به نام خدا

دانشکده‌ی علوم ریاضی

مقدمه‌ای بر رمزنگاری ۲۹ بهمن ۱۳۹۱

جلسه‌ی ۴: تعریف امنیت کامل

مدرس: دکتر شهرام خزائی *نگارنده: فاطمه سادات ذبیحی*

هدف ما در این جلسه ارائه تعریفی برای مفهوم امنیت کامل برای سیستم رمز متقارن می‌باشد، یعنی وقتی حمله‌کننده متن رمز شده را ببیند نتواند هیچ اطلاعاتی راجع به متن اصلی کسب کند.

۱ امنیت کامل

به طور ایده‌ال، متن رمز شده[۱] نباید اطلاعات اضافه‌ای درباره متن اصلی[۲] به مهاجم بدهد. به عبارت دیگر، وقتی شنودگر یک متن رمزشده را شنود می‌کند، نباید ابهام او نسبت به متن اصلی کاهش یابد. تعریف امنیت کامل[۳] که در ادامه می‌آید از این شهود حاصل شده است. این تعریف به امنیت شانون[۴] یا امنیت تئوری اطلاعاتی[۵] نیز معروف است که اولین بار توسط شانون، مبدع تئوری اطلاعات، در سال ۱۹۴۸ ارائه شد.

تعریف ۱ (امنیت کامل) *سیستم رمز متقارن* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *روی فضای پیام* $\mathcal{M}$ *دارای امنیت کامل است اگر برای هر توزیع دلخواه روی* $\mathcal{M}$*، هر متن اصلی* $m \in \mathcal{M}$ *و هر متن رمزشده* $c \in \mathcal{C}$ *داشته باشیم:*

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

که $\mathbf{M}$ *و* $\mathbf{C}$ *به‌ترتیب بیانگر متغیرهای تصادفی متن اصلی و متن رمزی هستند. دقت کنید متغیر تصادفی* $\mathbf{C}$ *به متغیر تصادفی* $\mathbf{M}$ *و بیت‌های تصادفی که الگوریتم تولید کلید و (احیاناً) الگوریتم رمزنگاری استفاده می‌کند، وابسته است.*

توجه داشته باشید که در هر سیستم رمز دلخواه الگوریتم‌های تولید کلید و رمزنگاری به‌همراه فضای متن اصلی $\mathcal{M}$، فضاهای کلید و متن رمزشده را مشخص می‌کنند. تعریف فوق حمله‌ای را مدل می کند که مهاجم فقط قابلیت شنود دارد و فقط یک متن رمز شده می‌بیند که طبق این تعریف مهاجم چه متن رمز شده را ببیند و چه نبیند با یک احتمال متن اصلی را می‌تواند حدس بزند.
یک تعریف معادل از امنیت کامل در لم زیر آمده است. به طور شهودی، این تعریف بیان می‌کند که اگر در یک سیستم امن کامل، حمله‌کننده بتواند با دیدن متن رمز شده (متناظر با پیامی که قرار است ارسال شود) اطلاعاتی کسب کند، بدون دیدن متن رمز شده هم می‌تواند همان میزان اطلاعات کسب کند.

---
[۱] ciphertext
[۲] plaintext
[۳] perfect secrecy
[۴] Shannon
[۵] information-theoretic security

لم ۱ *سیستم رمز متقارن* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *روی فضای متن اصلی* $\mathcal{M}$ *دارای امنیت کامل است، اگر و تنها اگر برای هر توزیع دلخواه روی فضای پیام* $\mathcal{M}$*، هر متن اصلی* $m \in \mathcal{M}$ *و هر متن رمزشده* $c \in \mathcal{C}$ *رابطه زیر برقرار باشد:*

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

برهان. دو طرف تساوی را ضرب می‌کنیم در $\frac{\Pr\{\mathbf{M}=m\}}{\Pr\{\mathbf{C}=c\}}$. بدین صورت :

$$\Pr\{\mathbf{C} = c | \mathbf{M} = m\} \times \frac{\Pr\{\mathbf{M} = m\}}{\Pr\{\mathbf{C} = c\}} = \Pr\{\mathbf{C} = c\} \times \frac{\Pr\{\mathbf{M} = m\}}{\Pr\{\mathbf{C} = c\}}$$

که با استفاده از قاعده احتمال بیز به صورت زیر ساده می‌شود

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

باتوجه به اینکه در انتها به تعریف ۱ رسیدیم، امنیت کامل در این شرایط برقرار می‌باشد. ■
تعریف معادل دیگری از امنیت کامل در زیر آمده است. این تعریف از این منظر که دیگر به توزیع احتمال روی فضای پیام $\mathcal{M}$ اشاره نمی‌کند، ساده‌تر است.

لم ۲ *سیستم رمز متقارن* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *روی فضای متن اصلی* $\mathcal{M}$ *دارای امنیت کامل است، اگر و تنها اگر برای هر زوج متن اصلی* $m_0, m_1 \in \mathcal{M}$ *و هر متن رمزشده* $c \in \mathcal{C}$ *رابطه زیر برقرار باشد:*

$$\Pr\{\mathbf{C} = c | \mathbf{M} = m_0\} = \Pr\{\mathbf{C} = c | \mathbf{M} = m_1\}$$

برهان. ابتدا طرف اول را ثابت می‌کنیم. طبق لم ۱ اگر سیستم امن کامل باشد، به ازای هر زوج پیام دلخواه $m_0, m_1 \in \mathcal{M}$ داریم:

$$\Pr\{\mathbf{C} = c | \mathbf{M} = m_0\} = \Pr\{\mathbf{C} = c\}$$

و

$$\Pr\{\mathbf{C} = c | \mathbf{M} = m_1\} = \Pr\{\mathbf{C} = c\}$$

از برابری طرف راست آنها نتیجه می‌گیریم

$$\Pr\{\mathbf{C} = c | \mathbf{M} = m_0\} = \Pr\{\mathbf{C} = c | \mathbf{M} = m_1\}$$

حال طرف دوم را ثابت می‌کنیم. یک توزیع دلخواه روی فضای پیام $\mathcal{M}$ در نظر بگیرید. برای هر $m_0 \in \mathcal{M}$ و هر $c \in \mathcal{C}$ داریم:

$$\begin{aligned} \Pr\{\mathbf{C} = c\} &= \textstyle\sum_{m \in \mathcal{M}} \Pr\{\mathbf{C} = c | \mathbf{M} = m\} \Pr\{\mathbf{M} = m\} \\ &= \Pr\{\mathbf{C} = c | \mathbf{M} = m_0\} \textstyle\sum_{m \in \mathcal{M}} \Pr\{\mathbf{M} = m\} \\ &= \Pr\{\mathbf{C} = c | \mathbf{M} = m_0\} \end{aligned}$$

پس به ازای هر پیام اصلی دلخواه رابطه موجود در لم ۱ برقرار است در نتیجه طبق لم ۱ سیستم امن کامل است. ■

۲ رمز یکبار مصرف

تعریف ۲ (رمز یکبار مصرف (OTP[۶]) یا ورنام[۷]) *سیستم رمز رمز یکبار مصرف یک سیستم رمز متقاران است که در آن فضای کلید و فضای متن اصلی مجموعه‌ی همه رشته‌های n- بیتی هستند، یعنی $\mathcal{M} = \mathcal{K} = \{۰,۱\}^n$، و الگوریتم‌های تولید کلید، رمزگذاری و رمزگشایی به صورت زیر تعریف می‌شوند.*

- Gen *یک رشته تصادفی k از $\mathcal{K}$ تولید می‌کند.*
- Enc *پیام اصلی $m \in \mathcal{M}$ و کلید $k \in \mathcal{K}$ را می‌گیرد و متن رمزی $c = m \oplus k$ را تولید می‌کند.*
- Dec *ورودی c و کلید k را می‌گیرد و اگر $c \in \mathcal{C} = \{۰,۱\}^n$ متن اصلی $m = c \oplus k$ را تولید می‌کند.*

قضیه ۳ *رمز یکبارمصرف دارای امنیت کامل است.*

برهان. فرض کنید $\mathbf{M}$ بیانگر متغیر تصادفی خروجی الگوریتم تولید کلید باشد. به ازای هر $m \in \mathcal{M}$ و هر $c \in \mathcal{C}$ داریم:

$$\begin{aligned} \Pr\{\mathbf{C} = c | \mathbf{M} = m\} &= \Pr\{\mathbf{M} \oplus \mathbf{K} = c | \mathbf{M} = m\} \\ &= \Pr\{\mathbf{K} = m \oplus c\} \\ &= \frac{۱}{۲^n} \end{aligned}$$

مشاهده می‌شود که متن رمزی مستقل از متن اصلی دارای توزیع یکنواخت است.

■

برای ارسال امن یک پیام با استفاده از سیستم رمز ورنام، باید دو طرف یک کلید کاملاً تصادفی به همان طول از قبل با یکدیگر به اشتراک بگذارند. این امر یک مشکل اساسی برای استفاده عملی از این سیستم، به جز در مواقع خاصی که امکان اشتراک گذاری کلید وجود داشته باشد، به حساب می‌آید. لازم به تأکید است که فقط یکبار از هر کلیدی می‌توان برای ارسال فقط یک پیام استفاده کرد. برای درک این موضوع، فرض کنید شنودگر متن‌های رمزی $c_۲$ و $c_۱$ را که رمز شده پیام‌های $m_۲$ و $m_۱$ تحت کلید یکسان k هستند، دریافت کرده باشد. روابط

$$\begin{aligned} c_۱ &= \mathsf{Enc}_k(m_۱) = m_۱ \oplus k \\ c_۲ &= \mathsf{Enc}_k(m) = m_۲ \oplus k \end{aligned}$$

نشان می‌دهد از روی xor متن‌های رمزی می‌توان xor متن‌های اصلی را حدس به‌دست آورد:

$$c_۱ \oplus c_۲ = m_۱ \oplus k \oplus m_۲ \oplus k = m_۱ \oplus m_۲$$

قضیه ۴ (شانون) *اگر سیستم رمز $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ روی فضای $\mathcal{M}$ دارای امنیت کامل باشد، آن‌گاه $|\mathcal{K}| \geq |\mathcal{M}|$ که $\mathcal{K}$ فضای کلیدهای تولیدشده توسط* Gen *است.*

۳ آزمایش تمایزناپذیری در برابر مهاجم شنودگر

بیان دیگری از لم ۲ را بدین صورت می‌توان ارائه کرد. فرض کنید $\mathbf{K}$ متغیر تصادفی بیان‌گر خروجی الگوریتم تولید کلید باشد. در اینصورت $\mathbf{C}_۰ = \mathsf{Enc}_{\mathbf{K}}(m_۰)$ و $\mathbf{C}_۱ = \mathsf{Enc}_{\mathbf{K}}(m_۱)$ به‌ترتیب بیان‌گر متغیرهای تصادفی متناظر با متن رمزشده پیام‌های $m_۰$ و $m_۱$ هستند. دقت کنید که این متغیرهای تصادفی صرفاً به توزیع $\mathbf{K}$ (که خود به مقادیر تصادفی که الگوریتم تولید کلید استفاده می‌کند وابسته است) و مقدار تصادفی که (احیاناً) الگوریتم رمزنگاری استفاده می‌کند بستگی دارد. تعبیر دیگر لم ۲ این است که توزیع متغیرهای تصادفی $\mathbf{C}_۰$ و $\mathbf{C}_۱$ یکسان است. معادلاً، بین یک نمونه از $\mathbf{C}_۰$ و یک نمونه از $\mathbf{C}_۱$ نمی‌توان تمایزی قائل شد. یعنی اگر مهاجم متن رمزی c را داشته باشد و بداند که حاصل رمزکردن یکی از دو متن $m_۰$ و $m_۱$ است که به تصادف انتخاب شده است، نمی‌تواند با احتمال بهتر از $\frac{۱}{۲}$ حدس بزند که متن اصلی متناظر کدام‌یک است. لازم به تأکید است که این محدودیت برای هر مهاجمی، حتی با قدرت محاسباتی نامحدود، بر قرار است. برای ارائه تعریف دیگری از امنیت کامل برای یک سیستم رمز Π، که مهاجم را به صورت مشهودتری در تعریف لحاظ می‌کند، از یک بازی[۸] (یا آزمایش[۹]) استفاده می‌کنیم که بین یک مهاجم[۱۰]، که با $\mathcal{A}$ نشان داده می‌شود، و یک چالشگر[۱۱] فرضی اجرا می‌شود. این آزمایش که آزمایش تمایزناپذیری تک‌پیامی در برابر مهاجم شنودگر[۱۲] نامیده می‌شود و با $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$ نشان داده می‌شود، به صورت زیر اجرا می‌شود و مهاجمی را که فقط قابلیت شنود یک متن رمز شده (جهت اعمال حمله فقط متن رمزی[۱۳]) را دارد، مدل می‌کند.

۱. چالشگر با اجرای الگوریتم تولید کلید، یک کلید k تولید می‌کند.

۲. مهاجم پیام‌های $m_۰, m_۲ \in \mathcal{M}$ را انتخاب کرده و به چالشگر می‌دهد.

۳. چالشگر بیت تصادفی b را تولید می‌کند.

۴. چالشگر با استفاده از الگوریتم رمزگذاری پیام m_b را تحت کلید k رمز و متن رمزی c را تولید می‌کند.

۵. چالشگر متن رمزی c را به مهاجم $\mathcal{A}$ می‌دهد و مهاجم بیت $\hat{b}$ را بیرون می‌دهد.

مراحل آزمایش فوق به طور خلاصه در آزمایش زیر تعریف شده است.

آزمایش. $[\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}]$ آزمایش امنیت کامل سیستم رمزمتقارن Π در برابر مهاجم شنودگر $\mathcal{A}$ به صورت زیر است:

۱. $k \leftarrow \mathsf{Gen}()$

۲. $m_۰, m_۱ \leftarrow \mathcal{A}()$

۳. $b \leftarrow \{۰, ۱\}$

۴. $c \leftarrow \mathsf{Enc}_k(m_b)$

---

[۸] game
[۹] experiment
[۱۰] Adversary
[۱۱] challenger
[۱۲] eavesdropper
[۱۳] ciphertext-only attack

۵. $\hat{b} \leftarrow \mathcal{A}(c)$

خروجی آزمایش که با $\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$ نشان داده می‌شود برابر یک در نظر گرفته می‌شود اگر $\hat{b} = b$ و صفر است اگر $\hat{b} \neq b$. دقت کنید که خروجی آزمایش یک متغیر تصادفی است که به کلیه بیت‌های تصادفی که در آزمایش و الگوریتم‌ها مورد استفاده قرار می‌گیرد بستگی دارد، که عبارتند از:

- مقدار تصادفی که در الگوریتم تولید کلید در مرحله ۱ به‌کار می‌رود.
- مقادیر تصادفی که مهاجم (احیاناً) در مراحل ۲ و ۵ استفاده می‌کند.
- بیت تصادفی که چالشگر در مرحله ۳ انتخاب می‌کند.
- مقدار تصادفی که (احیاناً) در الگوریتم رمزگذاری در مرحله ۴ به‌کار می‌رود.

با استفاده از آزمایش فوق می‌توان یک تعریف معادل از امنیت کامل ارائه کرد.

لم ۵ *یك سیستم دارای امنیت کامل است اگر به ازای هر مهاجم $\mathcal{A}$ که در آزمایش بالا شرکت کند، احتمال موفقیت‌اش دقیقاً $\frac{۱}{۲}$ باشد. یعنی:*

$$\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = ۱\} = \frac{۱}{۲}\,. \qquad (۱)$$

به طور شهودی، تفسیر مفهوم امنیت کامل با استفاده از آزمایش فوق بدین صورت است: در یک سیستم با امنیت کامل وقتی مهاجم یک متن رمزی را می‌بیند، حتی اگر بداند که رمزشده یکی از دو پیامی است که خود او انتخاب کرده است، نمی‌تواند تشخیص دهد که متن رمزی، رمزشده کدامیک از آن دو پیام است. در واقع بهترین کاری که مهاجم برای کسب اطلاعات در مورد متن اصلی می‌تواند بکند، حدس یکی از دو پیام انتخاب شده به تصادف است.

نکته ۱ *اگر در لم ۵ رابطه ۱ را با نامساوی زیر جایگزین شود باز هم لم معتبر است:*

$$\Pr\{\mathsf{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = ۱\} \leq \frac{۱}{۲}\,.$$