

مسئلہ انتخابی: در اتفاق اس استراتژی رصب و جور عالم حالت فرض برآن بود که متن آن اکثر مقابل سُناسی است، کیا حسن فرضی همراه صحیح است؟ به حد فرمی برآن به عورت خورکار بازرسی نیک برای حسن عمل را نجات دارد؟

۸ قدرت ماسیبائی چهاجم

در این دسته بندی کلیه می‌تلران قدرت چهاجم را به دو رده زیر تقسیم نمی‌کرد:

۱ قدرت ماسیبائی محدود: در این دسته چهاجم در بازه زمانی مخصوصی (عنه) خود چیزی بر حسب امسیت خود را نظری می‌گذراند اسکریپت اتفاق اتفاق را امداد می‌کند.

۲ قدرت ماسیبائی نامحدود

که: در این دسته، چهاجم محدودیت زمانی ندارد
می‌گذراند اسکریپت اتفاق اتفاق خود را به عنوان گروهی زمانی امداد می‌کنند.

متوجه باشد! در اصل مفهوم این پیشتر زیر تعریف می‌شود:

۱ امسیت ماسیبائی: یک ستم رمزنگاری در مقابل چهاجم با قدرت ماسیبائی محدود امن باشد، دلار امنیت ماسیبائی است.

۲ امنیت مطلقاً: یک ستم رمزنگاری که در مقابل چهاجم با قدرت ماسیبائی نامحدود امن است، دلار امنیت مطلقاً است، به عبارت دیگر مستقل از قدرت ماسیبائی در دسترس، منع امنیت اطلاع کافی برای نیس قطعی منع امنیت اطراف از این نظر لذت.

۹ جمع بندی: یا توصیر به مباحثه تعریف سده عکس در راهیه با تحلیل رمز، همراه یک ستم رمزنگاری بیان نکرید مسکون تعریف سده و امنیت آن این ذاتی سود.

درینه عدل کنند و بخشن امسالی زیرک در راه به با آنها در بخش های قبل متعجب کرده ایم، پس
هستند:

۱ صیزان رانس مهاجم

۲ قدرت مهابات مهاجم

۱۵ سیم های رمز نلاسک

نهاده شده سیم های رمز نلاسک از زمان حبّت چهارم دوّم و قبل از بوجور امده اند
سیم های کامپوتری امروزی بخصوص استرس صور اسکاره قراری ترقیت شدند. این نوع
در دو مرحله زیر تقسیم شدند:

* سیم های رمز نگاری نلاسک - جاستیشن (Substitution): در این نوع
هر کاراکتر باشد که کاراکتر دیگر در صورت انتقال و نهایت قادرست اکتفا نماید
درینه آنکه
می شود.

+ سیم های رمز نگاری نلاسک - جایگایه (Transposition): در این نوع هر کاراکتر
آنچنان آنکه باشد که کاراکتر دیگر در همان صفت جایگای سود.

در ادامه برخی از سیم های رمز نگار نلاسک برای هر دو مرحله بالا آورده شده است.

۴ چند سیستم رمزنگاری کلاسیک و برخی حملات مطرح برای آنها

۱.۴ سیستم‌های رمزنگاری کلاسیک - جانشینی

۱.۴.۱ سیستم رمز سزار

تعریف ۲ (سیستم رمز سزار) مطابق تعریف رسمی فوق برای سیستم‌های رمزنگاری متقارن، سیستم رمز سزار^{۱۰} را به صورت زیر تعریف می‌کنیم:

$$\mathcal{M} = \{a, b, \dots, z\}^*$$

- تعریف Gen: یک عدد تصادفی از مجموعه‌ی $\{0, 1, \dots, 25\} = \mathcal{K}$ تولید می‌کند.

• تعریف Enc:

$$\begin{aligned} \text{Enc}_k(m_1m_2\cdots m_t) &= c_1c_2\cdots c_t \\ c_i &= m_i + k \quad i = 1, 2, \dots, t \end{aligned}$$

• تعریف Dec:

$$\begin{aligned} \text{Dec}_k(c_1c_2\cdots c_t) &= m_1m_2\cdots m_t \\ m_i &= c_i - k \quad i = 1, 2, \dots, t \end{aligned}$$

در واقع سیستم رمز سازار یک کلید تصادفی در K انتخاب می‌کند و حروف متن را به آن اندازه شیفت می‌دهد. توجه کنید الگوریتم Enc در این سیستم قطعی است. با اینحال در حالت کلی و بدون اطلاع از مقدار کلید، خروجی این الگوریتم می‌تواند در قالب یک متغیر تصادفی¹¹ در نظر گرفته شود و در نتیجه مقادیر مختلفی را با یک توزیع احتمالاتی معین اختیار کند. حمله‌ی متن رمزی به سیستم رمز سازار، ایده‌ی حمله به رمز سازار استفاده از توزیع غیر یکنواخت حروف زبان انگلیسی است که اندازه‌گیری‌های آماری نشان می‌دهد به شکل زیر است:

جدول ۱: توزیع حروف زبان انگلیسی بدون احتساب فاصله

a	8.17%	n	6.75%
b	1.49%	o	7.51%
c	2.78%	p	1.92%
d	4.25%	q	0.09%
e	12.70%	r	5.99%
f	2.23%	s	6.33%
g	2.01%	t	9.06%
h	6.09%	u	2.76%
i	6.97%	v	0.98%
j	0.15%	w	2.36%
k	0.77%	x	0.15%
l	4.02%	y	1.97%
m	2.41%	z	0.07%

اگر در جدول فوق فراوانی سمبول i را f_i بنامیم، خواهیم داشت:

$$\sum_{i=0}^{26} f_i^2 = 0.065$$

با علم به این موضوع، حمله‌ی خودکار به رمز سازار را می‌توان به شکل زیر انجام داد:

1. محاسبه‌ی فراوانی حرف‌های متن رمز شده

2. محاسبه‌ی ضرایب انطباق¹²: ضرایب انطباق را به شکل زیر تعریف می‌کنیم:

$$I_j = \sum_{i=0}^{26} f_i \times p_{i+j}$$

اگر j برابر با k باشد و متن به اندازه‌ی کافی بزرگ باشد، انتظار داریم $I_j \approx 0.065$

3. حدس ما برای k اندیس زای است که عبارت $|I_j - 0.065|$ را کمیه کند.

¹¹Random Variable
¹²coincidence index

$$k = \arg \min_j \{|I_j - 0.065|\}$$

توجه کنید این روش، لزوماً بهترین روش نیست، اما روشی برای حمله به سیستم رمز ساز است. به عنوان مثال استفاده از توزیع دو حرفی ها^{۱۳} یا سه حرفی ها^{۱۴} به جای تک حرفی ها^{۱۵} می تواند منجر به حمله بیشتری شود.

۲.۱.۴ سیستم رمز جایگزینی ساده

تعريف ۳ سیستم رمز جایگزینی ساده^{۱۶} با الگوریتم های زیر روی فضای پیام^{*} $M = \{a, b, \dots, z\}$ تعریف می شود:

- تعریف Gen: یک جایگشت تصادفی از $(0, 1, \dots, 25)$ را به عنوان کلید k انتخاب می کند.
- تعریف Enc: $c_i = k(m_i) \quad i = 1, 2, \dots, t$

$$\text{Enc}_k(m_1 m_2 \cdots m_t) = c_1 c_2 \cdots c_t$$

$$c_i = k(m_i) \quad i = 1, 2, \dots, t$$

• تعریف Dec:

$$\text{Dec}_k(c_1 c_2 \cdots c_t) = m_1 m_2 \cdots m_t$$

$$m_i = k^{-1}(c_i) \quad i = 1, 2, \dots, t$$

جهت حمله به این سیستم می توان فراوانی حروف متن رمزی را بدست آورد و حروف را بر حسب فراوانی مرتب نمود و حرف i -ام این لیست را رمز شده i -امین حرف پر تکرار القا در نظر گرفت. اگر متن به اندازه کافی بزرگ باشد این روش، روش مناسبی جهت حمله است.

۳.۱.۴ سیستم رمز ویژنر

تعريف ۴ سیستم رمز ویژنر^{۱۷} با الگوریتم های زیر روی فضای پیام^{*} $M = \{a, b, \dots, z\}$ تعریف می شود:

- تعریف Gen: در این سیستم، الگوریتم Gen یک عضو مانند $(k_0, k_1, \dots, k_{d-1})$ را به تصادف از فضای کلید $\mathcal{K} = \{0, 1, \dots, 26\}^d$ انتخاب می کند.
- تعریف Enc:

$$\text{Enc}_k(m_0 m_1 \cdots m_{\ell-1}) = c_0 c_1 \cdots c_{\ell-1}$$

$$c_i = m_i + k_{(i \bmod d)}$$

• تعریف Dec:

$$\text{Dec}_k(c_0 c_1 \cdots c_{\ell-1}) = m_0 m_1 \cdots m_{\ell-1}$$

$$m_i = c_i - k_{(i \bmod d)}$$

در واقع در این سیستم، متن اصلی به پنجره های d -تایی تقسیم شده و i -امین حرف هر پنجره $(0 \leq i \leq d-1)$ ، k_i واحد جابجا می شود. وقت کنید برای حمله به این سیستم، اگر مقدار حدس زده شده برای d را \hat{d} بنامیم و $\hat{d} = d$ بناشیم، آنگاه برای متن به اندازه کافی طولانی، توزیع حروف برای حرف های i -ام پنجره ها $(0 \leq i \leq \hat{d}-1)$ برابر شیفت یافته توزیع حروف زبان انگلیسی می شود. اما اگر $d \neq \hat{d}$ توزیع های فوق به سمت توزیع یکنواخت می رود. پس برای حمله به این سیستم می توان معیار های $\sum f_i^2$ را برای عناصر هم مکان در پنجره ها تعریف نمود. سپس برای مقادیر مختلف \hat{d} ، معیارها را بررسی کرد. برای $\hat{d} = d$ مقدار تمام معیارها نزدیک ۶۵٪ خواهد شد. بدین ترتیب d بدست می آید. پس از آن رمزگشایی برای جایگاه های i -ام $(0 \leq i \leq d-1)$ از پنجره ها مانند سیستم ساز انجام می شود. از مزایای این سیستم این است که توزیع تک حرفی ها، دو حرفی ها و سه حرفی ها برای d های بزرگ، تقریباً یکنواخت خواهد بود.

¹³Bigrams

¹⁴Trigrams

¹⁵Monograms

¹⁶Simple Substitution Cipher

¹⁷Vigenère Cipher

۴.۱.۴ رمز هیل

تعريف ۵ سیستم رمز هیل^{۱۸}، یک سه تابی $(\text{Gen}, \text{Enc}, \text{Dec})$ II = به همراه فضای پیام

$$\mathcal{M} = (\{0, \dots, 25\})^d$$

است که:

$\text{Gen}()$: یک ماتریس تصادفی و معکوس پذیر $K_{d \times d}$ به پیمانه‌ی 26 تولید می‌کند، که d طول بلوک است.

الگوریتم‌های رمزگذاری و رمزگشایی به ترتیب به صورت زیر عمل می‌کنند:

$$\begin{aligned} \text{Enc}_K(m_1, \dots, m_{ld}) &= c_1, \dots, c_{ld} \\ \begin{pmatrix} c_{id+1} \\ \vdots \\ c_{id+d} \end{pmatrix} &= K \begin{pmatrix} m_{id+1} \\ \vdots \\ m_{id+d} \end{pmatrix} \mod 26 \end{aligned}$$

$$\begin{aligned} \text{Dec}_K(c_1, \dots, c_{ld}) &= m_1, \dots, m_{ld} \\ \begin{pmatrix} m_{id+1} \\ \vdots \\ m_{id+d} \end{pmatrix} &= K^{-1} \begin{pmatrix} c_{id+1} \\ \vdots \\ c_{id+d} \end{pmatrix} \mod 26. \end{aligned}$$

نکته ۱ بیا در بحث می‌کرد که عدد صحیح a در هنگ m دارای معکوس است (یعنی معادله‌ی $ax = b \mod m$ دارای جواب یکتا است)، اگر و تنها اگر $\gcd(a, m) = 1$. این نتیجه قابل تعمیم به حالت ماتریسی نیز هست: ماتریس A روی \mathbb{Z}_m معکوس پذیر است یعنی (معادله‌ی $AX = B \mod m$ دارای جواب یکتا است)، اگر و تنها اگر $\gcd(\det A, m) = 1$. بنابراین ماتریس K که به عنوان کلید برای رمز هیل تولید می‌شود، معکوس پذیر است اگر و فقط اگر $\gcd(\det K, 26) = 1$.

نکته ۲ تعداد ماتریس‌های معکوس پذیر روی \mathbb{Z}_{26} برابر است با

$$26^{d^2} \prod_{i=1}^d \left(1 - \frac{1}{2^i}\right) \prod_{i=1}^d \left(1 - \frac{1}{13^i}\right) \geq 2^{4.7d^2 - 1.8} \geq 0.29 \times 2^{4.7d^2}.$$

به عبارت دیگر احتمال اینکه یک ماتریس تصادفی روی \mathbb{Z}_{26} معکوس پذیر باشد حداقل 0.29 است.

برای اثبات رابطه فوق ضمیمه ۱ را بینید. به طور مثال به ازای $d = 8$ اندازه فضای کلید برابر 2^{299} است که عدد بسیار بزرگی است. طول کلید رمزهای مدرن معمولاً کمتر از ۲۵۶ بیت است.

مثال ۶ فرض کنید در سیستم رمز هیل داشته باشیم $d = 2$ و $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$. برای رمزگذاری پیام fly let us fly، ابتدا متن اصلی را به بلوک‌های به طول 2 تقسیم و به صورت بردارهایی روی $(\mathbb{Z}_{26})^2$ به صورت زیر نمایش می‌دهیم:

$$\begin{pmatrix} 11 \\ 4 \end{pmatrix}, \begin{pmatrix} 19 \\ 20 \end{pmatrix}, \begin{pmatrix} 18 \\ 5 \end{pmatrix}, \begin{pmatrix} 11 \\ 24 \end{pmatrix}.$$

$$M = \begin{pmatrix} 11 & 19 & 18 & 11 \\ 4 & 20 & 5 & 24 \end{pmatrix} \text{ را تشکیل داده و مقدار سپس ماتریس متن اصلی}$$

$$C = K \cdot M \mod 26 = \begin{pmatrix} 23 & 5 & 4 & 1 \\ 9 & 15 & 11 & 19 \end{pmatrix}$$

¹⁸Hill Cipher, 1929.

را محاسبه می‌کنیم که نمایش متن رمزی $xjfpelbt$ است.
می‌توان بررسی نمود که

$$K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

$$K^{-1} \cdot C = \begin{pmatrix} 11 & 19 & 18 & 11 \\ 4 & 20 & 5 & 24 \end{pmatrix}$$

که نمایش متن اصلی اولیه است.

حمله‌ی متن اصلی معلوم به سیستم رمز هیل. سیستم رمز هیل در مقابل حمله‌ی متن اصلی معلوم به شدت ضعیف است. برای حمله‌ی متن اصلی معلوم به صورت زیر عمل می‌کنیم: فرض کنید ما متن اصلی m و رمز شده‌ی آن c را در اختیار داشته باشیم، در این صورت m را به بلوک‌های d -تایی تقسیم کرده و ماتریس $1 \times d$ متناظر با هر بلوک را کنار یک دیگر قرار داده در این صورت به ماتریس متن اصلی $t \times d$ می‌رسیم که t تعداد بلوک‌های متن اصلی است، این ماتریس را M بنامید، همین کار را با c تکرار کرده و ماتریس حاصل را C بنامید، می‌دانیم:

$$C = K \cdot M$$

بنابراین کافی است معکوس ماتریس M به پیمانه ۲۶ را حساب کنیم، یعنی:

$$K = C \cdot M^{-1};$$

نکته ۳ روش فوق به شرطی قابل اجرا است که ماتریس M معکوس پذیر باشد (\mathbb{Z}_{26} روی)، یعنی

$$\gcd(\det M, 26) = 1$$

به طور مثال به ازای $d = 5$ اگر پیام‌ها تصادفی انتخاب شوند، احتمال موفقیت با توجه به نکته ۲، برابر ۰.۲۹ خواهد بود.

۲.۴ سیستم‌های رمزگاری کلاسیک - جابه‌جایی

رمز جابه‌جایی ستوانی^{۱۹} جزء دسته‌ای از رمزهای کلاسیک به نام رمزهای جابه‌جایی^{۲۰} است که فقط مکان حرف‌های متن اصلی را در متن رمز شده جابه‌جا می‌کند.

تعریف ۷ سیستم رمز جابه‌جایی ستوانی، یک سه‌تایی $(\text{Gen}, \text{Enc}, \text{Dec})$ به همراه فضای پیام

$$\mathcal{M} = (\{a, \dots, z\})^d$$

است که:

• $\text{Gen}()$: یک جایگشت تصادفی k از $\{0, 1, \dots, d-1\}$ تولید می‌کند.

• الگوریتم رمزگذاری به صورت زیر عمل می‌کند:

$$\text{Enc}_k(m_0 m_1 \dots m_{l-1}) = c_0 c_1 \dots c_{l-1}$$

که برای $j = 0, \dots, l-1$ و $i = 0, \dots, d-1$ $c_{i+jd} = m_{k(i)+jd}$

• الگوریتم رمزگشایی به صورت زیر عمل می‌کند:

$$\text{Dec}_k(c_0 c_1 \dots c_{l-1}) = m_0 m_1 \dots m_{l-1}$$

که برای $j = 0, \dots, l-1$ و $i = 0, \dots, d-1$ $m_{i+jd} = c_{k^{-1}(i)+jd}$

¹⁹Columnar transposition

²⁰transposition cipher

در حقیقت الگوریتم رمزگذاری متن اصلی m را به بلوکهای d تابی تقسیم می‌کند و جایگشت k را روی هر بلوک اعمال می‌کند.

نکته ۴ رمز جابه‌جایی ستونی حالت خاص رمز هیل است که در آن ماتریس K ، یک ماتریس جایگشت (ماتریسی که هر سطر و هر ستون آن دقیقاً یک عدد ۱ داشته باشد و بقیه عناصر آن صفر باشد) است.

قرارداد ۱ روش‌های مختلفی برای نمایش یک جایگشت روی $\{0, \dots, n-1\}$ وجود دارد؛ در اینجا یک جایگشت k را با $k = k(0), k(1), \dots, k(n-1)$ نشان می‌دهیم، به طور مثال $k = (1 \ 4 \ 3 \ 2 \ 0)$ بیانگر جایگشت $= k(0) = 1, k(1) = 4, k(2) = 3, k(3) = 2, k(4) = 0$ است.

مثال ۸ فرض کنید $3 \times d = (1 \ 0 \ 2)$ و $m = m_0m_1m_2m_3m_4m_5m_6m_7m_8$ به متن رمز شده $c = m_1m_0m_2m_4m_3m_5m_7m_6m_8$ نگاشته می‌شود.

مثال ۹ فرض کنید $6 \times d = (3 \ 2 \ 0 \ 5 \ 1 \ 4)$ و متن اصلی به صورت زیر باشد:

he walked up and down the passage two or three times

در این صورت برای رمزگذاری می‌توان متن را در شش ستون به صورت زیر نوشت

hewalk
edupan
ddownt
hepass
agetwo
orthre
etimes

و سپس ستون‌ها را با ترتیبی که جایگشت k تعیین می‌کند با یکدیگر تعویض می‌کنیم، در این مثال ستون‌ها به صورت زیر چیده خواهند شد

wlehka
uadenp
onddtw
psehsa
ewgaot
trroeh
ietesm

و در نهایت متن را به صورت سطری به صورت زیر کنار هم می‌نویسیم و متن رمزی بدست خواهد آمد.

wlehkaudenpondtupsehsaeuwgaottrroehietesm

حمله‌ی متن رمزی به سیستم رمز جابه‌جایی ستونی. در رمز جابه‌جایی ستونی فرکانس تک حرکتی‌ها ثابت باقی می‌ماند، اما فرکانس دو حرکتی‌ها و سه حرکتی‌ها و ... در متن رمزی دیگر با فرکانس دو حرکتی‌ها و سه حرکتی‌ها و ... در زبان انگلیسی یکسان نیست. پس از طریق فرکانس دو حرکتی‌ها می‌توان به این سیستم حمله کرد، ابتدا متن رمزی را به صورت زیر بازنوسی کنید:

$$\begin{pmatrix} c_0 \\ c_d \\ \vdots \\ c_{(\ell-1)d} \end{pmatrix}, \begin{pmatrix} c_1 \\ c_{d+1} \\ \vdots \\ c_{(\ell-1)d+1} \end{pmatrix}, \dots, \begin{pmatrix} c_{d-1} \\ c_{2d-1} \\ \vdots \\ c_{\ell d-1} \end{pmatrix}.$$

حال به دنبال این هستیم که ستون‌هایی که محتمل‌تر هستند که مجاور باشند تشخیص دهیم. به عبارت دیگر برای هر ستون i از بین ستون‌های باقی‌مانده ستونی را برابر می‌گرینیم که وقتی در کنار آن قرار گیرد فرکانس دو حرکتی‌ها بیشترین تطابق را با فرکانس دو حرکتی‌های زبان انگلیسی داشته باشد، اگر همه‌ی حدس‌ها درست باشند، بدین ترتیب یک جایگشت دوری از کلید بدست می‌آید که با امتحان کردن d حالت ممکن می‌توان جایگشت صحیح را پیدا کرد.

ضمیمه ۱ - فضای کلید سیستم رمز هیل

هدف از این قسمت محاسبه تعداد ماتریس‌های معکوس پذیر روی \mathbb{Z}_m برای حالت خاصی که $m \in \mathbb{N}$ حاصل ضرب اعداد اول متمایز باشد، است. نتایج این بخش را می‌توان برای حالت کلی‌تر نیز ارائه کرد، اما پیچیده‌تر است.

قضیه ۱ اگر p عددی اول و $d \in \mathbb{N}$ در این صورت تعداد ماتریس‌های معکوس پذیر $d \times d$ روی \mathbb{Z}_p برابر است با

$$\prod_{i=0}^{d-1} (p^d - p^i).$$

برهان. از جبرخطی می‌دانیم که یک ماتریس معکوس پذیر است اگر و تنها اگر ستون‌های آن مستقل خطی باشند. بنابراین هدف ما حساب کردن تعداد ماتریس‌های $d \times d$ است که d ستون آن به پیمانه p مستقل خطی باشند. برای ساخت اولین ستون تنها محدودیت ما این است که تمام صفر نباشد (و چون هر ستون d درایه دارد و برای هر درایه p تا انتخاب داریم)، بنابراین $1 - p^d$ تا انتخاب برای ستون اول داریم. حال فرض کنید که i ستون اول مستقل خطی $c_1 c_2 \dots c_i$ ساخته‌ایم، برای ساخت ستون $i+1$ ام، این ستون باید از i ستون قبلی مستقل خطی باشد یا به عبارت دیگر ترکیب خطی از i ستون قبلی نباشد (یا به عبارت دیگر وجود نداشته باشد؛ $c_1, \dots, c_i, c_{i+1} = c_1 \cdot c_2 + \dots + c_i \cdot c_{i+1}$). پس $(p^d - p^i)$ حالت برای انتخاب ستون $i+1$ داریم زیرا هر c_i ، p ، حالت دارد؛ بنابراین تعداد کل ماتریس‌های معکوس پذیر $d \times d$ روی \mathbb{Z}_p برابر است با $\prod_{i=0}^{d-1} (p^d - p^i)$.

■

قضیه ۲ اگر p_1, \dots, p_ℓ اعداد اول متمایز و $d \in \mathbb{N}$ در این صورت تعداد ماتریس‌های معکوس پذیر $d \times d$ روی \mathbb{Z}_m که $m = \prod_{k=1}^\ell p_k$ برابر است با

$$\prod_{k=1}^\ell \prod_{i=0}^{d-1} (p_k^d - p_k^i).$$

برهان. می‌توان نشان داد که یک یکریختی از مجموعه ماتریس‌های معکوس پذیر روی $\mathbb{Z}_{p_1 p_2 \dots p_\ell}$ به ℓ -تایی‌های مرتب که مؤلفه‌ی k ام آن ماتریس‌های معکوس پذیر روی \mathbb{Z}_{p_k} می‌باشد، وجود دارد. این گزاره را می‌توان با استفاده از مفهوم یکریختی در نظریه گروه‌ها اثبات کرد که ما در اینجا بدان نخواهیم پرداخت. بنابراین بنا بر اصل ضرب و لم ۱ تعداد ماتریس‌های معکوس پذیر روی $\mathbb{Z}_{p_1 p_2 \dots p_\ell}$ برابر

$$\prod_{i=0}^{d-1} (p_1^d - p_1^i) \times \dots \times \prod_{i=0}^{d-1} (p_\ell^d - p_\ell^i)$$

است و حکم ثابت است.

■

نتیجه ۱۰ تعداد ماتریس‌های معکوس پذیر روی \mathbb{Z}_{26} برابر است با

$$26^{d^2} \prod_{i=1}^d \left(1 - \frac{1}{2^i}\right) \prod_{i=1}^d \left(1 - \frac{1}{13^i}\right)$$

■

برهان. در قضیه ۲ کافی است قرار دهیم $p_1 = 2, p_2 = 13$.

۱۱ تعریف همایش اتفاقاً (Index of coincidence) : خوشنودی x_1, x_2, \dots, x_n

اگر n کارتری از خود معلوم نباشد. همایش اتفاقاً x را بآمار (x) نشان داده و آن را احتمال اینکه دو عدد متفاوت از x میباشد باسند تعریف میکنیم.

خوشنودی فرکانس های تکرار A را در رشتہ x با $\frac{f_i}{25}$ به ترسیب میکنیم.

و اینچنان است $I_c(x) = \frac{n(n-1)}{\binom{n}{2}}$ روش بر انتساب $\frac{1}{2}$ عقیده از رشتہ x داریم و معمین میباشد اینکه دو عدد با این سینه میباشد انتساب سود میگیرد $I_c(x) = \frac{f_i(f_i-1)}{\binom{n}{2}}$ روش دیگر دارد.

با درج به تعریف میگیریم: $I_c(x)$ را به صورت زیر در نظر گیریم:

$$I_c(x) = \frac{\frac{25}{2} \binom{f_i}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)} = \frac{\sum_{i=0}^{25} f_i^2 - \frac{25}{2} f_i}{n(n-1)}$$

$$= \frac{\left(\sum_{i=0}^{25} f_i^2 \right) - n}{n(n-1)}$$

وقتی n به حدست بخواهد میل کند، داریم:

$$I_c(x) = \frac{\sum_{i=0}^{25} f_i^2}{n^2}$$

$$\text{که از تعریف نسخه} \quad p_i = \frac{f_i}{n} \quad \text{آنکه داریم:}$$

$$I_c(x) = \sum_{i=0}^{25} p_i^2$$

۱۳) آزمون کاسیسکی (Kasiski examination): در علم تحلیل رمزیه عفران (کاسیسکی) برای کسر کلمه بین رزیگاری هار متنسته پر جاگایلزنه های حیند العباری (Polyalphabetic) ساخته می شود.

آزمون کاسیسکی حد واقع سرتیفیکی را برای تحلیل کننده فرموده تا در تجزیه هار مزیگاری قبیح بر جایگزینی حیند العباری می باشد طول مدلیور را سفاره را رافت تبریزید. تحلیل تر بدار اینچ طول مدلیور ممکن است از تحلیل هار مزیگاری ستم های رزیگاری هست میر جایگزین شد. العباری سفاره کسره و ستم افزایشی را صورت گیره می تردند.

خیلی نظریه آزمون کاسیسکی: این آزمون شامل مستجوبرای را می توان رشته های کارکرده تغییر داده در متن رضی است. همچنان رشته های باست ۳ کارکرده است باشد که این آزمون صویقیت کمتر باشد.

خاصله میان رخداد هار مبتدا به رشته های تغییری به اعمال زیاد صفتی از مدل مدلیور باشد. بنابرین پیدا کردن رشته های تغییری بسیار طول های ممکن برای کسر را می بینیم ترسبی توان بزرگترین معنی علم و مهندسی کام فاصله ها را بدست آورده.

داده ای بزرگترین معنی علم و مهندسی، بزرگترین عضو از صنعتی های مهندسی هار صعودی دارد اخراج موردنظر.

مثال: رشتہ زیر را در نظر بگیرید.

crypto is short for cryptography.

در این رشته crypto کسری است و خاطله می باشد توکل رشته ۳ است. اگر طلبدی کارکرده باشد این تغییر در متن رمزی خواهد بود و ۲ نیز برای تقسیم نیز است و آزمون کاسیسکی حقوق خواهد بود (برای تجربه).

اگر اگر طول مدلیور ۲ کارکرده باشد، متن رمز مختلف خاصله می شود و آزمون کاسیسکی در این حالت حقوق محمل نمی شود.