جلسه سوم :

قضیه شانون :

$\pi = (Gen, Enc, Dec)$ over $\mathcal{M}$

$|\mathcal{M}| = |K| = |C|$

is Perfect-secure $\iff$

1. $\forall k \in K : Pr[K=k] = \frac{1}{|K|}$
2. $\forall m \in \mathcal{M}, \forall c \in C \quad \exists! \, k \in K :$ $Enc_k(m) = c$

تعریف امنیت کامل:

$\forall m, c \quad Pr[C=c] > 0 :$

$Pr[M=m \mid C=c] = Pr[M=m]$

معادل $Pr[Enc_k(m)=c] = Pr[Enc_k(m')=c]$

فصل ۳ :

امنیت کامل $\rightarrow$ $|K| \geq |M|$

امنیت کامل $\rightarrow$ هیچ اطلاعاتی نمیده $\rightarrow$ برای مهاجم نامحدود کارسختی است (information-theoretical)

$\rightarrow$ مهاجم محدود نشود (توان محاسباتی مهاجم را کم کنیم)

ریلکس کردن تعریف امنیت کامل :

۱. برای مهاجم کارا (efficient)

↑ زمان اجرای مهاجم

۲. کم کردن احتمال برنده شدن مهاجم در آزمایش امنیت

negligible

۲ روش :

1. $\Pi = (Gen, Enc, Dec)$ is (t, ε)-secure

اگر مهاجم زمان اجرای t داشته باشد، ماکیمم با احتمال ε در آزمایش است موفق می‌شود.

→ Concrete Approach

← کاربرد: طراحی سیستم های عملی

2. Asymptotic Approach: پارامتر امنیت سیستم : n

مثال : $n = |k|$

مهاجم کارا ← زمان اجرا = $p(n)$ که p چندجمله‌ای

↑ می‌تونه تصادفی باشه (دسترسی به randomness)

کم بودن احتمال موفقیت ← negligble(n)

↑ کوچکتر از معکوس هر چند جمله‌ای

* سیستم امنه اگر برای هر مهاجم چندجمله‌ای تصادفی (PPT) احتمال شکسته شدن سیستم حداکثر برابر ناچیز (negligble) باشه.

PPT : Probabilistic Polynomial-Time

Asymptotic Approach:

- مهاجم A کارآست ← برای هر ورودی x

$A(x)$ در $p(|x|)$ گام اجرا می‌شود. (p چندجمله‌ای است)

- مهاجم A در همه‌ی کارها به یک عدد کاملا تصادفی دسترسی دارد.

"تصادفی بودن A"

- ناچیز بودن احتمال موفقیت A در آزمایش امنیت

تعریف توابع ناچیز (negligible):

$f: \mathbb{N} \to \mathbb{R}^{>0}$ is negligible if $\forall$ polynomial p

$\exists N$ such that $\forall n > N: f(n) < \frac{1}{p(n)}$

مثل n^{-c} که c ثابت است

مثال: 2^{-n}, $2^{-\sqrt{n}}$, $n^{-\log n}$

ویژگی‌های توابع ناچیز:

فرض کنید $negl_1$ و $negl_2$ توابع ناچیز هستند:

1. $negl = negl_1 + negl_2 \to negl$ ناچیزه

2. $p > 0$ is polynomial: $negl = p \cdot negl_1$ ناچیزه

کاربرد: اثبات امنیت پروتکل‌ها

تعریف امنیت ← تعریف شکسته شدن سیستم
← قدرت مهاجم

Asymptotic Approach:

یک سیستم امنه اگر برای هر مهاجم احتمالاتی چندجمله‌ای A (PPT)
احتمال موفقیت A در آزمایش امنیت ناچیز باشد.

---

relaxations of perfect security

concrete Approach
(t,ϵ) - secure
برای طراحی عملی سیستم‌ها

Asymptotic Approach
PPT adversary + negligible func. + security Parameter
برای تحلیل‌های نظری

- تعریف سیستم رمز متقارن (کلید محفی) : private-key encryption

$\Pi = (Gen, Enc, Dec)$ → الگوریتم‌ها PPT ← احتمالاتی چندجمله‌ای

- $Gen(1^n) \to k$ probabilistic , $|k| \geq n$

- $Enc(k, m) \to c$ $m \in \{0,1\}^*$, probabilistic / deterministic

- $Dec(k, c) \to m / \perp$ deterministic

- شرط صحت: $\forall n, \forall k \leftarrow Gen(1^n)$,
$\forall m \in \{0,1\}^*$: $Dec(k, Enc(k,m)) = m$

بررسی آزمایش امنیت :

$PrivK^{eav}_{\pi,A}(n)$:

1. $k \leftarrow Gen(1^n)$
2. $m_0, m_1 \leftarrow A(1^n)$ ، $|m_0| = |m_1|$
3. $c \leftarrow Enc_k(m_b)$ ، $b \xleftarrow{R} \{0,1\}$
4. $b' \leftarrow A(c)$

محاجم A برنده آزمایش است اگر $b = b'$. $(PrivK^{eav}_{\pi,A}(n) = 1)$

← امنیت : سیستم رمز π امن است اگر برای هر محاجم احتمالاتی چندجمله‌ای (PPT) A ،

$$Pr\left[PrivK^{eav}_{\pi,A}(n) = 1\right] \leq \frac{1}{2} + negl(n)$$

→ π is indistinguishable encryption in the presence of an eavesdropper.

تعریف معادل : π در مقابل شنودگر تمایزناپذیر است اگر برای هر محاجم شنودگر A ، تابع ناچیز negl وجود داشته باشد ، به طوری که :

$$\left| Pr\left[out_A(PrivK^{eav}_{A,\pi}(n,0) = 1\right] - Pr\left[out_A(PrivK^{eav}_{A,\pi}(n,1)) = 1\right] \right| \leq negl(n)$$

امنیت معنایی - semantic security