مدرس: دکتر مجتبی رفیعی نیمسال دوم ۱۴۰۰-۱۴۰۱

رمزنگاری

جلسه ۱۸: مفاهیم امنیتی رمزنگاری کلید عمومی

۱۵ خرداد ۱۴۰۱

فهرست مطالب

هدف ما در این جلسه ارائه تعریفی برای مفهوم رمز نامتقارن[1] و بررسی امنیت آن می‌باشد.

۱ سیستم رمز نامتقارن

تا اینجا برای رمزگذاری و رمزگشایی از یک کلید مشترک استفاده کردیم. به همین جهت به آن سیستم رمزنگاری متقارن گویند که تنها به یک کانال امن برای انتقال کلید نیاز دارد. در ادامه سیستم رمزنگاری نامتقارن یا سیستم رمزنگاری با کلید عمومی[2] را معرفی می‌کنیم. در این سیستم دو کلید متفاوت به نام کلید عمومی[3] و کلید خصوصی[4] (یا کلید مخفی[5]) وجود دارد، که کلید عمومی در دسترس همگان است ولی کلید خصوصی را تنها گیرنده پیام دارد.

[1] asymmetric cryptography
[2] public-key cryptography
[3] public-key
[4] private-key
[5] secret-key

تعریف ۱ *سیستم رمز نامتقارن یک سه‌تایی مرتب به صورت* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *روی فضای متن* $\mathcal{M}$ *از الگوریتم‌های چند جمله‌ای تصادفی* (PPT)[6] *است و الگوریتم‌های آن بدین صورت تعریف می‌شوند:*

- Gen *الگوریتم تولید کلید است که با ورودی* 1^n *زوج مرتب* (pk, sk) *را که به ترتیب کلید عمومی و کلید خصوصی هستند، تولید می‌کند.*

$$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

- Enc *الگوریتم رمزگذاری است که با داشتن کلید عمومی* pk *و متن* $m \in \mathcal{M}$ *به عنوان ورودی، متن رمز شده* c *را تولید می‌کند.*

$$c \leftarrow \mathsf{Enc}_{pk}(m)$$

- Dec *الگوریتم رمزگشایی است که قطعی است و با داشتن کلید خصوصی* sk *و متن رمز شده* c*، متن* $m \in \mathcal{M} \cup \{\perp\}$ *را تولید می‌کند.*

$$m \leftarrow \mathsf{Dec}_{sk}(c)$$

- *به ازای همه‌ی* $n \in \mathbb{N}$ *و* $m \in \mathcal{M}$

$$\Pr[(sk, pk) \leftarrow \mathsf{Gen}(1^n) : \mathsf{Dec}_{sk}(\mathsf{Enc}_{pk}(m)) = m] = 1$$

نکته ۱ *خروجی تابع* Dec *در فضای* $\mathcal{M} \cup \{\perp\}$ *است که* $\perp$ *تنها وقتی خروجی خواهد بود که متن ورودی* c *نامعتبر باشد.*

۱.۱ امنیت رمز نامتقارن

بیاد بیاورید که شانون امنیت کامل برای سیستم رمز متقارن را با استفاده از تمایزناپذیری توزیع‌های زیر برای هر زوج پیام دلخواه m_0 و m_1 در فضای پیام تعریف کرد:

$$\{k \leftarrow \mathsf{Gen}(1^n) : \mathsf{Enc}_k(m_0)\}$$
$$\{k \leftarrow \mathsf{Gen}(1^n) : \mathsf{Enc}_k(m_1)\}$$

ابتدا توجه کنید که کلید عمومی سیستم رمز نامتقارن در اختیار همه، از جمله مهاجم، قرار می‌گیرد. بنابراین اگر علاقه‌مند به تعریف امنیت کامل برای سیستم رمز نامتقارن باشیم، به طور طبیعی باید سیستمی را امن کامل در نظر بگیریم که برای هر زوج پیام دلخواه m_0 و m_1 در فضای پیام آن، توزیع‌های زیر تمایزناپذیر باشند:

$$\{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : \langle pk, \mathsf{Enc}_{pk}(m_0)\rangle\} \tag{۱}$$

$$\{(pk, sk) \leftarrow \mathsf{Gen}(1^n) : \langle pk, \mathsf{Enc}_{pk}(m_1)\rangle\} \tag{۲}$$

قضیه ۱ (امکان‌ناپذیری امنیت کامل) *سیستم رمز نامتقارن با امنیت کامل وجود ندارد.*

برهان. یک زوج کلید عمومی و متن رمز شده را در نظر بگیرید. با توجه به شرط صحت رمزگشایی، امکان رمزگشایی متن رمز شده به دو متن متفاوت وجود ندارد. بنابراین وقتی یک متن دلخواه با استفاده از یک مقادیر تصادفی تحت کلید عمومی pk به یک متن رمز شده c تبدیل شده باشد، هیچ متن اصلی دیگری تحت هیچ مقدار تصادفی با استفاده از همان کلید pk به متن رمزشده c تبدیل نخواهد شد. لذا مهاجم با منابع نامحدود[7] می‌تواند به راحتی پیام m_0 و m_1 را با همه مقادیر تصادفی که الگوریتم Enc استفاده می‌کند تحت کلید عمومی دریافتی رمز کرده و با مقایسه آنها با متن رمزی دریافتی، متن اصلی صحیح را تشخیص دهد. ■

بنابراین برای سیستم رمز نامتقارن باید به امنیت محاسباتی بسنده کرد. همانند سیستم رمز متقارن می‌توان امنیت تک‌پیامی محاسباتی را بر مبنای تمایزناپذیری محاسباتی توزیع‌های (۱) و (۲) تعریف نمود. بجای این کار، امنیت را با استفاده از آزمایش که به دنبال می‌آید تعریف می‌کنیم که امنیت تک‌پیامی محاسباتی را نتیجه می‌دهد.

[6] probabilistic polynomial time
[7] unbounded adversary

آزمایش.[$\mathsf{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}$] آزمایش امنیت تک‌پیامی برای سیستم رمز نامتقارن Π در برابر مهاجم $\mathcal{A}$ به صورت زیر است:

۱. چالشگر با اجرای الگوریتم تولید کلید، کلید عمومی pk و کلید خصوصی sk، را تولید می‌کند.

$$(pk, sk) \leftarrow \mathsf{Gen}(1^n)$$

۲. مهاجم $\mathcal{A}$ با دریافت کلید pk دو پیام m_0 و m_1 از فضای $\mathcal{M}$، که $|m_0| = |m_1|$، را تولید می‌کند و به چالشگر بر می‌گرداند.

$$(m_0, m_1) \leftarrow \mathcal{A}(pk)$$

۳. چالشگر یک بیت تصادفی انتخاب می‌کند.

$$b \leftarrow \{0, 1\}$$

۴. چالشگر متن رمزی c، که رمز شده متن اصلی m_b تحت کلید pk است را محاسبه می‌کند و برای چالشگر می‌فرستد.

$$c \leftarrow \mathsf{Enc}_{pk}(m_b)$$

۵. مهاجم با گرفتن متن رمز شده c، بیت $\hat{b}$ را تولید می‌کند.

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

خروجی آزمایش که با $\mathsf{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n)$ نشان داده می‌شود برابر ۱ است اگر $b = \hat{b}$ و صفر است اگر $\hat{b} \neq b$.

تعریف ۲ (امنیت تک پیامی در سیستم رمز نامتقارن) *سیستم رمز نامتقارن* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *دارای امنیت تک‌پیامی است اگر برای هر مهاجم چندجمله‌ای احتمالاتی مانند* $\mathcal{A}$ *تابع ناچیز* $\epsilon(n)$ *وجود داشته باشد که*

$$\Pr\{\mathsf{PubK}^{\mathrm{eav}}_{\mathcal{A},\Pi}(n) = 1\} \leq \frac{1}{2} + \epsilon(n)$$

تفاوت تعریف بالا، با تعریف‌های مشابه در سیستم رمزهای متقارن، در این است که کلید عمومی به مهاجم داده می‌شود که خودبه‌خود دسترسی اوراکلی به الگوریتم رمزنگاری را برای او فراهم می‌سازد. بنابراین، امنیت تک‌پیامی، امنیت متن اصلی انتخابی را نیز نتیجه می‌دهد. همانند سیستم رمزنگاری متقارن، می‌توان تعاریف را به امنیت چندپیامی گسترش داد. می‌توان نشان داد داریم در سیستم رمز نامتقارن امنیت چندپیامی با امنیت تک‌پیامی معادل است.

قضیه ۲ (معادل‌بودن امنیت‌ها) *سیستم رمز نامتقارن امن تک‌پیامی، داری امنیت چندپیامی و متن اصلی انتخابی است.*

در سیستم‌های رمز نامتقارن نمی‌توان از الگوریتم‌های رمزنگاری قطعی استفاده کرد، زیرا اگر الگوریتم رمزنگاری قطعی باشد آنگاه چون مهاجم کلید عمومی را در اختیار دارد، می‌تواند رمز شده‌ی m_0 و m_1 را بدست آورد و با متن رمز شده مقایسه کند و به احتمال ۱ جواب صحیح را برگرداند.

قضیه ۳ (لزوم رمزنگاری‌تصادفی) *سیستم رمز نامتقارن با الگوریتم رمزنگاری قطعی، امنیت تک‌پیامی ندارد.*