدادار است. بنابراین محتمل به نظر نمی‌رسد که مستطیل صحیح، مستطیلی به عرض یازده ستون باشد.

حال توجه خود را معطوف به عرض ۷ می‌کنیم. کلمهٔ اوّل چه کلمه‌ای ممکن است باشد؟ شاید مقلوب‌سازی حروف سطر اوّل تاحدی مشکل باشد. در این صورت قدم بعدی باید تلاش برای جفت‌کردن دو ستون به منظور به دست آوردن دوحرفیهای مناسب باشد. (برای این کار، مفید است که ستونها را در نوارهای کاغذی مجزا بنویسیم تا جابه‌جا کردن

آنها آسان باشد.) متوجه می‌شویم که اگر ستون ۲ بعد از ستون ۷ واقع شود دو حرفیهای مناسب بسیاری حاصل می‌شود، به ویژه اینکه دوبار TH ظاهر می‌شود.

7	2
C	E
N	C
T	E
T	H
C	H
E	E
I	T
E	Y
T	H
U	S
S	N

سطر هفتم مستطیل هفت ستونی نشان می‌دهد که می‌توان Hای را پس از Tی ستون دوم قرار داد. این H در ستون ۴ قرار دارد. اگر ستون ۴ را در کنار ستون ۲ قرار دهیم، ترکیبات بسیار خوبی حاصل می‌شود، به ویژه کلمهٔ THE و سه‌حرفی THA. تنها ترکیب غیرممکن SNS در سطر آخر است. آیا به این دلیل باید از ترکیباتی که به دست آورده‌ایم، صرف نظر کنیم؟ آنچه دردست داریم بسیار خوب به‌نظر می‌رسد. امکان دارد که حروف SNS در خط آخر حروفی بی‌معنی باشند (که برای پرکردن مستطیل اضافه شده‌اند).

1	3	5	6
E	G	E	R
O	N	U	N
E	D	S	Y
Y	D	I	A
E	D	A	R
G	D	R	A
T	E	W	N
R	T	K	U
N	O	D	E
P	C	R	Y
S	R	I	I

7	2	4
C	E	A
N	C	E
T	E	R
T	H	A
C	H	E
E	E	M
I	T	H
E	Y	T
T	H	E
U	S	C
S	N	S

سه حرفی THA کلمهٔ THAT را تداعی می‌کند، اما در سطر ۴ حرف T موجود نیست، در سطر ۵ هم حرف T وجود ندارد تا بتوان ستون ۴ را آخرین ستون دانست. گفتن اینکه چه حرفی باید پس‌از THA بیاید مشکل به نظر می‌رسد. اگر ستونهای مستطیل را از بالا به پایین بررسی کنیم، در سطر ۷ به نظر می‌رسد که مناسب است W قبل از ITH واقع شود. بنابراین آن ستون را پیش از سه ستونی که قبلاً داشته‌ایم قرار می‌دهیم.

1 3 6	5 7 2 4
E G R	E C E A
O N N	U N C E
E D Y	S T E R
Y D A	I T H A
E D R	A C H E
G D A	R E E M
T E N	W I T H
R T U	K E Y T
N O E	D T H E
P C Y	R U S C
S R I	I S N S

حال جواب به چشم می‌خورد. سطر هشتم کلمهٔ TURKEY [ترکیه] را تداعی می‌کند و سطر دهم کلمهٔ CYPRUS [قبرس] را. در نتیجه ملاحظه می‌کنیم کلمهٔ اول GREECE [یونان] است. بنابراین رمز انتقالی فوق گشوده شده و کلید آن ۴ ۲ ۷ ۵ ۱ ۶ ۳ است. دو حرف آخر N و S به وضوح حروف بی‌معنی هستند و باید آنها را دور بیندازیم.

با استفاده از این روش کلی، گشودن رمز انتقالیِ متناظر با مستطیل کاملاً پر ممکن است. مقلوب‌سازی ستونها برای تشکیل متن صریح فرایند نسبتاً سرراستی است. ممکن است لازم باشد مستطیلهای با عرضهای گوناگون بررسی شوند، اما گشودن رمز معمولاً تنها نیاز به صرف وقت دارد.

تمرین

۷۶. رمز انتقالی زیر را که مبتنی بر مستطیلی کاملاً پر است بگشایید:

```
EOECO HENIO DAART TARTL ODYFS OVNQN AELAF SGNOP TESWP
NITET IENOI EHIGI RLBIE CSTEC EFDOW ECXTR SRXSU ONCSV
AIHGE PAA
```

۷۷. رمز انتقالی زیر را بگشایید (به این نکته که X به دفعات تکرار شده توجه کنید، این نکته به‌تعیین طول کلمهٔ کلیدی کمک می‌کند):

```
NSGVA ENXEH THLSO XNDFP ESNIA OAGDI RXPMR YEALS AECHN
TAEOU OASMU XMERE NNTXO UYART LXLCP SAECX
```

۳.۵ مستطیلهای ناکامل

دیدیم که اگر مستطیل کاملاً پر باشد، وظیفهٔ رمزگشا صرفاً مقلوب‌سازی ستونهاست. یک تغییر بسیار جزئی در سیستم رمزنگاری، یعنی کوتاهترکردن سطر آخر مستطیل از عرض مستطیل، سبب افزایش زیادی در ایمنی سیستم می‌شود. در صورت لزوم می‌توان حروف بی‌معنی در انتهای متن صریح آورد تا خانه‌های خالی در انتهای سمت راست سطر آخر پیدا شود.

ابتدا این موضوع را بررسی می‌کنیم که بر اثر این دگرگونی در سیستم، عملیات از رمز درآوردن و به رمز درآوردن چه تغییری می‌کنند. فرض کنید کلمهٔ کلیدی کلمهٔ PRINCETON بوده و پیام به قرار زیر باشد:

THE HOUSE VOTED YESTERDAY TO CUT BACK FOREIGN AID

[دیروز مجلس به کاهش کمکهای خارجی رأی داد]

نمودار انتقال (مستطیل ناکاملی که برای انتقال به کار می‌رود) به قرار زیر است:

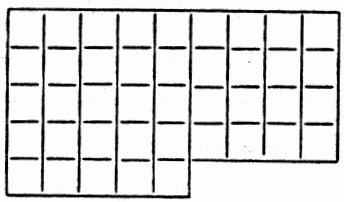
```
P R I N C E T O N
7 8 3 4 1 2 9 6 5
-----------------
T H E H O U S E V
O T E D Y E S T E
R D A Y T O C U T
B A C K F O R E I
G N A I D
```

و پیام رمزی عبارت است از:

OYTFD UEOOE EACAH DYKIV ETIET UETOR BGHTD ANSSC R

برای از رمزدرآوردن این پیام، تعیین نمودار انتقال لازم است. برای انجام دادن این کار، رمزگشا کارخود را با شمارش تعداد حروف، به منظور تعیین طول ستونها، آغاز می‌کند. تعداد حروف پیام ۴۱ حرف و طول کلمهٔ کلیدی ۹ حرف است. از آنجا که حاصل تقسیم ۴۱ بر ۹ خارج قسمت ۴ و باقیماندهٔ ۵ است، چهار سطر کامل و یک سطر ناکامل ۵ حرفی وجود دارند، یا به عبارت دیگر، پنج ستون پنج حرفی و ۴ ستون که هر یک چهار حرفی‌اند وجود دارند. بنابراین نموداری که برای از رمز درآوردن باید به کار رود عبارت است از:

7 8 3 4 1 2 9 6 5



پیام رمزی به ترتیب اعداد کلید در داخل نمودار نوشته می‌شود. OYTFD در ستون ۱ قرار می‌گیرد، UEOO در ستون ۲، EEACA در ستون ۳ و الی آخر، تا پیام رمزی به طور کامل به شکل انتقالی درآید.

7	8	3	4	1	2	9	6	5
		E		O	U			
		E		Y	E			
		A		T	O			
		C		F	O			
		A		D				

آنگاه متن صریح را می‌توان به طور معمولی خواند.

تمرین

۷۸. پیام زیر را با کلید انتقال زیر از رمز درآورید:

۱ ۵ ۴ ۳ ۶ ۲ ۷ ۸.

```
TEAEF OBHIT NERDC MOSHS SPCHT SIIYE EAATI RFERH YYDER
EEMOE TPOIS FRNAR OESER TITDV OFMTT S
```

۷۹. پیام زیر را با استفاده از کلید انتقال مبتنی بر کلمهٔ GEOMETRY از رمز درآورید:

```
ILSOR ANSNE SUDUA CEFES HOTNO MAEAR HTOMM IHOIK GSTWE
TTTCE HEYHH TIHTC DACTS WTNON KMEHS EG
```

۴.۵ گشودن مستطیلهای ناکامل به روش کلمهٔ احتمالی

رمزگشایی که می‌خواهد یک رمز انتقالی ستونی ناکامل را بگشاید، در مقایسه با حالت کاملاً پُر، مسالهٔ بسیار مشکلتری دارد. حتی اگر طول کلمهٔ کلیدی را بداند (که درواقع باید آن را تعیین کند)، نمی‌داند که کدام ستونها بلند و کدام کوتاه هستند. این موضوع مسألهٔ تلاش برای تعیین حدود دنباله‌های حروف را، برای تشکیل ستونهای کامل به منظور مقلوب‌سازی آنها، پیچیده می‌سازد.

البته اگر رمزگشا بتواند دو حرف را برای تشکیل یک دوحرفی صحیح کنار هم قرار دهد، آنگاه از دنباله‌های حروف شامل آن دو حرف بلافاصله تعدادی ترکیب صحیح در زیر و بالای آن دوحرفی حاصل می‌شود. اگر بتواند دنبالهٔ سومی از حروف را بیابد که با افزودن آن به این دوحرفیها ترکیبات سه‌حرفی مناسبی تشکیل شود، ممکن است بتواند آرایهٔ حاصل را گسترش دهد و به تدریج رمز را بگشاید. زیرا، در حین آنکه این آرایه گسترش می‌یابد، با تعیین حدودی برای سطرهای بالایی و پایینی این آرایه که ترکیبات صریح مناسب در بین آنها یافت می‌شوند و نیز با بررسی فواصل بین حروفی از متن رمزی که در متن صریح کنار هم قرار می‌گیرند، نشانه‌هایی در مورد عرض مستطیل و طول صحیح ستونها به دست می‌آید.

در مثال زیر، مسألهٔ گشودن یک مستطیل ناکامل با استفاده از یک کلمهٔ احتمالی را بررسی می‌کنیم.

اگر رمزگشا اطلاعاتی دربارهٔ پیام داشته باشد که با استفاده از آنها بتواند وجود کلمهٔ معینی را در پیام به درستی حدس بزند، این کلمه مجموعه‌ای از ترکیبات را در اختیار او می‌گذارد که برای تشکیل آنها در مستطیل رمزنگاری کار کند و بنابراین فایدهٔ زیادی برای او دارد. اگر این کلمهٔ احتمالی طولانیتر از عرض مستطیل باشد، تعیین تعداد ستونها ممکن می‌شود.

برای روشن ساختن این نکته، فرض کنید می‌خواهیم پیام زیر را بگشاییم:

```
ARLHI KVENN UVHEV AMADF IWNDE YRTOS LTEND RTPET UVSIC
OESIL SDCTL NMAED NREHM HEYRD OEYEO ATNEE VAUHE GRTEE
SIEAS DNET
```

به علاوه فرض کنید دلیلی برای این گمان که متن شامل کلمهٔ COMMUNISTS باشد داشته باشیم.

اگر عرض مستطیل کمتر از ۱۰ ستون باشد، کلمهٔ COMMUNISTS در یک سطر جا نمی‌گیرد و قسمتی از انتهای آن در زیر قسمتی از ابتدای آن قرار می‌گیرد.

فرض کنید کلید به طول نُه حرف باشد. در این صورت، صرف‌نظر از اینکه جای کلمهٔ COMMUNISTS در مستطیل کجاست، جای S آخر آن در زیر C خواهد بود. بنابراین در رمز انتقالی، ستون شامل C دوحرفی رمزی CS را ایجاد خواهد کرد. اما در پیام رمزی هیچ‌جا S بعد از C نیامده است. بنابراین اگر کلمهٔ COMMUNISTS در پیام باشد، مستطیل به عرض نُه ستون نخواهد بود.

اگر طول کلید هشت حرف باشد، دوحرف انتهای کلمهٔ COMMUNISTS زیر دو حرف ابتدای آن قرار می‌گیرند و متن رمزی شامل دوحرفیهای CT و OS خواهد بود. هر دو ترکیب در متن رمزی آمده‌اند، و این نشان می‌دهد که طول کلید ممکن است هشت حرف باشد. البته ممکن است که این زوجها تصادفاً ظاهر شده باشند. رمزگشا باید امکان ترکیبات تصادفی را به خاطر بسپارد و در جریان کار در پی‌یافتن شواهد دیگری برای تأیید حدس خود باشد. اگر به همین ترتیب هر یک از طولهای کمتر از هشت را بررسی کنیم در می‌یابیم که هیچ یک از این طولها با کلمهٔ COMMUNISTS سازگار نیست.

با پذیرفتن این ایده که مستطیل به عرض هشت‌ستون بوده و پیام شامل کلمهٔ COMMUNISTS است، خواهیم توانست دو دنباله ازحروف شامل ترکیبات CT و OS را کنار هم قراردهیم.

```
EN
SD
IE
LY
SR
DT
CO
TS
LL
NT
ME
AN
ED
```

هنوز ایده‌ای دربارهٔ اینکه دو ستون فوق را چقدر می‌توانیم در زیر و بالای دو دوحرفی شناخته شدهٔ خود ادامه دهیم نداریم، زیرا نمی‌دانیم کلمهٔ COMMUNISTS در کجای پیام صریح می‌آید. اما با استفاده از طول پیام (۹۹حرف) می‌دانیم که ستونها ۱۲ یا ۱۳ حرف طول دارند، زیرا از تقسیم ۹۹ بر ۸ خارج قسمت ۱۲ و باقیماندهٔ ۳ به دست می‌آید.

همچنین می‌دانیم که پس از Oی CO باید M بیاید، و قبل از Tی TS باید S بیاید. بهتر است M را که فراوانی آن خیلی کمتر از S است برای ادامهٔ کار انتخاب کنیم. اگر چه سه M در پیام وجود دارند، تنها دوتای آنها باید در نظر گرفته شوند، زیرا فاصلهٔ Mای که در متن رمزی در MAED آمده با C نزدیکتر از آن است که در متن صریح بتواند کنار CO بیاید.

حال دو دنبالهٔ حروف شامل دو M دیگر را در کنار ستون OS می‌نویسیم و سه حرفیهای حاصل را بررسی می‌کنیم.

	فراوانی		فراوانی
ENU	1	ENE	5
SDV	0	SDD	0
IEH	0	IEN	10
LYE	1	LYR	0
SRV	1	SRE	13
DTA	4	DTH	22
COM		COM	
TSA	2	TSH	2
LLD	2	LLE	5
NTF	0	NTY	1
MEI	1	MER	14
ANW	0	AND	8
EDN	0	EDO	1
	12		81

احتمال درستی سه‌حرفیهای سمت راست بسیار بیشتر از سمت چپ است. این موضوع را می‌توان به طریق آماری با فهرست کردن فراوانی دوحرفیهای واقع در دو ستون سمت راست هر یک از دو دستهٔ فوق و مقایسهٔ مجموع فراوانیهای این دو دسته تأیید کرد. (اعدادی که در فهرست بالا آمده‌اند با گردکردن فراوانی واقعی دوحرفیها، که در ضمیمهٔ الف آمده‌اند، به نزدیکترین مضرب صد، حاصل شده‌اند.)

دربررسی سه حرفیهای تشکیل شده ترکیب SDD را مشاهده می‌کنیم که ترکیب ناممکنی در زبان صریح است. بنابراین باید فرض کنیم که ستونها در بالای IEN ادامه نمی‌یابند. از اطلاعاتی که دربارهٔ طول ستونها در دست داریم، می‌توانیم دنباله‌های حروف خود را تا دو حرف دیگر در جهت پایین ادامه دهیم.

IEN
LYR
SRE
DTH
COM
TSH
LLE
NTY
MER
AND
EDO
DRE
NTY

حال می‌توانیم از دو M مذکور، M دیگر را به دنبال COM بیاوریم:

IENH
LYRE
SREV
DTHA
COMM
TSHA
LLED
NTYF
MERI
ANDW
EDON
DRED
NTYE

این ترکیبات همگی خوب هستند به استثنای IENH در بالای ستون، که گر چه غیرممکن نیست ولی چندان هم محتمل نیست. حال به دنبال Uیی می‌گردیم که بعد از COMM

بیاید. سه U وجود دارند، اما به سرعت آشکار می‌شود که بهترین U اولین حرف از دستهٔ نهم است.

IENHT
LYREP
SREVE
DTHAT
COMMU
TSHAV
LLEDS
NTYFI
MERIC
ANDWO
EDONE
DREDS
NTYEI

حال قطعاً می‌توانیم سطر بالایی را کنار بگذاریم، بنابراین آرایه‌ای که اکنون داریم آرایهٔ فوق بدون سطر بالایی است.

در ادامهٔ عملیات مقلوب‌سازی طبعاً باید N از کلمهٔ COMMUNISTS را پس از COMMUبیاوریم و پس از آن I و در آخر S را بیاوریم، تا متن صریح کاملاً به دست آید.

به جای روش فوق از روش زیر نیز می‌توان استفاده کرد. فرض کنید در متن رمز ستونهایی را که قبلاً جایشان مشخص شده علامتگذاری کنیم، و به هر کدام از آنها عددی را که متعلق به بالای آن ستون است اختصاص دهیم. این اعداد متوالیاً افزایش می‌یابند زیرا، در فرایند به رمز درآوردن، ستونها با همین ترتیب از مستطیل انتقال بازنویسی شده‌اند.

1	2	3	4
ARLHIKVENNUVH	EVAMADFIWNDE	YRTOSLTENDRT	PETUVSICOESI

5	6	7
LSDCTLNMAEDN	REHMHEYRDOEY	EOATNEEVAUHEGRTEESIEASDNET

با انجام‌دادن این کار، مشاهده می‌کنیم که دنباله‌های حروفی که هنوز در مقلوب‌سازی ما وارد نشده‌اند عبارت‌اند از یک دنبالهٔ ۱۳ حرفی نشاندهندهٔ ستون ۱، و یک دنبالهٔ ۲۶ حرفی نشاندهندهٔ ستونهای ۷ و ۸. می‌توانیم ۲۶ حرف اخیر را به دو مجموعهٔ ۱۳تایی

تقسیم کنیم، و آنگاه سه ستون باقیمانده را در کنار ستونهایی که قبلاً مقلوب ساخته‌ایم قرار دهیم.

	1 7 8
LYREP	A E R
SREVE	R O T
DTHAT	L A E
COMMU	H T E
TSHAV	I N S
LLEDS	K E I
NTYFI	V E E
MERIC	E V A
ANDWO	N A S
EDONE	N U D
DREDS	U H N
NTYEI	V E E
	H G T

حروفی از کلمهٔ COMMUNISTS که تا به حال به کار نرفته‌اند در پنجمین سطر سه ستون آخر ظاهر شده‌اند و از آنجا معلوم می‌شود که این ستونها باید به ترتیب ۱ ۸ ۷ درآیند.

سرانجام، از آنجا که ستونهای بلند مستطیل انتقال قبل از ستونهای کوتاه واقع می‌شوند، ستونهایی که با ۷ و ۱ و ۸ شماره‌گذاری شده‌اند متعلق به سمت چپ مستطیل‌اند.

7 1 8 5 3 6 2 4
E A R L Y R E P
O R T S R E V E
A L E D T H A T
T H E C O M M U
N I S T S H A V
E K I L L E D S
E V E N T Y F I
V E A M E R I C
A N S A N D W O
U N D E D O N E
H U N D R E D S
E V E N T Y E I
G H T

به این ترتیب کلید و نیز تمام متن صریح را به دست آورده‌ایم.

تمرین

رمزهای انتقالی زیر را با استفاده از کلمهٔ احتمالی داده شده **بگشایید.**

۸۰. کلمهٔ احتمالی: LOS ANGELES

```
HPYCR OEMDR SRIHD RNNSU YEAAE TSSED ETCCS FAIRN DAFTE
OGSOM ETSCA ALLMO ERNIR PMEUF BA
```

۸۱. کلمهٔ احتمالی: WASHINGTON

```
NTHTL ASNAE TTOHE FMIPW TNTOO NKTGO EKINM HTSTO EIETT
CHOYL HHCTM OMWEN GOEHM OCEET ILLAO DWFNE XNCEA EINTF
IAL
```

۵.۵ مستطیلهای ناکامل در حالت کلی

دیدیم که اگر کلمه‌ای در پیام شناخته شده باشد، و به ویژه اگر این کلمه طولانیتر از عرض مستطیل باشد، گشودن پیام به کمک مقلوب‌سازی ممکن است.

حال یک رمز انتقالی ستونی را که اطلاعی از کلمات احتمالی آن نداریم بررسی می‌کنیم.

```
GAELT CCRNT EOMEL EDOND GSBDH SOEDU HDAEE EEINT
TEEAQ UENES EGGTO EGPHI NNUUL SANEB YEAHM IESNA
RLBBV DE
```

این رمز از کیفیت کاملاً خاصّی برخوردار است. رمز شامل حرف Q است. این حرف در زبان انگیسی دارای این خاصیت جالب است که در انتهای هیچ کلمه‌ای نمی‌آید و همواره بعد از آن حرف U می‌آید، به استثنای کلمات اختصاری بخصوصی مانند .G.H.Q یا اسامی خاص مانند Iraq (عراق). از این نکته برای شروع کار می‌توان استفاده کرد: سعی می‌کنیم دنباله‌ای از حروف را بیابیم که با دنبالهٔ حروف شامل Qترکیب شود. حرف U که در متن رمزی سمت راست Q واقع شده است نمی‌تواند در متن صریح با آن ترکیب شود. بنابراین، پس از Q باید یکی از سه Uی باقیمانده بیاید. بنابراین اگر کار را با ترکیب دوحرفی QU شروع کنیم، فقط سه حالت ممکن را باید بررسی کنیم (با فرض آنکه Q حرفی بی‌معنی نباشد).

اگر دنبالهٔ حروف شامل Q را تشکیل دهیم ـ مثلاً در هر طرف آن پنج حرف را بگیریم ـ خواهیم توانست برای هربار ظهور حرف U، دنباله‌ای شامل آن حرف U با طول مساوی دنبالهٔ فوق درکنار آن قرار دهیم.

T	H	P	H
T	S	H	I
E	O	I	N
E	E	N	N
A	D	N	U
Q	U	U	U
U	H	U	L
E	D	L	S
N	A	S	A
E	E	A	N
S	E	N	E

اگر بخت‌یار باشد، به وضوح معلوم خواهد بود که کدام مجموعه از دوحرفیها، مجموعهٔ صحیح است. اگر نشانهٔ واضحی از جواب صحیح در دست نباشد، درصدد استفاده از نتیجهٔ بررسی فراوانی دوحرفیهایی بر می‌آییم که ازکنار هم‌گذاشتن دنباله‌های حروف تشکیل می‌شوند. البته در استفاده از فراوانی دوحرفیها با ابهاماتی مواجهیم، زیرا نه می‌دانیم طول ستون مربوطه در مستطیل انتقال چقدراست و نه می‌دانیم QU درکجای آن قرارگرفته است.

با پذیرفتن این ایده که پنج حرف در بالای Q و پنج حرف در زیر آن قرار داشته باشند، فراوانی دوحرفیهای مختلف را یادداشت می‌کنیم (ضمیمهٔ الف را ملاحظه کنید). به این ترتیب جدول زیر به دست می‌آید:

دوحرفی	فراوانی	دوحرفی	فراوانی	دوحرفی	فراوانی
TH	22	TP	0	TH	22
TS	3	TH	22	TI	9
EO	0	EI	1	EN	10
EE	3	EN	10	EN	10
AD	3	AN	12	AU	1
QU		QU		QU	
UH	0	UU	0	UL	2
ED	9	EL	3	ES	9
NA	2	NS	3	NA	2
EE	3	EA	5	EN	10
SE	6	SN	0	SE	6
	51		56		81

ستون سمت راست بهتر از همه به‌نظر می‌رسد، زیرا مجموع فراوانیهای آن بسیار بیش از دو ستون دیگر است و به علاوه تنها ستونی است که دو حرفِ با فراوانی خیلی کم ندارد، یعنی درایه‌های صفر در آن ستون وجود ندارند. این نتایج قطعی نیستند. دوباره باید تأکید کنیم که با ملاحظات آماری سروکار داریم. اگر کار را با ستون سمت راست ادامه دهیم اما پیشرفتی حاصل نشود، ممکن است لازم شود برگردیم و دومین ستون مناسب از دوحرفیها را امتحان کنیم.

کاری را که در توضیح صفحهٔ ۸۴ در مورد استفاده از وزنهای لگاریتمی به‌جای فراوانیهای تک حرفی گفتیم، برای دوحرفیها نیز می‌توان انجام داد. برای این کار باید به‌جای فراوانی هر دوحرفی لگاریتم آن را قرار داد.

تا اینجا ترکیبات زیر را به دست آورده‌ایم:

TH
TI
EN
EN
AU
QU
UL
ES
NA
EN
SE

این دوحرفیها کمکی به تعیین حدود ستونها نمی‌کنند، زیرا می‌توانیم آنها را در هر دو جهت ادامه دهیم و ترکیبات ممکنی را به دست آوریم، اما می‌توانیم از طریق دیگری کمک بگیریم.

فرض کنید پیامی مشتمل بر n حرف داریم. در مثال ما، $n = ۸۷$. در این صورت ابعاد مستطیل، r و c (که r نشاندهندهٔ تعداد سطور است و c تعداد ستونها) باید چنان باشند که

$$n \leq r.c. \qquad (۱.۵)$$

تساوی تنها موقعی برقرار است که مستطیل کاملاً پر باشد، و در چنان حالتی طول تمام ستونها با هم برابر است. در غیر این صورت، ستونهای کوتاه به طول $r - ۱$ و ستونهای

بلند به طول r هستند، و

$$(r-۱).c < n < r.c \quad . \qquad (۲.۵)$$

حال اگر احتمال دهیم که دو حرف C_i و C_j از پیام رمزی (در مثال فوق Q و U) در متن صریح مجاور یکدیگرند، این دوحرف باید در یک سطر مستطیل قرار داشته باشند (مگر آنکه اوّلی در انتهای یک سطر و دومی در ابتدای سطر بعدی باشد، که در این حالت می‌توانیم استدلال خود را اصلاح کنیم). بنابراین، تفاضل $j-i$، یعنی فاصلهٔ آن دوحرف در پیام رمزی (در مثال ما $j-i=۱۹$) حاصلجمع طول چندستون است؛ یعنی حاصلجمع جمله‌هایی است که یا r هستند یا $r-۱$.

برای مثال، $۹+۱۰=۱۹$، بنابراین یک حالت ممکن عبارت است از:

$$r=۱۰, \quad r-۱=۹ \qquad (۱)$$

همچنین $۶+۶+۷=۱۹$، بنابراین یک حالت ممکن دیگر به قرار زیر است:

$$r=۷, \quad r-۱=۶ \qquad (۲)$$

از $۴+۵+۵+۵=۱۹$، به دست می‌آوریم:

$$r=۵, \quad r-۱=۴ \qquad (۳)$$

الی آخر.

برای هر یک از این مقادیر ممکنِ r، عرضی (c) متناظر با آن از رابطهٔ (۲.۵) به‌دست می‌آید. بدین ترتیب:

(۱) اگر $r=۱۰$، (۲.۵) نتیجه می‌دهد $۹c<۸۷<۱۰c$، در نتیجه $c=۹$؛

(۲) اگر $r=۷$، (۲.۵) نتیجه می‌دهد $۶c<۸۷<۷c$، در نتیجه $c=۱۳$ یا $c=۱۴$.

(۳) اگر $r=۵$، (۲.۵) نتیجه می‌دهد $۴c<۸۷<۵c$، در نتیجه c برابر است با ۱۸ یا ۱۹ یا ۲۰ یا ۲۱.

الی آخر.

این مقادیر c عرضهای ممکنِ مستطیل هستند، یعنی طولهای ممکنِ دنباله‌ای که به عنوان کلید به کار رفته است.

حال فرض کنید که در مستطیل ناکامل انتقال، Q در آخرین ستون سمت راست و U در اوّلین ستون، اما در سطر بعدی زیر آن قرار داشته باشد. در این صورت تعداد حروف

از U تا انتهای ستون آن یکی کمتر از حالتی خواهد بود که Q و U در یک سطر باشند، و در چنان موردی حاصلجمع سابق الذکر، یعنی حاصلجمع طول تعدادی از ستونهای کوتاه و بلند، به جای ۱۹، ۱۸ خواهد بود. از اینجا عرضهای ممکن دیگری برای مستطیل حاصل می‌شوند که باید درنظر گرفته شوند.

این نوع اطلاعات دربارهٔ عرضهای ممکن مستطیل، برای کمک به گسترش آنچه تا به‌حال کنار هم گذاشته‌ایم کافی نیست. کاری که هم اکنون باید انجام دهیم جستجوی دنبالهٔ سومی از حروف است تا به سمت چپ یا راست دوحرفیهای خود الحاق کنیم. بهتر است با سمت راست کار کنیم، زیرا می‌دانیم که بعد از QU باید یک حرف صدادار بیاید. همچنین می‌دانیم بسیار محتمل است که بعد از TH، E بیاید، و نیز می‌دانیم بعد از TI در بسیاری موارد O می‌آید (TIO از نظر فراوانی سومین سه‌حرفی است؛ بعد از TI تقریباً در ۵۰٪ موارد O می‌آید). این مطالب ما را به جستجوی مکانی در متن بر می‌انگیزد که ترکیب EO . . . v در آن آمده باشد، در اینجا v نمایندهٔ حرفی صدادار است. در پیام چنین مکانی وجود دارد. این حروف را به دنبالهٔ دوحرفیهای خود الحاق می‌کنیم.

THE
TIO
ENM
ENE
AUL
QUE
ULD
ESO
NAN
END
SEG

تمام این سه‌حرفیها ممکن به نظر می‌رسند، و چند تا از آنها ترکیبات بسیار خوبی هستند. اگر سعی کنیم ستونها را در بالا و پایین محدوده‌ای که با آن کار می‌کرده‌ایم ادامه دهیم، NPT را بالای THE و EBS را در زیر SEG به‌دست می‌آوریم. هیچیک از اینها شبیه یک ترکیب صریح ممکن نیستند. محتمل است که طول صحیح ستون حداکثر ۱۱ باشد ($r \leq ۱۱$). همچنین از تعداد زیاد سه‌حرفیهای مناسب به نظر می‌رسد که ستونها حداقل ۹ حرفی باشند ($r \geq ۹$). در متن صریح فاصلهٔ بین Eیی که در ترکیب QUE آمده و

Q، ۲۹ حرف است. ضمناً یادآوری می‌کنیم که نتیجهٔ یکی از محاسبات قبلی ما $r = ۱۰$ بود. از ترکیب این دو موضوع به این نتیجه می‌رسیم که ستونها به طولهای ۹ و ۱۰ هستند، و عرض مستطیل ۹ است. یعنی باید دو ستون بلند و یک ستون کوتاه در بین E و Q وجود داشته باشند.

حال دو راه مختلف برای ادامهٔ کار وجود دارند.

الف. برای تشکیل ستونهای آزمایشی به منظور مقلوب‌سازی، از اطلاعاتی که تا اینجا به دست آمده استفاده می‌کنیم. E از THE که ابتدای دنبالهٔ ... EOMEL است، در پیام رمزی در مکان ۱۱ آمده و به نظر می‌آید که در سطر بالای ستون قرار دارد، زیرا ترکیب NPT در بالای آن مردود شناخته شده است. بنابراین، ده حرف نخستِ پیام که ستون ۱ را تشکیل می‌دهند نشاندهندهٔ یک ستون بلند هستند. باید دوتا از سه ستون بعدی بلند و یکی از آنها کوتاه باشد، زیرا فاصلهٔ بین E(درستون ۲) و Q (در ستون ۵) ۲۹ است.

برای نشان‌دادن این وضعیت سه ستون ۲، ۳ و ۴ را در کنار ستون اول، مطابق آرایهٔ زیر، می‌نویسیم:

1	2	3	4
		D	U
G	E	G	H
A	O	S	D
E	M	B	A
L	E	D	E
T	L	H	E
C	E	S	E
C	D	O	E
R	O	E	I
N	N	D	N
T	D	U	

حروفی که در زیر آنها خط کشیده شده است، ممکن است به انتهای یک ستون یا ابتدای ستون بعدی تعلق داشته باشند، بسته به اینکه کدام یک از ستونهای ۲، ۳، ۴ کوتاه باشد.

حال، از آنجا که فاصلهٔ بین Q (از ستون ۵) و U (از ستون ۷) ۱۹ است، نتیجه می‌گیریم که یکی از ستونهای ۵ و ۶ بلند و دیگری کوتاه است. این موضوع مانند فوق

نشان داده می‌شود، یعنی یک حرف مشترک در انتهای ستون ۵ و ابتدای ستون ۶ می‌آید که فقط امکان دارد به یکی از آن دو متعلق باشد.

1 2 3 4 5 6 7

```
    D U   E
G E G H T S
A O S D T E
E M B A E G
L E D E E G
T L H E A T
C E S E Q O
C D O E U E
R O E I E G
N N D N N P
T D U   E
```

درنتیجه، تنها یکی از سه ستون آخر کوتاه است، زیرا تعداد کل حروف باقیمانده ۲۹ است. حال آرایهٔ زیر را داریم:

1 2 3 4 5 6 7 8 9

```
    D U   E   N S
G E G H T S H E N
A O S D T E I B A
E M B A E G N Y R
L E D E E G N E L
T L H E A T U A B
C E S E Q O U H B
C D O E U E L M V
R O E I E G S I D
N N D N N P A E E
T D U   E   N S
```

که در آن حروفی که در زیر آنها خط کشیده شده است یکی از دو وضعیت ممکن را اتخاذ کرده‌اند. اکنون با توجه به اینکه ممکن است لازم باشد بعضی از ستونها را یک محل به‌سمت پایین حرکت دهیم، قادر به انتقال ستونها برای مقلوب‌سازی، همانند مورد مستطیل کاملاً پر، خواهیم بود.

ب. راه ممکن دیگر گسترش آرایه‌ای است که به دست آمده بود. برای مثال، بعد از TIO خیلی اوقات N می‌آید، بنابراین می‌توانیم در پی دنباله‌ای از حروف بگردیم که چون به سه‌حرفیهای به دست آمده بیفزاییم چهارحرفی TION حاصل شود. پس از کنار گذاشتن Nهایی که در ستونهای به دست آمده قرار دارند، Nهای کمی باقی می‌مانند که باید بررسی شوند. بنابراین N موجود در مکان ۹ را نمی‌توان به کار برد، زیرا به انتهای ستون خود نزدیک است. N مکان ۱۹ قبلاً استفاده شده است. N مکان ۳۹ نیز قابل استفاده نیست، زیرا آن هم در انتهای ستون خود واقع است. با بررسی تمام Nها، درمی‌یابیم که تنها Nممکن برای الحاق به TIO، N مکان ۷۹ است. (توجه کنید که در آرایهٔ ستونها که درقسمت الف برای مقلوب‌سازی به دست آمد، به وضوح معلوم است که انتخاب این N تنها انتخاب ممکن است.)

```
5 7 2 9

T H E S
T I O N
E N M A
E N E R
A U L L
Q U E B
U L D B
E S O V
N A N D
E N D E
S E G
```

ترکیباتی که با افزودن این ستون تشکیل می‌شوند بسیار خوب‌اند. حال می‌توانیم حدس زدن کلمات را آغاز کنیم، به عنوان مثال کلمهٔ ممکن QUEBEC را می‌توانیم حدس بزنیم. Eبخصوصی که باید به QUEB الحاق شود به سرعت معلوم می‌شود، و در نتیجه آرایهٔ زیر حاصل می‌شود:

```
5 7 2 9 4

T H E S U
T I O N H
E N M A D
E N E R A
A U L L E
Q U E B E
U L D B E
E S O V E
N A N D I
E N D E N
S E G
```

حال با تکمیل کلمهٔ QUEBEC، به متن صریح و کلید زیر می‌رسیم:

5 7 2 9 4 1 3 8 6

موفقیت ما در گشودن این رمز مرهون خصوصیات مساعدی درآن بود. وجود Q تقریباً مسجل‌کرد که بعد از آن U می‌آید و از آنجا مجموعه‌ای از دوحرفیها به دست آمد که توانستیم آن را گسترش دهیم.

اگر مستطیل کاملا پر نباشد و دوحرفی آشکاری وجود نداشته باشد که تشکیل آن مدخلی برای گشودن رمز باشد، چه باید کرد؟ یک راه چاره ممکن است این باشد که یک زوج از حروفی که احتمال ترکیبشان باهم زیاد است، مانند TH یا RE، انتخاب شود و سپس هر دو دنباله از حروفی که شامل این زوج‌اند امتحان شوند و آن دودنباله‌ای که دارای مناسبترین ترکیبات‌اند درکنار هم قرار داده شوند. اگر یکی از حروف دوحرفی انتخاب شده فراوانی کمی داشته باشد ـنظیر V در ترکیب VEـ تعداد حالتهای ممکن به مقدار زیادی کاهش می‌یابد. اگر از میان ستونهای دوحرفی، که تحت بررسی هستند، بهترین ستون به‌سهولت آشکار نباشد، با استفاده از محاسبهٔ فراوانیها می‌توان ستون خوبی را انتخاب کرد.

راه زیر که مبتنی بر چنین ترکیبات خاصی نیست، می‌تواند راهی کلی برای گشودن رمزهای انتقالیِ ستونی باشد: فرض کنید کار را با ابتدای پیام شروع کنیم. یکی از دو سر ستون ۱، یعنی ابتدای آن شناخته شده است و مشکلی برای تعیین حد این ستون در سمت بالای آن نیست. دنباله‌ای از حروف ابتدای پیام را انتخاب می‌کنیم و آن را در مقابل تمام دنباله‌های دیگر هم طول با آن قرار داده، جابه‌جا می‌کنیم تا دو حرفیهای مناسبی ساخته شوند. ممکن است بعضی از وضعیتها به دلیل اینکه شامل ترکیبات غیرممکن‌اند بلافاصله کنار گذاشته شوند، مثلاً نظیر ترکیبی که در آن بعد از V حرف بی‌صدا آمده باشد. احتمالاً تعداد چنین موارد غیرممکنی کم است، زیراممکن است اولین حرف یک دوحرفی نشاندهندهٔ انتهای یک کلمه و دومین حرف آن نشاندهندهٔ ابتدای کلمهٔ دیگری باشد.

در وضعیتهای بسیار مساعد، ممکن است مجموعه‌ای از دوحرفیها مجموعهٔ خوبی از زوجهای با فراوانی زیاد باشد به طوری که صحت آن بسیار محتمل به نظر برسد. در چنان موردی، قدم بعدی تلاش برای قراردادن دنبالهٔ سومی از حروف قبل یا بعد از دوحرفیهای مناسب است تا سه‌حرفیهای مناسبی ساخته شوند. ادامهٔ این عملیات رفته‌رفته به بازسازی تمام پیام منجر می‌شود.

هنگامی که دو یا سه ستون به طور صحیح کنار هم قرار داده شوند، ممکن است کلمات کاملی تداعی شود، طول ستونها آشکار شود، و گشودن رمز با سرعت فزاینده‌ای پیشرفت کند. مشکلترین مرحلهٔ کار تشکیل اولین مجموعهٔ دوحرفیهاست.

برای سهولت کار در این مرحله می‌توانیم فراوانی هر دوحرفی را یادداشت کرده مجموع فراوانیهای هر ستون از دو حرفیهای تحت بررسی را به عنوان شاخص به آن ستون نسبت دهیم، به این امید که بزرگترین شاخص نشاندهندهٔ دوحرفیهایی باشد که به درستی کنار هم قرارگرفته‌اند. حتی اگر یکی از این شاخصها آشکارا بزرگتر از بقیه نباشد، با این‌کار ستونهای محتمل به تعداد کمی محدود خواهد شد.

در اینجا مثالی برای این روش ارائه نمی‌کنیم، زیرا مفصل بوده و تا درجهٔ زیادی شامل آزمایش و خطاست. با این حال استفاده از این روش از لحاظ نظری امکان‌پذیر است و با صرف وقت کافی، می‌توان با استفاده از آن رمز را گشود.

تمرین

۸۲. رمز انتقالی زیر را که حدس می‌زنیم شامل کلمهٔ EARTHQUAKE [زلزله] است، بگشایید:

```
DPSEW NKKWR EEILG UOSIA ANLEA HAKAD SMLAQ TAESA NOIAO
TEIIA OMHHL ITREW TGEPE FWDFF ATCES TDDLD RICTH EAIHE
WLE
```

۶.۵ عبارات تکراری در پیامهای متفاوت؛ پیامهای هم‌طول

به نظر می‌رسد که استفاده از انتقال ستونی با مستطیل ناکامل ممکن است گاهی اوقات موجب تأخیر درگشوده شدن رمز شود، شاید هم گاهی اوقات موجب تأخیر نسبتاً طولانی شود. البته اگر تنها یک پیام برای بررسی در دست باشد، احتمالاً موضوع فوق درست خواهد بود. اما اگر پیامهای متعددی با کلید یکسان در دست باشند، آنگاه گاه حالات خاصّی روی می‌دهند که به گشودن پیام کمک زیادی می‌کنند.

دو مورد از چنین حالاتی را بررسی می‌کنیم. ابتدا این امکان را که هر یک از دو پیام شامل عبارت صریح طولانی یکسانی باشند بررسی می‌کنیم. در این صورت، این موضوع را می‌توان تشخیص داد و برای گشودن رمز به کار برد.

برای روشن شدن مطلب، فرض کنید به پیامهای رمزی زیر دست یافته باشیم:

1. FRIIT ECESE ONEAS DHLIS NTTDR CONML RDONR SDDSM
   AFGHI HHTTA ONDAT ELTAB TETMA YVRTS NYADE EIOTI
   AACAE EHLMS ARETE INRE

2. ANART AONIN SDBEH LMONT BATRE ASIOE EOPET MNEPT
   ITTDD SCNEI SEYRC OTEOT UOFRI NCLAL HBEEI OT

در بررسی فراوانی سه‌حرفیهای این پیامها با هشت دنبالهٔ تکراری از حروف مواجه می‌شویم که در زیر آنها در دو متن خط کشیده شده است.

علت این تکرارها واضح به نظر می‌رسد. موضوع این است که از انتقالهای ستونی هم عرض (فرض بر این است که کلید هر دو پیام یکی باشد) برای دو پیام که هر دو شامل عبارت طولانی یکسانی هستند استفاده شده است. این عبارت در قسمتهای مختلف دو مستطیل ظاهر می‌شود. در نتیجه حروفی از عبارت که در ستونی از یک پیام می‌آیند در پیام دیگر در ستونی دیگر می‌آیند. به این دلیل است که دنباله‌های تکراری حروف در دو مکان مختلف از دو پیام می‌آیند.

هشت دنبالهٔ تکراری وجود دارند (۵سه‌حرفی، ۲ چهارحرفی، ۱ پنج‌حرفی) که نشاندهندهٔ آن است که مستطیل انتقالِ هر دو پیام ۸ ستونی است، و احتمالاً عبارت تکراری حداقل سه‌سطر را اشغال می‌کند؛ بنابراین حداقل شامل ۲۴ حرف است.

حال که عرض مستطیلها را می‌دانیم، می‌توانیم تعداد ستونهای کوتاه و بلند را در هر پیام محاسبه کنیم. پیام اول دارای ۹۹ حرف است. از تقسیم ۹۹ بر ۸ خارج قسمت ۱۲ و باقیماندهٔ ۳ به دست می‌آید؛ یعنی پیام اول دارای ۳ ستون ۱۳ حرفی و ۵ ستون ۱۲ حرفی است. پیام دوم دارای ۷۷ حرف است. بنابراین باید شامل ۵ ستون به طول ۱۰ و ۳ ستون به طول ۹ باشد.

به علاوه، از آنجا که حروف FRI در ابتدای پیام اول قسمتی از عبارت تکراری هستند، ابتدای این عبارت تکراری طولانی باید در سطر اول مستطیل ۱۳ × ۸ که شامل متن صریح پیام اول است باشد. ممکن هم هست که درست در آغاز پیام باشد. در پیام دوّم، عبارت تکراری طولانی باید در داخل پیام ظاهر شود، زیرا در دو طرفِ حروف TAO از ستون ۱ حروف دیگری از این ستون قرار دارند.

حال در هر پیام، اجزای این عبارت تکراری طولانی را از هر ستون به همراه عددی از کلید که به آن ستون مربوط است یادداشت می‌کنیم. اعداد کلید را می‌دانیم زیرا بازنویسی پیام رمزی از روی مستطیل اصلی به ترتیب اعداد متوالی صورت می‌گیرد. بنابراین داریم:

	پیام ۱		پیام ۲
1	FRI	1	TAON
2	EAS	2	EHLM
3	RCO	3	EAS
4	DDS	4	ETM
5	TAON	5	DDS
6	ETM	6	RCO
7	EEIOT	7	FRI
8	EHLM	8	EEIOT

فرض کنید حرف اول این دو عبارت تکراری در دو مستطیل انتقال،x ستون از یکدیگر فاصله داشته باشند. در این صورت همین مطلب برای هر حرف مشترک دیگری از این دو عبارت صادق است؛ یعنی مکانهای هر دو حرف مشترک در دو پیام x ستون از یکدیگر فاصله دارند.

بنابراین از آنجا که FRI از پیام ۱ در ستون ۱ آمده، نتیجه می‌گیریم که ستون ۷، که ستونی است که FRI از پیام ۲ در آن آمده، باید در مستطیل انتقال x ستون دورتر از ستون ۱ باشد، و از آنجا که EAS در ستون ۲ از پیام ۱ و ستون ۳ از پیام ۲ واقع است، ستون ۳ باید به فاصلهٔ x ستون از ستون ۲ باشد. می‌توان برای هر دو ستون که شامل بخش یکسانی از عبارت تکراری باشند همین نتیجه را گرفت.

بنابراین از فرایند زنجیره‌ای زیر استفاده می‌کنیم: بعد از عدد هر ستونی از پیام ۱ عدد ستونی از پیام ۲ را می‌آوریم که با آن ستونِ پیامِ ۱ دارای بخش مشترکی از عبارت تکراری است. چرخهٔ حاصل، یعنی (۱,۷,۸,۲,۳,۶,۴,۵) چنان است که هر زوج متوالی از اعداد، نشاندهندهٔ ستونهایی هستند که در مستطیل اصلی به فواصل یکسان قرار دارند. اما این به آن مفهوم است که این دنبالهٔ اعداد طرحی چند درمیان از کلید انتقال است.

حال تنها کاری که باید برای گشودن پیامها انجام دهیم عبارت است از تعیین فاصلهٔ طرح چند درمیان. زیرا، هنگامی که این فاصله شناخته شود، خواهیم توانست کلید انتقال را بازسازی کنیم. یک راه انجام دادن این کار آن است که هر یک از طرحهای چند درمیان را امتحان کنیم. طرح صحیح متن صریح را ایجاد خواهد کرد.

راه دیگر آن است که متن را در داخل مستطیلی که کلید آن دنبالهٔ حاصل در فوق است بنویسیم. اگر این کار را برای پیام اول انجام دهیم، به این ترتیب که حرف اول هر جزء از عبارت تکراری را در بالای ستون آن قرار دهیم، به دست می‌آوریم:

1	7	8	2	3	6	4	5
F	E	E	E	R	E	D	T
R	E	H	A	C	T	D	A
I	I	L	S	O	M	S	O
I	O	M	D	N	A	M	N
T	T	S	H	M	Y	A	D
E	I	A	L	L	V	F	A
C	A	R	I	R	R	G	T
E	A	E	S	D	T	H	E
S	C	T	N	O	S	I	L
E	A	E	T	N	N	H	T
O	E	I	T	R	Y	H	A
N		N	D	S	A	T	B
		R			D		T
		E					

در اینجا مسأله‌ای در مورد ستونهای ۷ و ۸ وجود دارد. اولی زیاده از حد کوتاه و دومی زیاده از حد بلند است. بنابراین حرف E در بالای ستون ۸ باید به انتهای ستون ۷ تعلق داشته باشد، این وضع به این دلیل رخ داده است که این E تصادفاً تکرار شده و متعلق به عبارت تکراری نبوده است. بنابراین ستونهای ۷ و ۸ را اصلاح می‌کنیم.

1	7	8	2	3	6	4	5
F	E	H	E	R	E	D	T
R	E	L	A	C	T	D	A
I	I	M	S	O	M	S	O
I	O	S	D	N	A	M	N
T	T	A	H	M	Y	A	D
E	I	R	L	L	V	F	A
C	A	E	I	R	R	G	T
E	A	T	S	D	T	H	E
S	C	E	N	O	S	I	L
E	A	I	T	N	N	H	T
O	E	N	T	R	Y	H	A
N	E	R	D	S	A	T	B
		E			D		T

سه ستون بلند باید به سمت چپ مستطیل تعلق داشته باشند. در بالای این سه ستون حروف HETقرار دارند که از آنها چنین برمی‌آید که کلمهٔ اول THE باشد. بنابراین کلید صحیح با ۵۸۶ آغاز می‌شود و فاصلهٔ طرح چند درمیانِ دنبالهٔ حاصل در فوق ۳ است. بنابراین کلید عبارت است از:

5 8 6 1 2 4 7 3

با استفاده از این کلید پیام رمزی گشوده می‌شود.

حالت خاص دیگری که شرح می‌دهیم حالتی است که در آن هر نوع سیستم انتقال را می‌توان گشود. این حالت به در دسترس داشتن دو یا تعداد بیشتری پیام هم‌طول باکلید یکسان بستگی دارد. درچنان مجموعه‌ای از پیامها، هر قدر هم که سیستم انتقال پیچیده باشد، حروفی که در متنهای صریح پیامها دارای عدد مکان یکسانی هستند، در پیامهای رمزی هم عدد مکان یکسانی خواهند داشت. اگر پیامها را یکی پس از دیگری زیر هم بنویسیم، به طوری که حروف اول همهٔ پیامها در یک ستون باشند، و حروف دوم در ستون بعدی، و الی آخر، عملیات گشودن پیامها شامل مقلوب‌سازی این ستونها خواهد بود. به عنوان مثال، اگر پنج پیام در دسترس باشند، ستونهای پنج حرفی را می‌توان در فرایند مقلوب‌سازی جابه‌جا کرد.

به عنوان مثال، اگر احتمال دهیم که دو حرف بخصوص از یکی از پیامها در متن صریح مجاور هم‌قرار دارند، از کنار هم گذاشتن ستونهای شامل آنها باید ترکیبات مناسبی به دست آید. هنگامی که مجموعهٔ مناسبی از دوحرفیها یافته شود، ممکن است حرف دیگری یافته شود که با افزودن ستون آن، سه حرفیهای مناسبی حاصل شود، و ممکن است این کار را بتوان ادامه داد. اگر کار به درستی آغاز شود، پابه‌پای پیشرفت مراحل کار افزودن ستون جدید به ستونهایی که قبلاً در کنار هم گذاشته شده‌اند آسانتر خواهد شد. همچنین، مانند انتقال ستونی، روش استفاده از حاصلجمع فراوانیها ممکن است سودمند باشد.

اگر تعداد پیامهای هم‌طولی که برای بررسی در دسترس‌اند زیاد باشد، گشودن رمز با استفاده از مقلوب‌سازی نسبتاً قطعی خواهد بود. اما از اینجا نمی‌توان نتیجه گرفت که گشودن پیامهایی با طولهای دیگر نیز قطعی است. برای انجام‌دادن این کار با کلیدی که از پیامهای هم‌طول حاصل شده است، لازم است که اطلاعاتی دربارهٔ سیستم کلی و شیوه‌ای که بر طبق آن کلیدهای ویژه به پیامها نسبت داده شده‌اند به دست آید تا بتوان پیامهای با

طولهای دیگر را گشود.

تمرین

۸۳. پیامهای زیر را که از یک مبدأ ارسال شده‌اند بگشایید:

1. ATDCC ITSFA IAEIT EARTF RTARL NRNAL RCUOY SSEHO STNNC OTTER AOTSU UITDS FEHTI RWPOT RNEEN TNAER TIISO LOIRI BONUI OEAEE

2. EENNI ERILA HTICY SRSJT NUIDO TETSE ITOAV DROHU OYNUO AARUI SOEAE IDAST ARLBU ELOTT SUMNY SSNDN NCDNT YIDRD CCEMS ANAY

۸۴. پیام زیر را که شامل کلمات PRESIDENT JOHNSON است بگشایید:

EHENA FONEG SROTE IXTIE ISAAT SASPJ IHNII NCDON REEAE EHSYN TMADT STRSN ZLSNM EEYME TENOF EV

۸۵. پیام زیر را که کلمات احتمالی آن عبارت‌اند از UNITED STATES بگشایید:

AVEUT DTSTH SONGP NSITE ABEIF TESTN TESCL SHADM DOFSR DRTEI EDOMT EOIYN MNRNE SLOSE CTEAF OEUET AMELH KNPLT TROOD DRUDP UEYIF L

۸۶. پیام زیر را بگشایید:

LNTIO PANSC RNIEE STUEE NCEYR AENCA SVCDL OEPSE NCOHT IOPLH RDMNL VMISC RGYHE FTYAO EUEYD OTHEF TPDCE YASPE IAS

۸۷. پیام زیر را بگشایید:

ACNNT LHENT PSOAC TEETE EETRC OMUNC TVNRE EGBNS INRSV ERERU OIRII SOHOT SRMOD TESBB DAEFO CSDEL MREDT OMUEO NIERY Y

ضمیمهٔ الف

جدول فراوانی دوحرفیها

حرف اول \ حرف دوم	·A	·B	·C	·D	·E	·F	·G	·H	·I	·J	·K	·L	·M	·N	·O	·P	·Q	·R	·S	·T	·U	·V	·W	·X	·Y	·Z
A ·	7	125	251	304	13	65	151	13	311	13	67	681	182	1216	5	144	0	764	648	1019	89	137	37	17	202	15
B ·	114	7	2	1	394	0	0	0	74	7	0	152	6	0	118	0	0	81	28	6	89	2	0	0	143	0
C ·	319	0	52	1	453	0	0	339	202	0	86	98	4	3	606	0	1	113	23	237	92	0	0	0	25	0
D ·	158	3	4	33	572	1	20	1	273	5	0	19	27	8	111	0	1	49	75	2	91	15	6	0	40	0
E ·	492	27	323	890	326	106	93	16	118	4	27	340	253	1029	30	143	25	1436	917	301	36	160	153	113	90	3
F ·	98	0	0	0	150	108	0	0	188	0	0	35	1	1	326	0	0	142	3	58	54	0	0	0	5	0
G ·	122	0	0	2	271	0	20	145	95	0	0	23	3	51	129	0	0	150	29	28	58	0	0	0	6	0
H ·	646	2	5	3	2053	0	0	2	426	0	0	6	6	14	287	0	0	56	10	85	31	0	4	0	15	0
I ·	236	51	476	285	271	80	174	1	10	0	31	352	184	1550	554	62	5	212	741	704	7	155	0	14	1	49
J ·	18	0	0	0	26	0	0	0	5	0	0	0	0	0	45	0	0	1	0	0	48	0	0	0	0	0
K ·	14	1	0	1	187	1	0	7	56	0	4	7	1	20	7	0	0	3	39	1	1	0	0	0	4	0
L ·	359	5	6	197	513	28	29	0	407	0	21	378	22	1	208	11	0	9	104	68	72	15	3	0	219	0
M ·	351	65	5	0	573	2	0	0	259	0	0	2	126	8	240	139	0	5	47	1	65	1	0	0	37	0
N ·	249	2	281	761	549	46	630	6	301	4	30	33	47	88	239	2	3	5	340	743	56	31	8	1	71	2
O ·	48	57	91	130	21	731	46	14	52	8	44	234	397	1232	125	164	0	861	201	223	533	188	194	7	23	2
P ·	241	0	1	0	310	0	0	42	75	0	0	144	13	1	268	103	0	409	32	51	81	0	0	0	3	0
Q ·	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	73	0	0	0	0	0
R ·	470	15	79	129	1280	14	80	8	541	0	94	75	139	149	510	25	0	97	300	273	88	65	8	1	140	0
S ·	200	4	94	9	595	8	0	186	390	0	30	48	37	7	234	128	3	9	277	823	192	0	13	0	27	0
T ·	381	2	22	1	872	4	1	2161	865	0	0	62	27	9	756	2	0	295	257	131	120	3	54	0	125	3
U ·	72	87	103	51	91	11	80	2	54	0	3	230	69	318	4	81	0	306	256	263	6	3	0	2	3	1
V ·	65	0	0	2	522	0	0	0	223	0	0	0	1	0	46	0	0	0	2	0	1	1	0	0	5	0
W ·	282	1	0	4	239	0	0	175	259	0	0	5	0	44	159	0	0	13	45	2	0	0	0	0	3	0
X ·	9	0	15	0	17	0	0	1	15	0	0	0	1	0	1	47	0	0	0	23	0	0	0	5	0	0
Y ·	17	1	3	2	84	0	0	0	20	0	1	5	11	5	64	9	0	9	44	5	4	0	3	0	2	1
Z ·	18	0	0	0	36	0	0	0	17	0	0	1	0	0	4	0	0	0	0	0	1	0	0	0	0	2

ضمیمهٔ ب

وزنهای لگاریتمی

A	1.863	N	1.892
B	0.954	O	1.869
C	1.477	P	1.431
D	1.644	Q	0.477
E	2.114	R	1.887
F	1.447	S	1.799
G	1.204	T	1.969
H	1.544	U	1.431
I	1.869	V	1.114
J	0.301	W	1.204
K	0.477	X	0.699
L	1.544	Y	1.279
M	1.398	Z	0.000

ضمیمهٔ ج

فراوانی حروف الفبا در یک نمونهٔ ۱۰۰۰ حرفی. ستون سمت چپ به ترتیب حروف الفبا و ستون سمت راست برحسب فراوانی مرتب شده است.

A	73	E	130
B	9	T	93
C	30	N	78
D	44	R	77
E	130	I	74
F	28	O	74
G	16	A	73
H	35	S	63
I	74	D	44
J	2	H	35
K	3	L	35
L	35	C	30
M	25	F	28
N	78	P	27
O	74	U	27
P	27	M	25
Q	3	Y	19
R	77	G	16
S	63	W	16
T	93	V	13
U	27	B	9
V	13	X	5
W	16	K	3
X	5	Q	3
Y	19	J	2
Z	1	Z	1

ضمیمهٔ د

فراوانی حروفی که در یک نمونهٔ ۱۶۴۱۰ کلمه‌ای انتخاب شده از روزنامه، در اول کلمات واقع شده‌اند. ستون سمت چپ به ترتیب حروف الفبا و ستون سمت راست برحسب فراوانی مرتب شده است.

A	1802	T	2614
B	757	A	1802
C	918	S	1213
D	459	O	1176
E	410	I	922
F	666	C	918
G	293	W	833
H	636	P	768
I	922	B	757
J	95	F	666
K	88	H	636
L	348	M	578
M	578	R	513
N	401	D	459
O	1176	E	410
P	768	N	401
Q	31	L	348
R	513	G	293
S	1213	U	224
T	2614	Y	126
U	224	V	100
V	100	J	95
W	833	K	88
X	10	Q	31
Y	126	X	10
Z	6	Z	6

ضمیمهٔ ۸

فراوانی حروفی که در یک نمونهٔ ۱۶۴۱۰ کلمه‌ای انتخاب شده از روزنامه، در آخر کلمات واقع شده‌اند. ستون سمت چپ به ترتیب حروف الفبا و ستون سمت راست برحسب فراوانی مرتب شده است.

A	480	E	3325
B	25	S	2077
C	107	D	1649
D	1649	N	1592
E	3325	T	1587
F	744	R	906
G	463	Y	903
H	407	O	745
I	72	F	744
J	6	L	599
K	148	A	480
L	599	G	463
M	220	H	407
N	1592	M	220
O	745	W	166
P	84	K	148
Q	1	C	107
R	906	P	84
S	2077	I	72
T	1587	X	34
U	29	U	29
V	15	B	25
W	166	V	15
X	34	J	6
Y	903	Z	5
Z	5	Q	1

پاسخ تمرینها

۱. COWARDS DIE MANY TIMES BEFORE THEIR DEATHS

۲. THE EVIL THAT MEN DO LIVES AFTER THEM

۳. الف) چهارشنبه ب) $\frac{۱}{۴}$

۴. $x = ۱$ ۵. $y = ۲$

۶. الف) AOL MHBSA KLHY IYBABZ PZ UVA PU VBY ZAHYZ IBA PU VBYZLSCLZ

ب) THERE IS A TIDE IN THE AFFAIRS OF MEN WHICH TAKEN AT THE FLOOD LEADS ON TO FORTUNE

۷. عدد کلیدی K برابر ۹ است. ۸. $K = ۲۱$ ۹. $K = ۱۴$

۱۰. $K = ۵$

۱۱. الف) $y = ۱۰$ ب) $x = ۲, ۵, ۸$

۱۲. ۳

۱۳. هر مضربی از ۲ یا ۳

هر عددی که عامل مشترکی با n داشته باشد

۱۴. الف) ۷

ب)

صریح	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
رمزی	G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X	E	L	S	Z

ج) ORDER IS HEAVENS FIRST LAW

۱۵. $C = ۹P$ ۱۶. $C = ۵P$ ۱۷. الف) ۸ ب) ۵ ج) ۴

۱۸. الف) $x = ۲, ۵, ۸$ ب) $x = ۱, ۱۴$

۱۹. الف) ۵ ب) ۳ ج) ۲۱ ۲۰. $C = ۷P$ ۲۱. $C = ۹P + ۴$

۲۲. $C = P + ۷$ ۲۳. $C = ۲۱P + ۱۱$ ۲۴. $C = ۲۵P + ۱$

۲۵. $C = ۱۱P + ۲$ ۲۶. $C = P + ۱۵$ ۲۷. $C = ۷P + ۷$

۲۸. الف) SECRET MESSAGE ب) UNITED NATIONS

ج) UNITED STATES د) WIRELESS

ه) NEW YORK TIMES

در تمرینهای ۲۹ـ۳۲ دنباله‌های رمزی، دنباله‌های درهم‌ریختهٔ انتقالی مبتنی بر کلمات کلیدی زیر هستند:

۲۹. SIGNAL ۳۰. UNIVERSITY

۳۱. GONE WITH THE WIND ۳۲. SUNDOWN

۳۳. SHORT WAVE BROADCASTING CARRIES FURTHER THAN THAT USING REGULAR WAVES IT IS USED BY AMATEURS AND IN FREQUENCY MODULATION AND FOR TRANS-OCEANIC TELEPHONY

۳۴. OF ALL THE STARS THE SUN IS NEAREST TO THE EARTH AND IT IS THE CENTER OF THE SOLAR SYSTEM ALL THE PLANETS MOVE AROUND IT

۳۵. FEMALES OF SOME BREEDS OF SHEEP WEIGH AS LITTLE AS ONE HUNDRED POUNDS OTHER EWES MAY WEIGH OVER TWO HUNDRED TWENTY POUNDS

در تمرینهای ۳۶ـ۴۰، دنبالهٔ صریح معمولی است وکلمهٔ کلیدی دنبالهٔ رمزی (همهٔ دنباله‌های رمزی دنبالهٔ درهم آمیختهٔ انتقالی مبتنی برکلمهٔ کلیدی هستند) عبارت است‌از:

۳۶. HUMAN ۳۷. MILLIONAIRE ۳۸. PHONETICS

۳۹. BLUESTOCKING ۴۰. WASHINGTON

۴۱. THE CHAIRMAN OF THE FEDERAL RESERVE BOARD SAID YESTERDAY THAT A TAX INCREASE IS NEEDED NOW

۴۲. I.C.ها عبارت‌اند از: ص ۳۱: ۰٫۰۸۵ ص ۳۷ : ۰٫۰۶۱

۴۳. توزیعهای مذکور مربوط به پیامهای رمزی تک‌الفبایی یا چندالفبایی‌اند که تعداد الفباهای هر یک در زیر آمده است:

	(۱)	(۲)	(۳)	(۴)	(۵)
تعدادالفباها:	۷	۱	۵	۱	۲۶
I.C.:	۰٫۰۴۱	۰٫۰۶۴	۰٫۰۴۲	۰٫۰۷۶	۰٫۰۳۷

۴۴. ۷ ۴۵. ۵

۴۶. دنبالهٔ صریح: معمولی
دنبالهٔ رمزی: معمولی
کلمهٔ کلیدی: SOLVING

۴۷. دنبالهٔ صریح: معمولی
دنبالهٔ رمزی:معمولی
کلمهٔ کلیدی: WHIST

۴۸. A از توزیع ۱ در مقابل S از توزیع ۲. I.C. برابر است با ۰٫۰۷۶.

۴۹. A از توزیع ۱ در مقابل Y از توزیع ۲. I.C. برابر است با ۰٫۰۷۸.

۵۰. بله. وقتی W از توزیع مرکب ۴۹ در مقابل A از توزیع مرکب ۴۸ قرار گیرد، دو توزیع مطابقت می‌یابند.

۵۱. در چنین صورتی توزیع دو پیام در هیچ حالتی با یکدیگر مطابقت نمی‌یابند.

۵۲. کلمهٔ کلیدی برای دنبالهٔ صریح: JOHNS
کلمهٔ کلیدی برای دنبالهٔ رمزی: HOPKINS

در تمرینهای ۵۳ـ۶۱، تمام دنباله‌های درهم‌ریخته دنباله‌های درهم‌ریختهٔ انتقالی مبتنی برکلمهٔ کلیدی هستند، مگر آنکه خلاف آن تصریح شده باشد:

	دنبالهٔ صریح	دنبالهٔ‌رمزی	کلمهٔ کلیدی برای انتخاب الفباها	تقابل (حروف کلیدی در مقابل این حروف قرار می‌گیرند)
۵۳.	معمولی	معمولی	BROKEN	A_p
۵۴.	معمولی	معمولی	THUNDER	A_p
۵۵.	PHILOSOPHY (غیرانتقالی)	معمولی	VINEGAR	A_p
۵۶.	AGRICULTURE	معمولی	FARMS	A_p
۵۷.	معمولی	EARTHQUAKES (غیرانتقالی)	ISTANBUL	A_p
۵۸.	UNIVERSITY	معمولی	PICTURE	U_p
۵۹.	MONSTER	معمولی	MARYLAND	M_p
۶۰.	UNDERWATER	HYDROGRAPHY	HONEY	U_p
۶۱.	PEANUTS	CARTOON	FUDGE (۱) AMERICA (۲)	P_p P_p

۶۲. **DIFFICULTIES ARE THINGS THAT SHOW WHAT MEN ARE**

۶۳. **IRRATIONALLY HELD TRUTHS MAY BE MORE HARMFUL THAN REASONED ERRORS**

۶۴. الف) $\begin{pmatrix} ۲۳ & ۱۲ \\ ۲۶ & ۲۳ \end{pmatrix}$ ب) $\begin{pmatrix} ۱۱ & ۲۴ \\ ۲۰ & ۹ \end{pmatrix}$

۶۵. الف) ۵ ب) ۱ ج) ۱۸ د) ۹

۶۶. الف) $\begin{pmatrix} ۳ & ۲۴ \\ ۱۹ & ۵ \end{pmatrix}$ ب) $\begin{pmatrix} ۲۴ & ۵ \\ ۱۹ & ۱۴ \end{pmatrix}$ ج) $\begin{pmatrix} ۴ & ۱۱ \\ ۱ & ۲۲ \end{pmatrix}$

۶۷. الف) ۳ ب) (۱) وارون ندارد (۲) ۷ (۳) ۳

۶۸. الف) ۳ ب) ۴ ۶۹. الف) ۲۴ ب) ۱۱ ج) ۸

۷۰. CIDECI

۷۱. $\begin{pmatrix} ۳ & ۴ \\ ۱۱ & ۲۳ \end{pmatrix}$ ۷۲. $\begin{pmatrix} ۷ & ۳ \\ ۱۰ & ۱۹ \end{pmatrix}$ ۷۳. $\begin{pmatrix} ۳ & ۹ \\ ۲ & ۲۳ \end{pmatrix}$

۷۴. **THE THREE GENERAL REGIONS OF THE SOUTH PACIFIC ARE POLYNESIA MICRONESIA AND MELANESIA**

۷۵. **THE HIGH ISLANDS OF THE SOUTH PACIFIC ARE THE EXPOSED SUMMITS OF SUBMERGED VOLCANOES**

۷۶. کلمهٔ کلیدی: JOHNSON ۷۷. کلمهٔ کلیدی: CHESSBOARD

۷۸. **THE SENATE YESTERDAY APPROVED A CODE OF ETHICS FOR ITS MEMBERS FOR THE FIRST TIME IN HISTORY**

۷۹. **HIGH SCHOOL STUDENTS TODAY KNOW MUCH MORE MATHEMATICS THAN THE WISEST OF THE ANCIENT GREEKS**

۸۰. کلمهٔ کلیدی: RAINBOW ۸۱. کلمهٔ کلیدی: MENDING

۸۲. کلید: ۱ ۵ ۲ ۴ ۶ ۸ ۹ ۳ ۱۰ ۷

۸۳. کلمهٔ کلیدی برای هر دو پیام: LEGITIMATE

۸۴. کلمهٔ کلیدی: INVARIANT ۸۵. کلمهٔ کلیدی: REPUBLICAN

۸۶. کلمهٔ کلیدی: WORLD ۸۷. کلمهٔ کلیدی: GEOMETRY

منابعی برای مطالعهٔ بیشتر

رمزشناسی

غیر از اولین کتابی که در فهرست زیر آمده است، هیچ کتاب دیگری در مورد روشهای رمزگشایی به زبان انگلیسی موجود نیست. بیشتر کتابهایی که در مورد رمزشناسی منتشر شده‌اند به تاریخچه و شرح وقایع هیجان‌انگیزی پرداخته‌اند که در آنها رمزگشایی نقش مهمی داشته است. کتابهایی را که در زیر فهرست شده‌اند به این دلیل انتخاب کرده‌ایم که در آنها به اینکه رمزها چگونه گشوده شده‌اند نیز اشاره شده است.

Gaines, H. F., *Cryptanalysis*, Dover, New York, 1956.

این کتاب شامل مباحثی غیرریاضی دربارهٔ روشهای گشودن متون رمزی است. سیستمهایی که در این کتاب بررسی شده بیشتر همانهایی هستند که در کتاب حاضر نیز آمده‌اند.

Kahn, David, *The Code Breakers*, Macmillan, New York, 1967.

کتاب فوق تاریخچهٔ جامعی است از رمزشناسی از قدیمترین ایام تا اوایل قرن بیستم. به‌علاوه شامل شرح وقایع بسیاری مربوط به رمزشناسی پیش از جنگ‌جهانی دوم و در طی این جنگ است.

Pratt, Fletcher, *Secret and Urgent*, Blue Ribbon Books, Garden City, N.Y., 1942.

کتاب فوق چندین واقعهٔ تاریخی را که در آنها زبان رمزی نقش مهمی را ایفا کرده است شرح می‌دهد. این کتاب شامل تعدادی جدول است که در آنها اطلاعات مربوط به

فراوانیها در زبان انگلیسی و چهار زبان اروپایی آمده است. به‌علاوه فهرستی از کلمات الگودار رایج در زبان انگلیسی نیز در این کتاب آمده است.

Yardley, H. O., *The American Black Chamber*, Bobbs Merrill, Indianapolis, 1931.

این کتاب در مورد موفقیتهای یکی از دوایر رمزگشایی در ایالات متحده در طی سالهای ۱۹۱۹ـ۱۹۲۸ بحث می‌کند. آنچه در این کتاب شرح داده شده، تماماً در مورد مکاتبات سیاسی است.

Cleator, P. E., *Lost Languages*, Mentor Books, New American Library, New York, 1959.

این کتاب شرح چگونگی استفاده از قواعد رمزگشایی در بازسازی زبانهای مرده است، مانند زبانهایی که به خط هیروگلیف مصری، یا خط میخی یا خط هجایی «ب» مینوسی نوشته شده‌اند.

Friedman, William F. and Elizabeth S., *The Shakespearean Ciphers Examined*, Cambridge University Press, England, 1957.

این کتاب یک تحقیق آکادمیک رمزگشایانه است که ثابت می‌کند احتمال وجود رمزهای پنهان در نمایشنامه‌های شکسپیر منتفی است.

حساب همنهشتی

LeVeque, W. J., *Topics in Number Theory*, Vol. 1, Addison Wesley, Reading, Mass., 1956.

Gardner, K. L., *Discovering Modern Algebra*, Oxford University Press, 1966. (Also includes material on permutations and matrices)

Griffin, Harriet, *Elementary Theory of Numbers*, McGraw Hill, New York, 1954.

آمار و احتمال

Mosteller, F., Rourke, R. E. K., Thomas, G. B., *Probability with Statistical Applications*, Addison Wesley, Reading, Mass., 1961.

Mendenhall, W., *Introduction to Probability and Statistics*, Wadsworth Publishing Co., Belmont, Calif., 1967.

Hoyt, J. P., *Probability Theory*, International Textbook Co., Scranton, Penna., 1967.

ماتریس

School Mathematics Study Group, *Introduction to Matrix Algebra*, Yale University Press, New Haven, 1961.

Davis, P. J., *The Mathematics of Matrices*, Blaisdell, Waltham, Mass., 1965.

Bowman, F., *Introduction to Determinants and Matrices*, English Universities Press, 1962.

جایگشت

Burnside, W., *Theory of Groups of Finite Order*, Dover, New York, 1955.

Carmichael, R. D., *Introduction to the Theory of Groups of Finite Order*, Dover, New York, 1956.

فهرست راهنما

I.C. ← شاخص‌انطباق
M.F. ← شاخص‌ناهمواری

ابزار رمزی ارتش آمریکا ۱۲
ابهام در حل معادلهٔ همنهشتی ۴۱،۲۵
احتمال وقوع ۷۱،۱۸
از رمز درآوردن ۵
از رمزدرآوری
  الفبای ــ ۶۱،۴۴
اعدادِ نسبت به هم اول ۲۶
اعداد هم‌ارز ۸
اعداد همنهشت ۸ و چند صفحهٔ بعد
الفباهای درهم‌ریخته
  رمزهای مبتنی‌بر ــ ۴۵ و چند صفحهٔ بعد
الفبای
  ــ از رمزدرآوری ۶۱،۴۴
  ــ باطرح‌چند درمیان ۳۰وچندصفحهٔبعد
  ــ به رمزدرآوری ۴۴
  ــ تصادفی ۴۲
  ــ جایگذاری ۶
  ــ درهم(ریخته) ۴۱ و چند صفحهٔ بعد، ۴۵
  ــ متعارف مستقیم ۱۱ و چندصفحهٔ بعد، ۳۶
  ــ متعارف وارونه ۱۲
  ــ معمولی
  فراوانی حروف ــ ۱۹
الگودار
  کلمات رمزی ــ ۵۹
الگوهای فراوانی حروف ۳۳
الگوی فراوانیهای مشخصه ۳۱
انتقال ۱۵۵
  تشخیص ــ ۱۶۲
  ــ ستونی ۱۵۹

اول
اعدادِ نسبت به هم ــ ۲۶
ایمنی ۱۵۳،۲۴،۲۳

بازسازی دنبالهٔ درهم (ریخته) ۶۱،۵۱
به رمزدرآوردن ۵
به رمزدرآوری
الفبای ــ ۶۱،۴۴

پیامها
منبع ــ ۳
پیمانه ۱۰

تبدیل خطی ۱۲۶،۴۱،۳۶
تطابق الفباها ← تناظرالفباها
تطبیق الفباها ← تناظرالفباها
تطبیق الفباها
ــ باجستجو ۹۲
ــ به‌روش‌آماری ۹۲ و چند صفحهٔ بعد
تک‌الفبایی
تبدیل رمز چندالفبایی به‌رمز ــ ۱۰۲ و چند صفحهٔ بعد
جایگذاری ــ باهم‌ارزها ۱۱۱
رمز ــ ۶۲،۱۴
تکمیل دنبالهٔ صریح ۱۴ و چند صفحهٔ بعد، ۱۷
تناظر الفباها ۲۱ و چند صفحهٔ بعد
توزیع (فراوانی) ۲۱
ــ تک‌حرفی ۶۱،۲۱
ــ دوحرفی ۶۱،۵۴
ــ سه‌حرفی ۵۶،۵۵
ناهمواری ــ ۷۰
ــ هموار ۷۰
توزیعها
ترکیب ــ ۹۹ و چندصفحهٔ بعد

جایگذاری تک‌الفبایی باهم‌ارزها ۱۱۱
جایگشت ۱۵۶
جواب معادلهٔ همنهشتی ۲۷

حاصلضرب دو ماتریس ۱۳۴
حروف آغازی کلمات
فراوانی ــ ۱۹۷،۴۶
حروف بی‌صدا
ویژگیهای ــ در ترکیب چندحرفی ۵۴،۵۳،۴۷
حروف پایانی کلمات
فراوانی ــ ۱۹۳،۴۶
حروف‌صدادار
تشخیص ــ از حروف بی‌صدا ۵۵
فاصله‌های ــ ۵۸
ویژگیهای ــ در ترکیب چندحرفی ۴۷، ۵۳، ۵۴، ۵۷، ۶۱
حساب همنهشتی ۷ و چندصفحهٔ بعد، ۲۵
تفریق در ــ ۱۰
تقسیم در ــ ۲۵
جمع در ــ ۱۰
ضرب در ــ ۲۵

دترمینان ۱۳۷
ــ حاصلضرب ماتریسها ۱۳۹
دنبالهٔ درهم (ریخته)

ــ انتقالی مبتنی بر کلمهٔ کلیدی ۴۳
بازسازی ــ ۵۱
ــ مبتنی بر کلمهٔ کلیدی۴۲
دنبالهٔ صریح ۶
دوحرفیها (ی)
فراوانی مشخصهٔ ــ ۵۳، ۱۸۹
ــ مقلوب ۵۴، ۵۷
دورهٔ تناوب
ــ ماتریس ۱۴۰

رمز
ــ تک‌الفبایی ۱۴، ۶۲
ــ جایگذاری ۶
ــ سزاری ۵ و چندصفحهٔ بعد، ۲۳
ــ مبتنی بر الفبای در هم‌ریخته ۴۵ و چندصفحهٔ بعد
رمزشناسی ۲
رمزگشایی ۲
رمزنگاری ۱، ۲
ــ دوسطری ۱۵۵
وسیله‌ای برای ــ ۱۱ و ۱۲
رمزی
دنبالهٔ ــ ۶
نمادهای ــ ۶۱ و ۶۲

زبانهای مرده ۲

سه‌حرفی(ها) ۵۳، ۵۴
فراوانی ــ ۵۴، ۵۵
سیستم
ــ پلیفر ۱۲۵
ــ پنج حرفی ۱۵۴
ــ چندالفبایی ۶۴، ۶۷
ــ چندحرفی ۱۲۴
ــ چهارحرفی ۱۵۴
ــ دوحرفی ۱۲۴
تشخیص ــ ۱۴۲
ــ سه‌حرفی ۱۵۳
ــ کلی ۱۴، ۳۰
ــ هیل ۱۲۶ و چندصفحهٔ بعد

شاخص انطباق ۷۵
ــ توزیع مرکب ۹۲
ــ سیستم دوحرفی ۱۴۵
شاخص ناهمواری ۷۲ و چندصفحهٔ بعد

صورتهای رمزی تکراری
ــ اتفاقی ۷۷
فاصلهٔ بین ــ ۷۷، ۷۸

ضرب
ــ غیرجابجایی ۱۳۵
ــ ماتریسها ۱۳۳

طرح چند درمیان ۲۳، ۳۰، ۳۶

فاصلهٔ بین صورتهای رمزی تکراری ۷۷، ۷۸
فاصلهٔ طرح چند درمیان ۴۱
فراوانی ۱۸ و چندصفحهٔ بعد، ۶۹
توزیع ــ ۲۱، ۳۱
ــ حروف آغازی کلمات ۴۶، ۱۹۲
ــ حروف پایانی کلمات ۴۶، ۱۹۳
ــ حروف زبان صریح ۱۷، ۴۵، ۱۹۱

ـــ دوحرفیها ۵۳، ۱۸۹
ـــ سه‌حرفیها ۵۴، ۵۵
ـــ مشخصه ۱۹، ۱۴۵
ـــ نسبی ۱۸، ۷۰
فرایند زنجیره‌ای ۱۱۴

کازیسکی، فریدریش ۷۷
کلمات الگودار ۴۸
کلمهٔ احتمالی ۸۹، ۱۴۶، ۱۶۸
کلمهٔ کلیدی ۴۲، ۴۳، ۴۴، ۶۱
ـــ در رمز چندالفبایی ۶۴، ۶۵
ـــ در سیستم انتقال ستونی ۱۵۹
کلید ویژه ۱۴

ماتریس ۱۲۷
ـــ برگشتی ۱۴۰
دورهٔ تناوب ـــ ۱۴۰
ـــ همانی ۱۳۶
مانده(ها) ۸
ـــ در ضرب ۲۶
مجموعهٔ کامل ـــ ۸
متنهای رمزی روزنامه‌ای و مجله‌ای ۴۲ و ۵۲
مجموع ۱۹
حد بالای ـــ ۱۹
حد پایین ـــ ۱۹
مجموعهٔ کامل مانده‌ها ۸، ۲۵، ۲۶
مربع ویژنر ۱۳، ۶۴، ۹۰، ۱۱۲ و چند صفحهٔ بعد
مستطیل کاملاً پر ۱۶۰
مستطیل ناکامل ۱۶۶
معادلهٔ همنهشتی
جواب ـــ ۱۰ـ۱۱، ۲۷
معکوس عدد نسبت به ضرب ۲۸
مقدار تغییر مکان دنبالهٔ رمزی ← میزان انتقال دنبالهٔ رمزی
مقلوب‌سازی ۱۶۳
میزان انتقال دنبالهٔ رمزی ۱۱، ۱۲، ۲۰، ۲۳، ۴۱

ناهمواری
ـــ توزیع فراوانی ۷۰
شاخص ـــ ۷۲ و چندصفحهٔ بعد
نمادهای رمزی ۶۱، ۶۲

وارون عدد نسبت به ضرب ۲۸
وارون ماتریس ۱۳۰، ۱۳۲ و چندصفحهٔ بعد، ۱۳۶، ۱۳۷
وزنهای لگاریتمی ۸۴
ویژنر ۱۳، ۶۴

پیوست

برنامه‌های کامپیوتری ضمیمهٔ کتاب آشنایی با رمزگشایی نوشتهٔ آبراهام سینکوف

پال اروین

کالج دخترانهٔ رَندالف-مِیکن

فهرست پیوست

مقدمه ۲۰۷

۱. توزیع فراوانی سه‌حرفی ۲۰۹

۲. شاخص انطباق ۲۱۵

۳. تطبیق الفباها ۲۱۸

۴. توزیع فراوانی سه‌حرفی به‌ازای هریک از الفباهای یک رمز چندالفبایی تناوبی ۲۲۲

۵. توزیع فراوانی دوحرفی ۲۳۰

مقدمه

در طی چند تابستان گذشته، چند دوره درس رمزگشایی برای دانش‌آموزانی که در دبیرستان تیزهوشان ویرجینیا ثبت نام کرده بودند برگزار کردم. در این دوره‌ها از کتاب آشنایی با رمزگشایی نوشتهٔ پرفسور آبراهام سینکوف، به عنوان کتاب درسی استفاده کردیم. برای اینکه کاری کنم که دانش‌آموزان تا آنجا که ممکن است هم ریاضی بیاموزند و هم از درس لذت ببرند، چند برنامهٔ کامپیوتری تهیه کردم که بتوان بسیاری از کارهای معمول و گاهی خسته‌کننده‌ای را که در رمزگشایی پیام پیش می‌آیند با استفاده از این برنامه‌ها انجام داد. این برنامه‌ها، که دانش‌آموزان کلاسهای مختلف دبیرستان مذکور به خوبی از آنها استفاده کردند، در اینجا ارائه شده‌اند.

تمام برنامه‌ها به زبان بیسیک نوشته شده‌اند و حتی دانش‌آموزانی هم که هیچ اطلاعی از برنامه‌نویسی ندارند هنگامی که برنامه‌ها را وارد کامپیوتر کنند، می‌توانند از آنها استفاده کنند. این برنامه‌ها روی کامپیوتر DECSYSTEM-۲۰ مجهز به سیستم اشتراک زمانی درکالج رَندالف‌ـمِیکن اجرا شده‌اند. دقت شده که در آنها تنها از ویژگیهای متعارف بیسیک استفاده شود تا خواننده بتواند بدون هیچ تغییر و اصلاحی برنامه را درکامپیوتر خود وارد و اجرا کند. همچنین، با توجه به اینکه کامپیوترهای خانوادهٔ Hewlett-Packard به طریقی متفاوت روی آرایه‌های دنبالهٔ حروف عمل می‌کنند، برای آنکه مشکلی پیش نیاید، این برنامه‌ها به صورتی که درکامپیوترهای H-P قابل اجرا باشد نوشته شده و این صورت H-P به دنبال خروجی صورت DEC-20 آنها آورده شده است. استفاده کنندگان ازکامپیوترهای H-P باید توجه کنند که در زبان BASIC سازگار با H-P طول پیام به ۲۲۵ حرف محدود

می‌شود. آقای کارلو سِرنیوانی از دانشگاه نیویورک، مسئول تهیهٔ صورت H-Pی این برنامه‌ها بوده است و من مدیون زحمات او هستم.

از پروفسور سینکوف برای تشویقها و پیشنهادهایش در طول تهیهٔ این رساله سپاسگزارم. پروفسور انلی لکس و اعضای بخش کتب«ریاضیات پیش دانشگاهی» در کمیتهٔ انتشارات انجمن ریاضی امریکا نیز در تمام مدت تهیهٔ این رساله یار و مشوق من بوده‌اند.

پال اروین

لینچبرگ، ویرجینیا

۱. توزیع فراوانی سه‌حرفی

این برنامه تعداد حروف پیام و سپس خود پیام را در دسته‌های ده‌حرفی از شما می‌گیرد، و جدولی از سه‌حرفیها که بر حسب حرف وسطشان مرتب شده‌اند برایتان تهیه می‌کند. خروجی این برنامه شبیه جدولی است که در صفحهٔ ۵۶ از کتاب آشنایی بارمزگشایی[۱] آمده است. توزیع فراوانی سه‌حرفی، در مجموع، نموداری از فراوانی تک‌تک حروف ایجاد خواهد کرد.

۱. مقصود کتاب حاضر است. در این برنامه و سایر برنامه‌ها هر جا "ELEMENTARY CRYPTANALYSIS" آمده مقصود همین کتاب است. (م.)

```
00100 REM ************************************************************
00110 REM * PROGRAM TO GIVE TRIGRAPHIC FREQUENCY DISTRIBUTION TABLE *
00120 REM * OF MESSAGES AS ON PAGE 56 OF "ELEMENTARY CRYPTANALYSIS".*
00130 REM *      ARRAY A$( ) WILL HOLD THE ALPHABET IN NORMAL ORDER  *
00140 REM *      ARRAY M$( ) WILL HOLD THE LETTERS IN THE ENCIPHERED *
00150 REM *         MESSAGE                                          *
00160 REM *      N = NUMBER OF CHARACTERS IN THE MESSAGE             *
00170 REM ************************************************************
00180 REM
00190 REM
00200 PRINT " THIS PROGRAM GIVES THE TRIGRAPHIC DISTRIBUTION TABLE "
00210 PRINT " OF MESSAGES AS ON PAGE 56 OF ELEMENTARY CRYPTANALYSIS."
00220 PRINT
00230 PRINT
00240 DIM A$(26),M$(500)
00250 REM
00260 REM ********************READY TO READ IN ARRAY A$( )************
00270 REM
00280 DATA A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
00290 FOR I = 1 TO 26
00300   READ A$(I)
00310 NEXT I
00320 REM
00330 REM ***************** READY TO INPUT N ************************
00340 REM
00350 PRINT "WHEN YOU SEE THE QUESTION MARK, ENTER THE NUMBER OF "
00360 PRINT " LETTERS IN THE MESSAGE, THEN PRESS THE RETURN KEY "
00370 INPUT N
00380 REM
00390 REM **** READY TO LOAD DUMMY CHARACTER "*" INTO BEGINNING AND *
00400 REM **** END OF THE MESSAGE ************************************
00410 REM
00420 LET M$(0) = "*"
00430 LET M$(N+1) = "*"
00440 REM
00450 REM **** THERE ARE NOW N+2 CHARACTERS IN THE MESSAGE **********
00460 REM
00470 REM **** READY TO INPUT THE MESSAGE IN P GROUPS OF 10 LETTERS**
00480 REM **** THEN THE FINAL N - P*10 LETTERS **********************
00490 REM
00500 LET P = INT(N/10)
00510 LET R = N - P*10
00520 PRINT "WHEN YOU SEE THE ? ENTER A GROUP OF TEN LETTERS IN THE  "
00530 PRINT "MESSAGE, SEPARATED BY COMMAS, THEN PRESS RETURN "
00540 FOR I = 0 TO P-1
00550   FOR K = 1 TO 10
00560           INPUT M$(I*10 + K),
00570   NEXT K
00580 NEXT I
00590 PRINT "NOW INPUT THE LAST ";R;" LETTERS SEPARATED BY COMMAS "
00600 FOR K = 1 TO R
00610   INPUT M$(P*10 + K),
00620 NEXT K
00630 REM
```

```
00640 REM *****READY TO PRINT OUT MESSAGE IN GROUPS OF 5 LETTERS ****
00650 REM *********** WITH 9 GROUPS PER LINE ************************
00660 REM
00670 PRINT "      THE CIPHER MESSAGE IS     "
00680 PRINT
00690 PRINT
00700 FOR I = 1 TO N
00710   PRINT M$(I);
00720   IF(I/5 <> INT(I/5)) THEN 740
00730   PRINT " ";
00740   IF (I/45 <> INT(I/45)) THEN 760
00750   PRINT
00760 NEXT I
00770 REM ***************************************************************
00780 REM * FOR EACH LETTER OF THE ALPHABET, A$(I), THE PROGRAM         *
00790 REM * SCANS THE ARRAY  M$( )  FOR EACH OCCURRENCE OF A$(I).       *
00800 REM * IF IT FINDS A$(I) IN THE MESSAGE AS M$(J), IT STORES THE   *
00810 REM * PRECEDING LETTER, M$(J-1), IN T$(L) AND THE FOLLOWING      *
00820 REM * LETTER, M$(J+1), IN T$(L+1). L IS THEN INCREASED BY 2.     *
00830 REM * THE ARRAY T$( ) IS THEN PRINTED IN PAIRS, THUS PRODUCING   *
00840 REM * THE LIST OF TRIGRAPHS CORRESPONDING TO A$(I). I IS THEN    *
00850 REM * INCREASED BY 1 AND THE ENTIRE PROCESS IS REPEATED.         *
00860 REM *  L1 = TOTAL NUMBER OF CHARACTERS IN T$( ) AFTER COMPLETE   *
00870 REM *       SCAN OF MESSAGE FOR ALL OCCURRENCES OF A$(I).       *
00880 REM ***************************************************************
00890 PRINT
00900 PRINT
00910 PRINT
00920 PRINT "      THE TABLE OF TRIGRAPHS IS "
00930 PRINT
00940 PRINT
00950 DIM T$(60)
00960 REM
00970 REM **** READY TO BEGIN SCAN OF MESSAGE FOR EACH OCCURRENCE OF A$(I) ****
00980 REM
00990 FOR I = 1 TO 26
01000   LET L = 1
01010   FOR J = 1 TO N
01020           IF(M$(J) <> A$(I)) THEN 1060
01030           LET T$(L) = M$(J-1)
01040           LET T$(L+1) = M$(J+1)
01050           LET L = L + 2
01060   NEXT J
01070 REM
01080 REM ***** READY TO PRINT OUT A$(I), AND T$( ) IF L1 IS NOT ZERO*
01090 REM
01100   LET L1 = L -1
01110   PRINT A$(I);":";
01120   IF (L1 = 0) THEN 1170
01130   PRINT " ";
01140   FOR L = 1 TO L1 STEP 2
01150           PRINT T$(L);T$(L+1);" ";
01160   NEXT L
01170   PRINT
01180 NEXT I
01190 END
```

```
 THIS PROGRAM GIVES THE TRIGRAPHIC DISTRIBUTION TABLE
 OF MESSAGES AS ON PAGE 56 OF ELEMENTARY CRYPTANALYSIS.


WHEN YOU SEE THE QUESTION MARK, ENTER THE NUMBER OF
 LETTERS IN THE MESSAGE, THEN PRESS THE RETURN KEY
 ? 121
WHEN YOU SEE THE ? ENTER A GROUP OF TEN LETTERS IN THE
MESSAGE, SEPARATED BY COMMAS, THEN PRESS RETURN
 ? M,Y,T,K,I,J,I,R,U,L
 ? A,Z,O,A,H,M,I,J,A,C
 ? U,Y,G,I,I,J,I,U,J,A
 ? C,H,E,T,R,J,M,R,U,Y
 ? M,J,F,A,G,R,M,R,P,J
 ? F,T,M,E,X,A,L,A,Z,U
 ? Y,M,R,Q,M,O,A,Z,E,X
 ? O,A,Z,R,U,A,R,T,R,I
 ? T,G,E,L,G,I,J,H,A,R
 ? J,I,T,J,U,A,V,Y,M,O
 ? Y,V,T,L,V,I,F,M,P,Y
 ? U,X,I,O,M,X,I,U,A,P
NOW INPUT THE LAST  1  LETTERS SEPARATED BY COMMAS
 ? A
      THE CIPHER MESSAGE IS


MYTKI JIRUL AZOAH MIJAC UYGII JIUJA CHETR JMRUY MJFAG
RMRPJ FTMEX ALAZU YMRQM OAZEX OAZRU ARTRI TGELG IJHAR
JITJU AVYMO YVTLV IFMPY UXIOM XIUAP A


     THE TABLE OF TRIGRAPHS IS


A: LZ OH JC JC FG XL LZ OZ OZ UR HR UV UP P*
B:
C: AU AH
D:
E: HT MX ZX GL
F: JA JT IM
G: YI AR TE LI
H: AM CE JA
I: KJ JR MJ GI IJ JU RT GJ JT VF XO XU
J: II IA II UA RM MF PF IH RI TU
K: TI
L: UA AA EO TV
M: *Y HI JR YJ RR TE YR QO YO FP OX
N:
O: ZA MA XA MY IM
P: RJ MY AA
Q: RM
R: IU TJ MU GM MP MQ ZU AT TI AJ
S:
T: YK ER FM RR IG IJ VL
U: RL CY IJ RY ZY RA JA YX IA
V: AY YT LI
W:
X: EA EO UI MI
Y: MT UG UM UM VM OV PU
Z: AO AU AE AR
```

PROG1

```
10  PRINT "this program gives the trigraphic distribution table"
20  PRINT "of messages as on page 56 of elementary cryptanalysis."
30  PRINT LIN(2);"when you see the question mark, enter the number of letters"
40  REM *************** INPUT VALUE FOR N ******************************
50  INPUT N
60  PRINT LIN(2)
70  DIM A$[26],M$[255],T$[60]
80  REM
90  REM ******************* initailize a$ string to alphabet chars. ****
100  A$="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
110  REM
120  REM **** ready to load dummy character "*" into beginning and ***
130  REM **** end of the message  ***************************************
140  REM
150  FOR I=1 TO 255
160  M$[I,I]=" "
170  NEXT I
180  M$[1,1]="*"
190  M$[N+1,N+1]="*"
200  REM
210  REM *** there are now n+2 characters in the message *************
220  REM *** ready to input the message in p groups of 10 letters ****
230  REM *** then the final n - p*10 letters ************************
240  P=INT(N/10)
250  R=N-P*10
260  PRINT "when you see the ? enter one group of 10 letters,then press return."
270  FOR I=0 TO P-1
280  INPUT M$[I*10+1,I*10+10]
290  NEXT I
300  M$=UPS$(M$)
310  PRINT "now input the last ";R;"letters separated by commas"
320  FOR K=1 TO R
330  INPUT M$[P*10+K,P*10+K]
340  NEXT K
350  M$=UPS$(M$)
360  REM ******** ready to print out message in groups of 5 letters *****
370  REM ***************** with 9 groups per line **********************
380  PRINT "        the coded message is";LIN(2)
390  FOR I=1 TO N
400  PRINT M$[I,I];
410  IF (I/5#INT(I/5)) THEN 430
420  PRINT " ";
430  IF (I/45#INT(I/45)) THEN 450
440  PRINT
450  NEXT I
460  REM
470  REM
480  REM
490  PRINT LIN(3);"       the table of trigraphs is ";LIN(2)
```

```
500  REM
510  REM ****** ready to begin scan of message for each occurrence of a$(i,i)
520  REM
530  FOR I=1 TO 26
540  L=1
550  FOR J=2 TO N
560  IF M$[J,J]$A$[I,I] THEN 600
570  T$[L,L]=M$[J-1,J-1]
580  T$[L+1,L+1]=M$[J+1,J+1]
590  L=L+2
600  NEXT J
610  REM
620  REM *** ready to print out a$(i,i) and t$(l,l) if l1 is not zero ***
630  REM ***
640  L1=L-1
650  PRINT A$[I,I];":";
660  IF (L1=0) THEN 710
670  PRINT " ";
680  FOR L=1 TO L1 STEP 2
690  PRINT T$[L,L];T$[L+1,L+1];" ";
700  NEXT L
710  PRINT
720  NEXT I
730  END
```

۲. شاخص انطباق

این برنامه فراوانی حروف پیام را می‌گیرد و شاخص انطباق را مطابق تعریف صفحهٔ ۷۵ ازکتاب آشنایی با رمزگشایی محاسبه می‌کند.

```
00100 REM ****************************************************************
00110 REM * THIS PROGRAM COMPUTES THE INDEX OF COINCIDENCE FOR A GIVEN *
00120 REM * FREQUENCY DISTRIBUTION AS DISCUSSED ON PAGE 75 OF          *
00130 REM * ELEMENTARY CRYPTANALYSIS .                                 *
00140 REM *      A$( ) HOLDS THE ALPHABET IN NORMAL ORDER.             *
00150 REM *      F( ) HOLDS THE FREQUENCIES OF THE LETTERS OF THE      *
00160 REM *           ALPHABET IN THE MESSAGE.                         *
00170 REM *      T IS A VARIABLE FOR THE SUM OF THE FREQUENCIES        *
00180 REM *      S IS USED FOR THE SUM IN THE NUMERATOR OF THE INDEX   *
00190 REM *          OF COINCIDENCE FORMULA.                          *
00200 REM *      C IS THE INDEX OF COINCIDENCE.                        *
00210 REM ****************************************************************
00220 REM
00230 REM **********READY TO READ THE ALPHABET INTO ARRAY A$( )********
00240 REM
00250 DIM F(26),A$(26)
00260 DATA A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
00270 FOR I = 1 TO 26
00280   READ A$(I)
00290 NEXT I
00300 PRINT
00310 PRINT "THIS PROGRAM ASKS FOR THE FREQUENCIES OF LETTERS AS INPUT "
00320 PRINT " AND COMPUTES THE INDEX OF COINCIDENCE. "
00330 PRINT
00340 PRINT
00350 REM ******* ASK FOR INPUT OF FREQUENCIES *************************
00360 REM
00370 PRINT "INPUT THE FREQUENCIES OF "
00380 FOR I = 1 TO 10
00390   PRINT A$(I);",";
00400 NEXT I
00410 PRINT "    SEPARATED BY COMMAS, THEN PRESS RETURN
00420 FOR I = 1 TO 10
00430   INPUT F(I),
00440 NEXT I
00450 PRINT
00460 PRINT " DO THE SAME FOR "
00470 FOR I = 11 TO 20
00480   PRINT A$(I);",";
00490 NEXT I
00500 PRINT
00510 FOR I = 11 TO 20
00520   INPUT F(I),
00530 NEXT I
00540 PRINT
00550 PRINT "DO THE SAME FOR "
00560 FOR I = 21 TO 26
00570   PRINT A$(I);",";
00580 NEXT I
00590 PRINT
00600 FOR I = 21 TO 26
00610   INPUT F(I),
00620 NEXT I
00630 PRINT
00640 REM
```

```
00650 REM ****** READY TO COMPUTE INDEX OF COINCIDENCE ******************
00660 LET S = 0
00670 LET T = 0
00680 FOR I = 1 TO 26
00690   LET S = S +F(I)*(F(I)-1)
00700   LET T = T + F(I)
00710 NEXT I
00720 LET C = S/(T*(T-1))
00730 PRINT "THE INDEX OF COINCIDENCE IS  ",C
00740 END

RUNNH

THIS PROGRAM ASKS FOR THE FREQUENCIES OF LETTERS AS INPUT
 AND COMPUTES THE INDEX OF COINCIDENCE.


INPUT THE FREQUENCIES OF
A,B,C,D,E,F,G,H,I,J,    SEPARATED BY COMMAS, THEN PRESS RETURN
 ? 1,3,1,1,5,0,0,0,3,1

 DO THE SAME FOR
K,L,M,N,O,P,Q,R,S,T,
 ? 1,6,2,6,3,1,5,13,5,2

DO THE SAME FOR
U,V,W,X,Y,Z,
 ? 1,15,6,0,18,0

THE INDEX OF COINCIDENCE IS                0.08699237


PROG2

10  REM   prog II
20  REM
30  DIM F[26],A$[26]
40  A$="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
50  PRINT LIN(2);"this prog. asks for the frequencies of letters as input"
60  PRINT "and computes the index of coincidence.";LIN(2)
70  PRINT "input the frequencies of the following letters:"
80  FOR I=1 TO 26
90  PRINT A$[I,I];" occurs";
100   INPUT F[I]
110  NEXT I
120  REM ***** ready to compute index of coincidence ****
130  S=T=0
140  FOR I=1 TO 26
150  S=S+F[I]*(F[I]-1)
160  T=T+F[I]
170  NEXT I
180  C=S/(T*(T-1))
190  PRINT "the index of coincidence is ";C
200  END
```

۳. تطبیق الفباها

در حالت رمزنگاری چندالفبایی مبتنی بر مربع ویژنر، می‌خواهیم بدانیم که هر دو الفبا از الفباهای رمزنگاری در چه وضعیتی با یکدیگر مطابقت می‌کنند. ۲۶ وضعیت ممکن وجود دارد. این برنامه فراوانی حروف مربوط به هر یک از این دو الفبا را می‌گیرد و کار تطبیق الفباها را همان‌طور که در بخش ۶.۳ (صفحهٔ ۹۵) از کتاب آشنایی با رمزگشایی شرح داده شده انجام می‌دهد.

```
00100 REM ************************************************************
00110 REM * PROGRAM TO PERFORM TECHNIQUE OF MATCHING ALPHABETS AS ON  *
00120 REM * PAGE 95 OF ELEMENTARY CRYPTANALYSIS.                      *
00130 REM *     A$( ) HOLDS THE ALPHABET IN NORMAL ORDER.            *
00140 REM *     F( ) HOLDS THE FREQUENCIES OF ALPHABET 1.            *
00150 REM *     F1( ) HOLDS THE FREQUENCIES OF ALPHABET 2.           *
00160 REM *     S IS THE SUM OF THE PRODUCTS F( )*F1( )              *
00170 REM ************************************************************
00180 REM
00190 REM **** READY TO READ THE ALPHABET INTO THE ARRAY A$( ) *******
00200 REM
00210 DIM A$(26),F(26),F1(26)
00220 DATA A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
00230 FOR I = 1 TO 26
00240   READ A$(I)
00250 NEXT I
00260 PRINT
00270 PRINT
00280 PRINT "THIS PROGRAM PERFORMS THE TECHNIQUE OF MATCHING ALPHABETS"
00290 PRINT
00300 PRINT
00310 REM ***** ASK FOR INPUT OF FREQUENCIES OF FIRST ALPHABET *******
00320 PRINT
00330 PRINT "FOR THE FIRST DISTRIBUTION "
00340 PRINT "INPUT THE FREQUENCIES OF "
00350 FOR I = 1 TO 13
00360   PRINT A$(I);",";
00370 NEXT I
00380 PRINT
00390 PRINT "SEPARATED BY COMMAS, THEN PRESS RETURN "
00400 FOR I = 1 TO 13
00410   INPUT F(I),
00420 NEXT I
00430 PRINT
00440 PRINT "NOW DO THE SAME FOR "
00450 FOR I = 14 TO 26
00460   PRINT A$(I);",";
00470 NEXT I
00480 PRINT
00490 FOR I = 14 TO 26
00500   INPUT F(I),
00510 NEXT I
00520 PRINT
00530 REM ***** ASK FOR INPUT OF FREQUENCIES OF SECOND ALPHABET ******
00540 REM
00550 PRINT "NOW DO EXACTLY THE SAME THING FOR THE SECOND DISTRIBUTION "
00560 FOR I = 1 TO 13
00570   INPUT F1(I),
00580 NEXT I
00590 FOR I = 14 TO 26
00600   INPUT F1(I),
00610 NEXT I
```

```
00620 REM
00630 REM ************  READY TO COMPUTE THE SUMS *****************
00640 REM
00650 PRINT
00660 PRINT
00670 PRINT " SUM OF F*F' FOR A OF "
00680 PRINT " ALPHABET 1 AGAINST   "
00690 PRINT " INDICATED LETTER OF "
00700 PRINT "   OF ALPHABET 2"
00710 PRINT "------------------------"
00720 FOR K = 0 TO 25
00730   LET S = 0
00740   FOR I = 1 TO 26
00750           IF I+K > 26 THEN 780
00760           LET S = S + F(I)*F1(I+K)
00770           GO TO 790
00780           LET S = S + F(I)*F1(I+K-26)
00790   NEXT I
00800   PRINT A$(K+1),S
00810 NEXT K
00820 END
```

```
RUNNH

THIS PROGRAM PERFORMS THE TECHNIQUE OF MATCHING ALPHABETS


FOR THE FIRST DISTRIBUTION
INPUT THE FREQUENCIES OF
A,B,C,D,E,F,G,H,I,J,K,L,M,
SEPARATED BY COMMAS, THEN PRESS RETURN
 ? 3,4,5,1,3,2,1,0,2,0,0,0,5

NOW DO THE SAME FOR
N,O,P,Q,R,S,T,U,V,W,X,Y,Z,
 ? 4,0,4,1,1,6,1,3,6,0,4,0,5

NOW DO EXACTLY THE SAME THING FOR THE SECOND DISTRIBUTION
 ? 2,2,1,1,2,1,0,0,0,10,0,0,4
 ? 1,5,6,1,1,4,0,4,1,5,2,2,6
```

```
 SUM OF F*F' FOR A OF
 ALPHABET 1 AGAINST
 INDICATED LETTER OF
   OF ALPHABET 2
-------------------------
A                 158
B                 129
C                 161
D                 122
E                 139
F                 136
G                 100
H                 169
I                 128
J                 124
K                 187
L                 87
M                 161
N                 138
O                 161
P                 138
Q                 107
R                 172
S                 129
T                 122
U                 185
V                 136
W                 149
X                 234
Y                 97
Z                 152
```

PROG3

```
10  REM   pros III
20  REM
30  DIM A$[26],F[26],G[26]
40  A$="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
50  PRINT LIN(2);"this program performs the technique of matching alphabets";LI
60  PRINT "for the first and second distribution inputted frequencies."
70  FOR I=1 TO 26
80  PRINT A$[I,I];" first , second:"
90  INPUT F[I],G[I]
100  NEXT I
110  REM
120  REM ************ ready to compute the sums ***************
130  REM
140  PRINT LIN(2);" sum of f*f' for a of"
150  PRINT " alphabet 1 against"
160  PRINT " indicated letter of "
170  PRINT "   of alphabet 2"
180  PRINT "-----------------------------"
190  FOR K=0 TO 25
200  S=0
210  FOR I=1 TO 26
220  IF I+K>26 THEN 250
230  S=S+F[I]*G[I+K]
240  GOTO 260
250  S=S+F[I]*G[I+K-26]
260  NEXT I
270  PRINT A$[K+1,K+1],S
280  NEXT K
290  END
```

۴. توزیع فراوانی سه‌حرفی به‌ازای هر یک از الفباهای یک رمز چندالفبایی تناوبی

در یک رمزنگاری چندالفبایی که در آن به‌نوبت از چند الفبا استفاده می‌شود، می‌خواهیم توزیع فراوانی سه‌حرفیِ حروفِ مربوط به هر یک از این الفباها را بیابیم. این برنامه تعداد حروف پیام و سپس خود پیام را در دسته‌های ده‌حرفی و سپس تعداد الفباهای به‌کار رفته در رمزنگاری را می‌گیرد. سپس به‌ازای هر یک از الفباهای رمزنگاری یک جدول توزیع فراوانی سه‌حرفی ایجاد می‌کند. خروجی این برنامه را می‌توان برای رسم نمودار فراوانی حروفِ مربوط به هریک از الفباها به کار برد، مانند آنچه در ضفحهٔ ۸۰ ازکتاب آشنایی با رمزگشایی آمده است.

```
00100 REM ************************************************************
00110 REM * PROGRAM TO PERFORM TRIGRAPHIC FREQUENCY DISTRIBUTIONS OF *
00120 REM * THE INDIVIDUAL ALPHABETS OF A PERIODIC POLYALPHABETIC     *
00130 REM * CIPHER. THE MESSAGE ON PAGE 68 OF "ELEMENTARY CRYPT-     *
00140 REM * ANALYSIS" WILL BE USED AS AN EXAMPLE.                     *
00150 REM *      ARRAY A$( ) WILL HOLD THE ALPHABET IN NORMAL ORDER.  *
00160 REM *      ARRAY M$( ) WILL HOLD THE LETTERS OF THE ENCIPHERED  *
00170 REM *            MESSAGE.                                      *
00180 REM *      N = THE NUMBER OF CHARACTERS IN THE MESSAGE.         *
00190 REM * IF N1 ALPHABETS WERE USED PERIODICALLY TO ENCIPHER THE    *
00200 REM * MESSAGE, THEN LETTERS 1, N1+1,2*N1+1, 3*N1+1...          *
00210 REM * WERE ENCIPHERED USING THE SAME ALPHABET. THESE ARE STORED*
00220 REM * IN THE ARRAY C$( ) AND A TRIGRAPHIC FREQUENCY DISTRIBU-  *
00230 REM * TION PERFORMED. THE PROCESS IS THEN REPEATED FOR LETTERS *
00240 REM * 2, N1+2, 2*N1+2, 3*N1+2...WHICH WERE ENCIPHERED USING    *
00250 REM * THE SECOND OF THE N1 ALPHABETS. THE PROCESS ENDS WHEN    *
00260 REM * LETTERS N1, 2*N1, 3*N1...HAVE BEEN USED TO PRODUCE A TRI-*
00270 REM * GRAPHIC FREQUENCY DISTRIBUTION.                          *
00280 REM ************************************************************
00290 REM
00300 DIM A$(26),M$(500)
00310 REM
00320 REM **********************READY TO READ IN ARRAY A$( )*******
00330 REM
00340 DATA A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
00350 FOR I = 1 TO 26
00360   READ A$(I)
00370 NEXT I
00380 REM
00390 REM ****************** READY TO INPUT N ********************
00400 REM
00410 PRINT "WHEN YOU SEE THE QUESTION MARK, ENTER THE NUMBER OF "
00420 PRINT " LETTERS IN THE MESSAGE, THEN PRESS THE RETURN KEY "
00430 INPUT N
00440 PRINT
00450 PRINT
00460 REM
00470 REM
00480 REM **** READY TO INPUT THE MESSAGE IN P GROUPS OF 10 LETTERS**
00490 REM **** THEN THE FINAL N - P*10 LETTERS ***********************
00500 REM
00510 LET P = INT(N/10)
00520 LET R = N - P*10
00530 PRINT "WHEN YOU SEE THE ? ENTER A GROUP OF TEN LETTERS IN THE
00540 PRINT "MESSAGE, SEPARATED BY COMMAS, THEN PRESS RETURN "
00550 FOR I = 0 TO P-1
00560   FOR K = 1 TO 10
00570         INPUT M$(I*10 + K),
00580   NEXT K
00590 NEXT I
00600 PRINT "NOW INPUT THE LAST ";R;" LETTERS SEPARATED BY COMMAS "
00610 FOR K = 1 TO R
00620   INPUT M$(P*10 + K),
00630 NEXT K
00640 PRINT
00650 PRINT
```

```
00660 REM
00670 REM *****READY TO PRINT OUT MESSAGE IN GROUPS OF 5 LETTERS ****
00680 REM ********** WITH 9 GROUPS PER LINE ************************
00690 REM
00700 PRINT '       THE CIPHER MESSAGE IS '
00710 PRINT
00720 PRINT
00730 FOR I = 1 TO N
00740   PRINT M$(I);
00750   IF(I/5 <> INT(I/5)) THEN 770
00760   PRINT ' ';
00770   IF (I/45 <> INT(I/45)) THEN 790
00780   PRINT
00790 NEXT I
00800 REM
00810 REM
00820 PRINT
00830 PRINT
00840 REM ***** READY TO INPUT N1, THE NUMBER OF ALPHABETS USED ****
00850 PRINT  'INPUT THE NUMBER OF ALPHABETS USED TO ENCIPHER THE MESSAGE'
00860 INPUT N1
00870 REM ***************************************************************
00880 REM * FOR EACH K BETWEEN 1 AND N1, EVERY N1-TH LETTER BEGINNING*
00890 REM *  WITH LETTER NUMBER K IS STORED IN THE ARRAY C$( ).       *
00900 REM *    M1 = THE NUMBER OF LETTERS IN THE ARRAY C$( ).        *
00910 REM *          (M1 DEPENDS ON THE VALUE OF K)                  *
00920 REM * AFTER M1 HAS BEEN DETERMINED, THE DUMMY CHARACTER '*' IS *
00930 REM * LOADED INTO THE FIRST AND LAST POSITIONS OF ARRAY C$( ). *
00940 REM * A TRIGRAPHIC FREQUENCY DISTRIBUTION IS THEN PERFORMED ON *
00950 REM * C$( ). K IS THEN INCREASED BY 1.                         *
00960 REM ***************************************************************
00970 DIM C$(250)
00980 FOR K = 1 TO N1
00990   LET M1 = INT(N/N1)
01000   IF K + M1*N1 > N THEN 1020
01010   LET M1 = M1 + 1
01020   FOR J = 1 TO M1
01030           LET C$(J) = M$(K+(J-1)*N1)
01040   NEXT J
01050   LET C$(0) = '*'
01060   LET C$(M1+1) = '*'
```

```
01070 REM ************************************************************
01080 REM * FOR EACH LETTER OF THE ALPHABET, A$(I), THE PROGRAM       *
01090 REM * SCANS THE ARRAY  C$( )  FOR EACH OCCURRENCE OF A$(I).     *
01100 REM * IF IT FINDS A$(I) IN THE MESSAGE AS C$(J), IT STORES THE *
01110 REM * PRECEDING LETTER, C$(J-1),IN  T$(L) AND THE FOLLOWING     *
01120 REM * LETTER, C$(J+1), IN T$(L+1). L IS THEN INCREASED BY 2.    *
01130 REM * THE ARRAY T$( ) IS THEN PRINTED IN PAIRS, THUS PRODUCING *
01140 REM * THE LIST OF TRIGRAPHS CORRESPONDING TO A$(I). I IS THEN  *
01150 REM * INCREASED BY 1 AND THE ENTIRE PROCESS IS REPEATED.       *
01160 REM *  L1 = TOTAL NUMBER OF CHARACTERS IN T$( ) AFTER COMPLETE *
01170 REM *         SCAN OF MESSAGE FOR ALL OCCURRENCES OF A$(I).    *
01180 REM ************************************************************
01190 PRINT
01200 PRINT
01210 PRINT
01220 PRINT '        THE TABLE OF TRIGRAPHS FOR ALPHABET ';K;' IS'
01230 PRINT
01240 PRINT
01250 DIM T$(60)
01260 REM
01270 REM **** READY TO BEGIN SCAN OF MESSAGE FOR EACH OCCURRENCE OF A$(I)***
01280 REM
01290 FOR I = 1 TO 26
01300   LET L = 1
01310   FOR J = 1 TO M1
01320             IF(C$(J) <> A$(I)) THEN 1360
01330             LET T$(L) = C$(J-1)
01340             LET T$(L+1) = C$(J+1)
01350             LET L = L + 2
01360   NEXT J
01370 REM
01380 REM ***** READY TO PRINT OUT A$(I), AND T$( ) IF L1 IS NOT ZERO*
01390 REM
01400   LET L1 = L -1
01410   PRINT A$(I);':';
01420   IF (L1 = 0) THEN 1470
01430   PRINT ' ';
01440   FOR L = 1 TO L1 STEP 2
01450             PRINT T$(L);T$(L+1);' ';
01460   NEXT L
01470   PRINT
01480 NEXT I
01490 NEXT K
01500 END
```

```
RUNNH
WHEN YOU SEE THE QUESTION MARK, ENTER THE NUMBER OF
 LETTERS IN THE MESSAGE, THEN PRESS THE RETURN KEY
 ? 268


WHEN YOU SEE THE ? ENTER A GROUP OF TEN LETTERS IN THE
MESSAGE, SEPARATED BY COMMAS, THEN PRESS RETURN
 ? A,P,W,V,C,D,K,P,A,K
 ? B,C,E,C,Y,W,X,B,B,K
 ? C,Y,V,S,E,F,V,T,L,V
 ? M,X,G,R,G,K,K,G,F,D
 ? L,R,L,Z,K,T,F,V,K,H
 ? S,A,G,U,K,Y,E,X,S,R
 ? S,I,Q,T,W,J,X,V,F,L
 ? L,A,L,U,I,K,Y,A,B,Z
 ? X,G,R,K,L,B,A,F,S,J
 ? C,C,M,J,T,Z,D,G,S,T
 ? A,H,B,J,M,M,L,G,E,Z
 ? R,P,Z,I,J,X,P,V,G,U
 ? O,J,X,H,L,P,U,M,V,M
 ? C,K,Y,E,X,S,R,S,I,Q
 ? K,C,W,M,C,K,F,L,Q,J
 ? F,W,J,R,H,S,W,L,O,X
 ? Y,P,V,K,M,H,Y,C,T,A
 ? W,E,J,V,Q,D,P,A,V,V
 ? K,F,L,K,G,F,D,L,R,L
 ? Z,K,I,W,T,I,B,X,S,G
 ? R,T,P,L,L,A,M,H,F,R
 ? O,M,E,M,V,Z,Q,Z,G,K
 ? M,S,D,F,H,A,T,X,S,E
 ? E,L,V,W,K,O,C,J,F,Q
 ? F,L,H,R,J,S,M,V,M,V
 ? I,M,B,O,Z,H,I,K,R,O
NOW INPUT THE LAST  8  LETTERS SEPARATED BY COMMAS
 ? M,U,H,I,E,R,Y,G


     THE CIPHER MESSAGE IS


APWVC DKPAK BCECY WXBBK CYVSE FVTLV MXGRG KKGFD LRLZK
TFVKH SAGUK YEXSR SIQTW JXVFL LALUI KYABZ XGRKL BAFSJ
CCMJT ZDGST AHBJM MLGEZ RPZIJ XPVGU OJXHL PUMVM CKYEX
SRSIQ KCWMC KFLQJ FWJRH SWLOX YPVKM HYCTA WEJVQ DPAVV
KFLKG FDLRL ZKIWT IBXSG RTPLL AMHFR OMEMV ZQZGK MSDFH
ATXSE ELVWK OCJFQ FLHRJ SMVMV IMBOZ HIKRO MUHIE RYG

INPUT THE NUMBER OF ALPHABETS USED TO ENCIPHER THE MESSAGE
 ? 2
```

THE TABLE OF TRIGRAPHS FOR ALPHABET 1 IS

A: *W KB LS SB
B: AE XC YX AM TS IZ
C: WK BV SM VY WF KF
D: TS GR MH
E: BY VV KS LR OV SV HY
F: KL KK XL CQ QJ MO CF FH
G: MG GK SK PO LD QM
H: JW DT FJ ME
I: LY RK ZT MB ZR
J: ZP FH WQ HM
K: CA GF LF FS GE IW VL VC
L: VM FL LK FL LI RA ME XU KG PM
M: LG CT BL VY LF GD JM MI RH
N:
O: GX WY FE
P: JG QV RL
Q: SW FF JP VG
R: XL EZ XI DZ SP IM
S: KG ES SQ AC DA BR TE
T: MD YW IB HS
U: LV
V: CE EL UC YM PK EQ EK
W: AC QX KC HO TJ
X: YB WF BR OL YR
Y: EX IB CX OV MT E*
Z: RJ RI BI

THE TABLE OF TRIGRAPHS FOR ALPHABET 2 IS

A: HU LU KZ CE DV LH FX
B: WK KF
C: KC CW JJ QM HA
D: VP GR VA
E: KS AV XL
F: ST BJ VK KL SA
G: KD ZK ZT MZ XT R*
H: VA TJ JP KC AR OK
I: RT PX WX UR
J: TV FC CZ HM UH LW OQ
K: PC BY RG UA GB ME ML PH FF LW ZS HO
L: VA KJ SX FL LK TA EW QR
M: JG PM MK CK RM MZ VO
N:
O: WJ MH KU
P: *V DK ZI HM XK
Q: SC JL
R: XK DZ XI WS HM LS IG
S: YF ES SQ RL KF RV
T: FV ZV IJ GH GL
U: AY AK VJ OI
V: PD TX TH JL XU ED AF SV VM
W: CB JR KI LO
X: VR YR IV LP IG AE
Y: KS UX
Z: RT AG JG GP MZ ZK

PROG4

```
10  DIM A$[26],C$[250],M$[255],T$[60]
20  REM *** initialize a$ ******
30  A$="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
40  REM *** ready to input n ****
50  PRINT "when you see the question mark, enter the number of "
60  PRINT " letters in the message, then press the return key"
70  INPUT N
80  PRINT LIN(2)
90  REM
100  REM **** ready to input the message in p groups of 10 letters**
110  REM **** then the final n   p*10 letters **********************
120  P=INT(N/10)
130  R=N-P*10
140  PRINT "when you seee the ? enter a group of ten letters in the "
150  PRINT "message, no blanks or commas between letters, then press return"
160  FOR I=0 TO P-1
170  INPUT M$[I*10+1,I*10+10]
180  NEXT I
190  IF R=0 THEN 220
200  PRINT "now input the last ";R;" letters separated by nothing ... as before"
210  INPUT M$[P*10+1,P*10+R]
220  M$=UPS$(M$)
230  PRINT LIN(2)
240  REM *** ready to print out message in groups of 5 letters **
250  REM **********with 9 groups per line ************************
260  PRINT "           the coded message is"
270  PRINT LIN(2)
280  FOR I=1 TO N
290  PRINT M$[I,I];
300  IF I/5=INT(I/5) THEN 320
310  PRINT " ";
320  IF I/45=INT(I/45) THEN 340
330  PRINT
340  NEXT I
```

```
350  REM ***** ready to input n1, the number of alphabets used ****
360  PRINT "input the number of alphabets used to  encipher the message"
370  INPUT N1
380  REM
390  REM
400  REM
410  FOR K=1 TO N1
420  M1=INT(N/N1)
430  IF K+M1*N1>N THEN 450
440  M1=M1+1
450  FOR J=1 TO M1
460  C$[J,J]=M$[K+(J-1)*N1,K+(J-1)*N1]
470  NEXT J
480  C$[1,1]="*"
490  C$[M1+1,M1+1]="*"
500  REM
510  REM
520  PRINT LIN(2);"         the table of trigraphs for alphabet ";K;" is";LIN
530  REM******** ready to  begin search for a$(i,i) ************
540  FOR I=1 TO 26
550  L=1
560  FOR J=1 TO M1
570  IF C$[J,J]$A$[I,I] THEN 610
580  T$[L,L]=C$[J-1,J-1]
590  T$[L+1,L+1]=C$[J+1,J+1]
600  L=L+2
610  NEXT J
620  REM **** ready to print out a$(i,i) and t$( ) if l1 is not zero ***
630  L1=L-1
640  PRINT A$[I,I];":";
650  IF L1=0 THEN 700
660  PRINT " ";
670  FOR L=1 TO L1 STEP 2
680  PRINT T$[L,L];T$[L+1,L+1];" ";
690  NEXT L
700  PRINT
710  NEXT I
720  NEXT K
730  END
```

۵. توزیع فراوانی دوحرفی

این برنامه تعداد حروف پیام و سپس خود پیام را در دسته‌های بیست‌حرفی می‌گیرد و سپس یک آرایهٔ ۲۶ × ۲۶ تولید می‌کند که در آن تعداد دفعات ظهور هر دوحرفی در پیام آمده است.

```
00100 REM ************************************************************************
00110 REM * PROGRAM TO CONSTRUCT A DIGRAPHIC FREQUENCY TABLE AS ON PAGE  *
00120 REM * 144 OF ELEMENTARY CRYPTANALYSIS.                             *
00130 REM *      ARRAY A$( ) WILL HOLD THE ALPHABET IN NORMAL ORDER      *
00140 REM *      ARRAY M$( ) WILL HOLD THE LETTERS IN THE ENCIPHERED     *
00150 REM *         MESSAGE.                                             *
00160 REM *      D(I,J) WILL BE THE NUMBER OF TIMES THAT THE DIGRAPH     *
00170 REM *           A$(I)A$(J) OCCURS IN THE MESSAGE.                  *
00180 REM *      N = THE NUMBER OF CHARACTERS IN THE MESSAGE.            *
00190 REM ************************************************************************
00200 REM
00210 REM
00220 PRINT " THIS PROGRAM ASKS FOR AN ENCIPHERED MESSAGE AS INPUT "
00230 PRINT " AND PRODUCES AS OUTPUT A DIGRAPHIC FREQUENCY TABLE AS "
00240 PRINT " ON PAGE 144 OF ELEMENTARY CRYPTANALYSIS."
00250 PRINT
00260 PRINT
00270 DIM A$(26),M$(500),D(26,26)
00280 REM
00290 REM *******READY TO READ IN THE ARRAY A$( ) ************************
00300 REM
00310 DATA A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,Q,R,S,T,U,V,W,X,Y,Z
00320 FOR I = 1 TO 26
00330   READ A$(I)
00340 NEXT I
00350 REM
00360 REM *********** READY TO INPUT N ***********************************
00370 REM
00380 PRINT " WHEN YOU SEE THE QUESTION MARK, ENTER THE NUMBER OF LETTERS "
00390 PRINT " IN THE MESSAGE, THEN PRESS RETURN "
00400 INPUT N
00410 REM
00420 REM ***** READY TO INPUT THE MESSAGE IN P GROUPS OF 20 LETTERS ***
00430 REM ***** THEN THE FINAL N - P*20 LETTERS ************************
00440 REM
00450 LET P = INT(N/20)
00460 LET R = N - P*20
00470 PRINT " WHEN YOU SEE THE ? ENTER A GROUP OF 20 LETTERS IN THE MESSAGE "
00480 PRINT " SEPARATED BY COMMAS, THEN PRESS RETURN "
00490 FOR I = 0 TO P-1
00500   FOR K = 1 TO 20
00510           INPUT M$(I*20 + K),
00520   NEXT K
00530 NEXT I
00540 PRINT
00550 PRINT "NOW INPUT THE LAST "|R|" LETTERS SEPARATED BY COMMAS "
00560 FOR K = 1 TO R
00570   INPUT M$(P*20 +K ),
00580 NEXT K
00590 PRINT
00600 PRINT
00610 REM
```

```
00620 REM ***** READY TO PRINT OUT MESSAGE IN GROUPS OF 5 LETTERS ****
00630 REM ***************** WITH 9 GROUPS PER LINE  ********************
00640 REM
00650 PRINT "                THE CIPHER MESSAGE IS "
00660 PRINT
00670 PRINT
00680 FOR I = 1 TO N
00690   PRINT M$(I);
00700   IF (I/5 <> INT (I/5)) THEN 720
00710   PRINT " ";
00720   IF (I/45 <> INT (I/45)) THEN 740
00730   PRINT
00740 NEXT I
00750 REM **************** READY TO INITIALIZE ARRAY D( , ) TO ZEROES ***********
00760 REM
00770 FOR J = 1 TO 26
00780   FOR K = 1 TO 26
00790           LET D(J,K) = 0
00800   NEXT K
00810 NEXT J
00820 REM ***********************************************************************
00830 REM * FOR EACH PAIR OF LETTERS M$(I) AND M$(I+1) IN THE MESSAGE    *
00840 REM * (WHERE I GOES FROM 1 TO N-1 IN STEPS OF 2), THE PROGRAM      *
00850 REM * SEARCHES THE ALPHABET UNTIL IT FINDS M$(I) AS THE JTH LETTER *
00860 REM * THEN M$(I+1) AS THE KTH LETTER. THEN D(J,K) IS INCREASED BY 1*
00870 REM ***********************************************************************
00880 REM
00890 FOR I = 1 TO N-1 STEP 2
00900   FOR J = 1 TO 26
00910           IF M$(I) = A$(J) THEN 930
00920   NEXT J
00930   FOR K = 1 TO 26
00940           IF M$(I+1) = A$(K) THEN 960
00950   NEXT K
00960   LET D(J,K) = D(J,K) + 1
00970 NEXT I
00980 REM
00990 REM ****** READY TO PRINT OUT DIGRAPHIC FREQUENCY TABLE  **********
01000 PRINT
01010 PRINT
01020 PRINT
01030 PRINT TAB(20); "DIGRAPHIC FREQUENCY TABLE "
01040 PRINT
01050 PRINT
01060 PRINT "   ";
01070 FOR I = 1 TO 26
01080   PRINT "  ";A$(I);
01090 NEXT I
01100 PRINT
01110 FOR J = 1 TO 26
01120   PRINT
01130   PRINT A$(J);"  ";
01140   FOR K = 1 TO 26
01150           IF D(J,K) = 0 THEN 1180
01160           PRINT D(J,K);
01170           GO TO 1190
01180           PRINT "   ";
01190   NEXT K
01200   PRINT
01210 NEXT J
01220 END
```

```
THIS PROGRAM ASKS FOR AN ENCIPHERED MESSAGE AS INPUT
AND PRODUCES AS OUTPUT A DIGRAPHIC FREQUENCY TABLE AS
ON PAGE 144 OF ELEMENTARY CRYPTANALYSIS.


WHEN YOU SEE THE QUESTION MARK, ENTER THE NUMBER OF LETTERS
IN THE MESSAGE, THEN PRESS RETURN
? 454
WHEN YOU SEE THE ? ENTER A GROUP OF 20 LETTERS IN THE MESSAGE
SEPARATED BY COMMAS, THEN PRESS RETURN
? I,X,X,Z,K,Y,R,V,G,P,J,T,C,M,M,G,I,Y,G,E
? Y,Q,M,X,Z,D,A,N,S,G,H,E,R,U,Q,J,C,Z,B,Q
? Z,Q,X,A,P,C,Q,C,S,G,R,U,I,P,B,C,D,A,X,Z
? A,N,M,I,Q,D,T,F,I,B,A,J,K,L,S,G,A,S,M,X
? S,Y,W,G,O,U,Q,U,F,F,C,P,S,G,A,Y,C,M,M,C
? S,X,K,M,R,I,N,A,X,A,F,N,E,S,E,F,H,T,Y,S
? I,J,G,E,Q,A,H,E,Y,N,L,Q,O,Q,D,C,I,Q,X,Z
? Q,A,X,Z,E,Z,Q,C,O,D,F,A,C,V,Y,Q,G,T,E,S
? Y,X,Y,S,Z,S,O,Z,W,A,C,K,L,A,R,S,E,S,B,L
? Y,Q,L,Q,X,A,L,A,Z,W,U,O,G,L,J,Y,Y,Y,X,Z
? A,N,Q,P,K,P,W,N,V,U,E,M,I,V,F,O,C,K,B,C
? B,M,L,E,D,I,A,E,H,E,Z,S,S,G,Y,Q,E,M,X,Z
? U,J,S,R,C,B,H,U,S,G,Q,W,M,K,Z,W,C,K,Z,Q
? R,F,S,O,Y,Q,G,L,Z,I,S,L,T,O,P,P,Q,A,E,J
? D,N,Z,Q,Z,W,G,Y,G,W,U,D,H,J,T,E,W,N,D,A
? V,G,B,G,Z,Q,Z,W,Q,J,J,U,P,X,B,C,D,A,M,X
? X,Z,Q,A,X,Z,A,N,K,Q,K,N,T,S,Z,Q,X,A,Z,Q
? Z,B,H,E,W,H,H,T,Q,A,X,Z,E,U,O,H,H,E,S,G
? T,O,X,A,X,V,U,B,B,R,Q,P,X,V,G,W,H,E,M,Q
? O,U,W,G,S,G,Q,A,A,N,T,C,V,P,M,N,Q,N,U,W
? F,M,X,K,W,H,X,J,E,F,W,H,C,M,S,G,X,Z,A,N
? K,Q,K,N,T,S,I,L,R,I,U,A,U,E,C,M,M,J,T,S

NOW INPUT THE LAST  14  LETTERS SEPARATED BY COMMAS
? Y,R,R,R,Q,C,T,A,X,Q,T,O,K,Y


              THE CIPHER MESSAGE IS


IXXZK YRVGP JTCMM GIYGE YQMXZ DANSG HERUQ JCZBQ ZQXAP
CQCSG RUIPB CDAXZ ANMIO DTFIB AJKLS GASMX SYWGO UQUFF
CPSGA YCMMC SXKMR INAXA FNESE FHTYS IJGEQ AHEYN LQOQD
CIQXZ QAXZE ZQCOD FACVY QGTES YXYSZ SOZWA CKLAR SESBL
YQLQX ALAZW UOGLJ YYYXZ ANQPK PWNVU EMIVF OCKBC BMLED
IAEHE ZSSGY QEMXZ UJSRC BHUSG QWMKZ WCKZQ RFSOY QGLZI
SLTOP PQAEJ DNZQZ WGYGW UDHJT EWNDA VGBGZ QZWQJ JUPXB
CDAMX XZQAX ZANKQ KNTSZ QXAZQ ZBHEW HHTQA XZEUO HHESG
TOXAX VUBBR QPXVG WHEMQ OUWGS GQAAN TCVPM NQNUW FMXKW
HXJEF WHCMS GXZAN KQKNT SILRI UAUEC MMJTS YRRRQ CTAXQ
TOKY
```

DIGRAPHIC FREQUENCY TABLE

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
A					1					1				6					1						1
B			3				1					1	1				1	1							
C		1									3		4			1						1			
D	3		1						1					1											
E						2				1			2						3		1				
F	1					1							1	1	1										
G					2							2				1				1			2		1
H					6					1										2	1				
I		1								1		1				1	1					1		1	1
J																				1	1				1
K												1	1	2		1	2								2
L	2				1												2								
M			1				1		1	1	1			1			1							3	
N	1																								
O				2				1									1				2				
P			1													1								1	
Q	6		3							2				1		2					1		1		
R						1			2									1	1		2	1			
S							9					1			1			1						1	1
T	1		1		1	1									3				3						
U	1	1		1	1					1					1								1		
V							1									1					1				
W	1						2	3						2											
X	5									1	1						1					2			
Y														1			5	1	2					1	1
Z		1		1					1								6		2				4		

```
>RUN

 10  PRINT "this program asks for an enciphered message as input"
 20  PRINT "and produces as output a digraphic frequency table as"
 30  PRINT "on page 144 of elementary cryptanalysis."
 40  PRINT LIN(2)
 50  DIM A$[26],M$[255],D[26,26]
 60  REM *** initialize a$ ****
 70  A$="ABCDEFGHIJKLMNOPQRSTUVWXYZ"
 80  REM *** ready to input n ****
 90  PRINT "when you see the ? , enter the number of letters"
100  PRINT "in the message, the press return."
110  INPUT N
120  REM ***
130  REM *** ready to input the message in P groups of 20 letters
140  REM *** then final n-P*20 letters ****
150  P=INT(N/20)
160  R=N-P*20
170  PRINT LIN(2);"when you see the ? enter a group of 20 letters in the message"
180  PRINT "no commas or spaces between letters. then press return."
190  FOR I=0 TO P-1
200  INPUT M$[I*20+1,I*20+20]
210  NEXT I
220  IF R=0 THEN 250
230  PRINT LIN(2);"now input the last ";R;" letters separated by nothing as abov
240  INPUT M$[P*20+1,P*20+R]
250  M$=UPS$(M$)
260  PRINT LIN(2)
270  REM *** ready to print message in groups of 5 letters ***
280  REM ******** with 9 groups per line **********************
290  PRINT "                    the coded message is"
300  PRINT LIN(2)
310  FOR I=1 TO N
320  PRINT M$[I,I];
330  IF I/5$INT(I/5) THEN 350
340  PRINT " ";
350  IF I/45$INT(I/45) THEN 370
360  PRINT
370  NEXT I
380  REM ready to initialize array d to zeroes ***
390  FOR I=1 TO 26
400  FOR J=1 TO 26
410  D[I,J]=0
420  NEXT J
430  NEXT I
440  REM
450  REM
460  REM
470  FOR I=1 TO N-1 STEP 2
480  FOR J=1 TO 26
490  IF M$[I,I]=A$[J,J] THEN 510
500  NEXT J
510  FOR K=1 TO 26
520  IF M$[I+1,I+1]=A$[K,K] THEN 540
530  NEXT K
540  D[J,K]=D[J,K]+1
550  NEXT I
```

```
560  REM **** ready to print out digraphic frequency table ****
570  PRINT LIN(2);TAB(20);"digraphic frequency table"
580  PRINT LIN(2);"  ";
590  FOR I=1 TO 26
600  PRINT "  ";A$[I,I];
610  NEXT I
620  PRINT
630  FOR J=1 TO 26
640  PRINT
650  PRINT A$[J,J];"  ";
660  FOR K=1 TO 26
670  IF D[J,K]=0 THEN 700
680  PRINT D[J,K];
690  GOTO 710
700  PRINT "  ";
710  NEXT K
720  PRINT
730  NEXT J
740  END
```

واژه‌نامهٔ پیوست

cipher message	پیام رمزی
digraph	دوحرفی
distribution	توزیع
encipher	به رمزدرآوردن
frequency	فراوانی
index of coincidence	شاخص انطباق
matching alphabets	تطبیق الفباها
periodic polyalphabetic cipher	رمز چندالفبایی تناوبی
trigraph	سه‌حرفی
trigraphic frequency distribution	توزیع فراوانی سه‌حرفی

مرکز نشر دانشگاهی

شابک: ۱۰_۰۷۵۹_۰۱_۹۶۴