به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۲۴ بهمن ۱۳۹۱

جلسه‌ی ۳: رمزنگاری سنتی و مدرن

مدرس: دکتر شهرام خزائی *نگارنده: سهراب ابوذرخانی‌فرد*

۱ رمز جایگشتی

رمز جایگشتی[۱] جزء دسته‌ای از رمزهای کلاسیک به نام رمزهای جابه‌جایی[۲] است که فقط مکان حرف‌های متن اصلی را در متن رمز شده جابه‌جا می‌کنند.

تعریف ۱ *سیستم رمز جایگشتی، یک سه‌تایی* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *به همراه فضای پیام*

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

است که:

- $\mathsf{Gen}()$*: یک جایگشت تصادفی* k *از* $\{0, 1, \cdots, d-1\}$ *تولید می‌کند.*
- *الگوریتم رمزگذاری به صورت زیر عمل می‌کند:*

$$\mathsf{Enc}_k(m_0 m_1 \cdots m_{l\,d-1}) = c_0 c_1 \cdots c_{l\,d-1}$$

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

- *الگوریتم رمزگشایی به صورت زیر عمل می‌کند:*

$$\mathsf{Dec}_k(c_0 c_1 \cdots c_{l\,d-1}) = m_0 m_1 \cdots m_{l\,d-1}$$

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

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

---

[۱] permutation cipher
[۲] transposition cipher

یادآوری ۱ *روش‌های مختلفی برای نمایش یک جایگشت روی* $\{۰, \cdots, n-۱\}$ *وجود دارد؛ در اینجا یک جایگشت* k *را با* $k = (k(۰)\ k(۱)\ \cdots\ k(n-۱))$ *نشان می‌دهیم. به طور مثال* $k = (۱\ ۴\ ۳\ ۲\ ۰)$ *بیانگر جایگشت* $k(۰) = ۱, k(۱) = ۴, k(۲) = ۳, k(۳) = ۲, k(۴) = ۰$ *است.*

مثال ۲ *فرض کنید* $d = ۳$ *و* $k = (۱\ ۰\ ۲)$ *در این صورت متن* $m = m_۰m_۱m_۲m_۳m_۴m_۵m_۶m_۷m_۸$ *به متن رمزشده* $c = m_۱m_۰m_۲m_۴m_۳m_۵m_۷m_۶m_۸$ *نگاشته می‌شود.*

مثال ۳ *فرض کنید* $d = ۶$ ، $k = \begin{pmatrix} ۳ & ۲ & ۰ & ۵ & ۱ & ۴ \end{pmatrix}$ *و متن اصلی به صورت زیر باشد:*

```
he walked up and down the passage two or three times
```

در این صورت جهت 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.

```
wlehkauadenponddtwpsehsaewgaottrroehietesm
```

۱.۱ حمله‌ی متن رمزی به سیستم رمز جایگشتی

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

$$\begin{pmatrix} c_۰ \\ c_d \\ \vdots \\ c_{(\ell-۱)d} \end{pmatrix}, \begin{pmatrix} c_۱ \\ c_{d+۱} \\ \vdots \\ c_{(\ell-۱)d+۱} \end{pmatrix}, \cdots, \begin{pmatrix} c_{d-۱} \\ c_{۲d-۱} \\ \vdots \\ c_{\ell d+(\ell-۱)} \end{pmatrix}.$$

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

۲ رمز هیل

تعریف ۴ *سیستم رمز هیل*[۳]*، یک سه تایی* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *به همراه فضای پیام*

$$\mathcal{M} = (\{۰, \cdots, ۲۵\})^{d})^{*}$$

است که:

- $\mathsf{Gen}()$ *: یک ماتریس تصادفی و معکوس‌پذیر* $K_{d\times d}$ *به پیمانه ی* ۲۶ *تولید می کند، که* d *طول بلوک است.*

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

$$\begin{aligned} \mathsf{Enc}_K(m_۱, \cdots, m_{ld}) &= c_۱, \cdots, c_{ld} \\ \begin{pmatrix} c_{id+۱} \\ \vdots \\ c_{id+d} \end{pmatrix} &= K \begin{pmatrix} m_{id+۱} \\ \vdots \\ m_{id+d} \end{pmatrix} \mod ۲۶ \\ \mathsf{Dec}_K(c_۱, \cdots, c_{ld}) &= m_۱, \cdots, m_{ld} \\ \begin{pmatrix} m_{id+۱} \\ \vdots \\ m_{id+d} \end{pmatrix} &= K^{-۱} \begin{pmatrix} c_{id+۱} \\ \vdots \\ c_{id+d} \end{pmatrix} \mod ۲۶. \end{aligned}$$

نکته ۱ *رمز جایگشتی 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.*

نکته ۲ *بیاد بیاورید که عدد صحیح* a *در هنگ* m *دارای معکوس است (یعنی معادله‌ی* $ax = b \mod m$ *دارای جواب یکتا است)، اگر و تنها اگر* $\gcd(a, m) = ۱$*. این نتیجه قابل تعمیم به حالت ماتریسی نیز هست: ماتریس* A *روی* $\mathbb{Z}_m$ *معکوس‌پذیر است یعنی (معادله‌ی* $AX = B \mod m$ *دارای جواب یکتا است)، اگر و تنها اگر* $\gcd(\det A, m) = ۱$*. بنابر این ماتریس* K *که به عنوان کلید برای رمز هیل تولید می‌شود، معکوس‌پذیر است اگر و فقط اگر* $\gcd(\det K, ۲۶) = ۱$ *باشد.*

[۳] Hill Cipher, 1929.

نکته ۳ *تعداد ماتریس‌های معکوس‌پذیر روی $\mathbb{Z}_{۲۶}$ برابر است با*

$$۲۶^{d^۲}\prod_{i=۱}^{d}(۱-\frac{۱}{۲^i})\prod_{i=۱}^{d}(۱-\frac{۱}{۱۳^i}) \geq ۲^{۴/۷d^۲-۱/۸} \geq ۰/۲۹ \times ۲^{۴/۷d^۲}\ .$$

به عبارت دیگر احتمال اینکه یک ماتریس تصادفی روی $\mathbb{Z}_{۲۶}$ معکوس‌پذیر باشد حداقل ۰/۲۹ است.

برای اثبات رابطه فوق ضمیمه آ را ببینید. به طور مثال به ازای $d = ۸$ اندازه فضای کلید برابر $۲^{۲۹۹}$ است که عدد بسیار بزرگی است. طول کلید رمزهای مدرن معمولا کمتر از ۲۵۶ بیت است.

مثال ۵ *فرض کنید در سیستم رمز هیل داشته باشیم $d = ۲$ و $K = \begin{pmatrix} ۱۱ & ۸ \\ ۳ & ۷ \end{pmatrix}$. برای رمزگذاری پیام* `letusfly` *، ابتدا متن اصلی را به بلوک‌های به طول $d = ۲$ تقسیم و به صورت بردارهایی روی $(\mathbb{Z}_{۲۶})^۲$ به صورت زیر نمایش می‌دهیم:*

$$\begin{pmatrix} ۱۱ \\ ۴ \end{pmatrix}, \begin{pmatrix} ۱۹ \\ ۲۰ \end{pmatrix}, \begin{pmatrix} ۱۸ \\ ۵ \end{pmatrix}, \begin{pmatrix} ۱۱ \\ ۲۴ \end{pmatrix}.$$

سپس ماتریس متن اصلی $M = \begin{pmatrix} ۱۱ & ۱۹ & ۱۸ & ۱۱ \\ ۴ & ۲۰ & ۵ & ۲۴ \end{pmatrix}$ را تشکیل داده و مقدار

$$C = K \cdot M \mod ۲۶ = \begin{pmatrix} ۲۳ & ۵ & ۴ & ۱ \\ ۹ & ۱۵ & ۱۱ & ۱۹ \end{pmatrix}$$

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

$$K^{-۱} = \begin{pmatrix} ۷ & ۱۸ \\ ۲۳ & ۱۱ \end{pmatrix}$$

و

$$K^{-۱} \cdot C = \begin{pmatrix} ۱۱ & ۱۹ & ۱۸ & ۱۱ \\ ۴ & ۲۰ & ۵ & ۲۴ \end{pmatrix}$$

که نمایش متن اصلی اولیه است.

۱.۲ حمله‌ی متن اصلی معلوم به سیستم رمز هیل

سیستم رمز هیل در مقابل حمله‌ی متن رمزی مقاوم است ولی 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 $d \times ۱$ متناظر باهر بلوک را کنار یک دیگر قرار داده در این صورت به ماتریس متن اصلی $d \times t$ 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 ی ۲۶ را حساب کنیم، یعنی:

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

نکته ۴ *روش فوق به شرطی قابل اجرا است که ماتریس M معکوس پذیر باشد (روی $\mathbb{Z}_{26}$)، یعنی*

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

به طور مثال به ازای $d = 5$ اگر پیام‌ها تصادفی انتخاب شوند، احتمال موفقیت با توجه به نکته ۳، برابر ۰/۲۹ خواهد بود.

۳ رمزنگاری سنتی و مدرن

رمزنگاری سنتی

روند رمزنگاری سنتی به‌صورت زیر بوده است:

۱. شخصی یک رمز طراحی می‌کند،

۲. ادعا می کند در برابر حملات شناخته شده امن است،

۳. رمز مورد استفاده قرار می گیرد،

۴. رمز شکسته می شود،

۵. رمز اصلاح می شود و ...

در رمزنگاری سنتی روند بالا پی‌درپی در حال اجرا است.

رمزنگاری مدرن

رمزنگاری مدرن یک علم است که مبتنی بر اصول زیر است:

۱. ارائه یک تعریف دقیق از عنصر رمزنگاری

۲. ارائه یک تعریف دقیق از امنیت

۳. ارائه‌ی یک ساختار

۴. اثبات امنیت تحت فرضیات مقبول (مانند تجزیه اعداد، لگاریتم گسسته و ...)

در این روش وقتی یک سیستم شکسته می‌شود کافی است مدل یا فرضیات را اصلاح کرد. تجربه نشان داده است که با تمرکز روی مدل‌ها و فرضیات می‌توان مدل‌ها را به مدل واقعی بسیار نزدیک کرد و فرضیات معقولی را نیز پذیرفت.

۴ امنیت

ببینیم به صورت شهودی چه انتظاراتی از یک سیستم رمز "امن" داریم و چگونه می‌توان یک تعریف رسمی از امنیت مبتنی بر این انتظارات حداقلی ارائه کرد.

۱. حمله‌کننده نتواند کلید را به‌دست آورد.

- این تعریف نمی‌تواند تعریف خوبی باشد، زیرا ممکن است یک سیستم به این صورت تعریف کنیم که رمز شده‌ی متن m برابر m است و کلید k یک رشته تصادفی با توزیع یکنواخت روی رشته‌های n بیتی به ازای nهای بزرگ است، در این صورت یافتن کلید در عمل غیرممکن است زیرا احتمال موفقیت $\frac{۱}{۲^n}$ است درحالی‌که متن رمزی کل اطلاعات راجع به متن اصلی را به ما می‌دهد.

۲. حمله‌کننده نتواند متن اصلی متناظر با یک متن رمزی را بدست آورد.

- این تعریف خوب نیست، چراکه امکان دارد قسمتی از متن اصلی را بدست آورد.

۳. حمله‌کننده نتواند هیچ بیتی از متن اصلی را بدست آورده یا حدس بزند.

- این تعریف خوب نیست، چراکه امکان دارد رابطه ای بین بیت‌های مختلف بدست آورد

۴. حمله‌کننده نتواند هیچ اطلاعاتی (حتی جزئی) از متن اصلی را بدست آورد.

- یک تعریف "قابل قبول" از امنیت باید حتی‌الامکان این خواسته را برآورده سازد.

تعریف ۶ (امنیت کامل) *فرض کنید $\mathcal{M}$ و $\mathcal{C}$ به ترتیب فضای متن اصلی و فضای متن رمزی باشند، در این صورت گوییم سیستم رمز $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ روی فضای $\mathcal{M}$ دارای امنیت کامل است اگر برای هر توزیع احتمال دلخواه روی $\mathcal{M}$ و هر $m \in \mathcal{M}$ و هر $c \in \mathcal{C}$ داشته باشیم:*

$$\Pr\{M = m | C = c\} = \Pr\{M = m\}.$$

که M و C به ترتیب بیانگر متغرهای تصادفی متن اصلی و متن رمزی هستند.

دقت کنید که آنگونه که ما فضای رمز، $\mathcal{C}$، را تعریف کردیم، به ازای هر $c \in \mathcal{C}$ داریم $\Pr\{C = c\} > ۰$ و لذا احتمال شرطی تعریف شده است. این تعریف را اولین بار شانون[۴] در سال ۱۹۴۸ برای امنیت ارائه کرد و تنها حمله‌ای را مدل می‌کند که مهاجم دارای توان محاسبه‌ی نامحدود و همچنین تنها قابلیت شنود داشته و فقط یک متن رمزی را دریافت کرده است.

[۴] C. E. Shannon: A mathematical theory of communication. Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October, 1948

آ فضای کلید سیستم رمز هیل

هدف از این قسمت محاسبه تعداد ماتریس‌های معکوس پذیر روی $\mathbb{Z}_m$، $m \in \mathbb{N}$ برای حالت خاصی که m حاصل‌ضرب 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 معکوس‌پذیر 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 پیمانه‌ی 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 $p^d - 1$ تا انتخاب برای ستون اول داریم. حال فرض کنید که i ستون اول مستقل خطی $c_1 c_2 \cdots c_i$ ساخته‌ایم، برای ساخت ستون $i+1$ ام، این ستون باید از i ستون قبلی مستقل خطی باشد یا به‌عبارت‌دیگر ترکیب خطی از i ستون قبلی نباشد (یا به‌عبارت‌دیگر وجود نداشته باشد $\alpha_1, \cdots, \alpha_i$ که $c_{i+1} = \alpha_1.c_1 + \cdots + \alpha_i.c_i$)، پس $(p^d - p^i)$ حالت برای انتخاب ستون $i+1$ داریم زیرا هر α_i، p حالت دارد؛ بنابراین تعداد کل ماتریس‌های معکوس‌پذیر $d \times d$ روی $\mathbb{Z}_p$ برابر است با $\prod_{i=0}^{d-1}(p^d - p^i)$.
■

قضیه ۲ *اگر $p_1, \ldots, p_\ell$ اعداد اول متمایز و $d \in \mathbb{N}$ در این صورت تعداد ماتریس‌های معکوس‌پذیر $d \times d$ روی $\mathbb{Z}_m$ که $m = \Pi_{k=1}^{\ell} p_k$ 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 مجموعه‌ی ماتریس‌های معکوس‌پذیر روی $\mathbb{Z}_{p_1 p_2 \cdots p_\ell}$ به ℓ-تایی‌های مرتب که مؤلفه‌ی kام آن ماتریس‌های معکوس‌پذیر 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 ولم ۱ تعداد ماتریس‌های معکوس‌پذیر روی $\mathbb{Z}_{p_1 p_2 \cdots p_\ell}$ برابر $\prod_{i=0}^{d-1}(p_1^d - p_1^i) \times \cdots \times \prod_{i=0}^{d-1}(p_2^d - p_\ell^i)$ است و حکم ثابت است.
■

نتیجه ۷ *تعداد ماتریس‌های معکوس‌پذیر روی $\mathbb{Z}_{26}$ برابر است با*

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

.

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