Perfect Secrecy

$\Pi = (Gen, Enc, Dec)$ is perfectly Secure if

for all dist over $\mathcal{M}$,
for all $m \in \mathcal{M}$, for all $c \in \mathcal{C}$

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

(Def^n 1)

(Alternative Def^n)

for all dist over $\mathcal{M}$, for all $m_0, m_1 \in \mathcal{M}$,
for all $c \in \mathcal{C}$,

$$Pr[Enc_k(m_0) = c] = Pr[Enc_k(m_1) = c]$$

(Def^n 2)

Def^n 2 $\Rightarrow$ Def^n 1

$\forall\ m_0, m_1, c$

$$Pr[Enc_K(m_0) = c] = Pr[Enc_K(m_1) = c] = p_c$$

$$Pr[M = m \mid C = c] = \frac{Pr[C = c \mid M = m] \cdot Pr[M = m]}{Pr[C = c]}$$

$$= \frac{Pr[Enc_K(M) = c \mid M = m] \cdot Pr[M = m]}{\sum_{m} Pr[C = c \mid M = m] \cdot Pr[M = m]} = \frac{\cancel{p_c} \cdot Pr[M = m]}{\cancel{p_c}}$$

$$Pr[A] = \sum_i Pr[A \mid B_i] \cdot Pr[B_i]$$

Def^n 1 $\Rightarrow$ Def^n 2

$$Pr[M = m \mid C = c] = Pr[M = m] \quad -(1)$$

To show,

$$Pr[Enc_k(m_0) = c]$$

$$= Pr[C = c \mid M = m_0] = \frac{Pr[M = m_0 \mid C = c] \cdot Pr[C = c]}{Pr[M = m_0]} = Pr[C = c]$$

$\forall\, m_0, m_1$

$$Pr[Enc_k(m_0) = c] = Pr[Enc_k(m_1) = c] = \cdots = Pr[C = c].$$

$Priv^{eav}_{\pi,A}$

Perfect Indistinguishability

Challenger Ch | Adversary A

$K \leftarrow Gen$

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

$m_0, m_1 \in \mathcal{M}$ ←

$c \leftarrow Enc_k(m_b)$

c →

$\hat{b}$ ←

Π is PI if

Adversary wins if $Priv^{eav}_{\pi,A} = 1$ ⇓ $\hat{b} = b$

$$Pr[\text{Adv wins}]$$
$$= Pr[Priv^{eav}_{\pi,A} = 1]$$
$$= Pr[\hat{b} = b]$$
$$= \frac{1}{2}.$$

$$Pr[Enc_k(m_0) = c]$$
$$= Pr[Enc_k(m_1) = c]$$

$Priv^{eav}_{\pi,A}$

Perfect Indistinguishability

Challenger Ch | Adversary A

$K \leftarrow Gen$

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

$m_0, m_1 \in \mathcal{M}$ ←

$c \leftarrow Enc_k(m_b)$

c →

$\hat{b}$ ←

$\Pr[Enc_k(m_0) = c]$

$= \Pr[Enc_k(m_1) = c]$

Adversary wins if $Priv^{eav}_{\pi,A} = 1$ ⟺ $\hat{b} = b$

π is PI if

$\Pr[\text{Adv wins}]$

$= \Pr[Priv^{eav}_{\pi,A} = 1]$

$= \Pr[\hat{b} = b]$

$= \frac{1}{2}$.

One Time Pad

$$\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$$

Gen: $k \xleftarrow{\$} \mathcal{K}$

Enc(k, m): $c = m \oplus k$.
return c.

Dec(k, c): $m = c \oplus k$
return m.

x	y	XOR
0	0	0
0	1	1
1	0	1
1	1	0

$k = k_1 k_2 \cdots k_n$
$m = m_1 m_2 \cdots m_n$
$c = k_1 \oplus m_1 \; k_2 \oplus m_2 \cdots k_n \oplus m_n$

$\forall i,$
$k_i \in \{0,1\}$
$m_i \in \{0,1\}$

OTP achieves Perfect Secrecy

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

$$= \frac{\Pr[C=c \mid M=m] \cdot \Pr[M=m]}{\Pr[C=c]}$$

$$= \frac{\frac{1}{2^n} \cdot \Pr[M=m]}{\frac{1}{2^n}}$$

Key can be used once.

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

$$= \Pr[Enc_k(M)=c \mid M=m]$$

$$= \Pr[Enc_k(m)=c]$$

$$= \Pr[m \oplus k = c]$$

$$= \Pr[k = m \oplus c]$$

$$= \frac{1}{2^n} \quad \left(\text{As } k \xleftarrow{R} \{0,1\}^n\right)$$

OTP achieves Perfect Secrecy

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

$$= \frac{\Pr[C=c \mid M=m] \cdot \Pr[M=m]}{\Pr[C=c]}$$

$$= \frac{\frac{1}{2^n} \cdot \Pr[M=m]}{\frac{1}{2^n}}$$

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

$$= \Pr[Enc_k(M)=c \mid M=m]$$

$$= \Pr[Enc_k(m)=c]$$

$$= \Pr[m \oplus k = c]$$

$$= \Pr[k = m \oplus c]$$

$$= \frac{1}{2^n} \quad \left(\text{As } k \xleftarrow{R} \{0,1\}^n\right)$$

Th^m For any Perfectly Secure encryption scheme,

$$|\mathcal{K}| \geq |\mathcal{M}|.$$

Assume that $|\mathcal{K}| < |\mathcal{M}|$. Then we have to show that the scheme (Π) is not perfectly secure.

Fix $c \in \mathcal{C}$.

$$\mathcal{M}_c = \{ m \mid \exists k, \; Dec(k,c) = m \}.$$

$\Rightarrow |\mathcal{M}_c| \leq |\mathcal{K}| < |\mathcal{M}|$ $\Rightarrow$ $\exists\, m \in \mathcal{M}$ and $m \notin \mathcal{M}_c$.

$$\Pr[M = m \mid C = c] = 0$$

$$\neq \Pr[M = m]$$

Th^m For any Perfectly Secure encryption scheme,

$$|\mathcal{K}| \geq |\mathcal{M}|.$$

Assume that $|\mathcal{K}| < |\mathcal{M}|$. Then we have to show that the scheme (Π) is not perfectly secure.

Fix $c \in \mathcal{C}$.

$$\mathcal{M}_c = \{ m \mid \exists k, \; Dec(k, c) = m \}.$$

$\Rightarrow |\mathcal{M}_c| \leq |\mathcal{K}| < |\mathcal{M}|$ $\Rightarrow$ $\exists\, m \in \mathcal{M}$ and $m \notin \mathcal{M}_c$.

$$Pr[M = m \mid C = c] = 0$$

$$\neq Pr[M = m]$$

Shannon's Theorem

$\Pi = (Gen, Enc, Dec)$, $|\mathcal{K}| = |\mathcal{M}| = |\mathcal{C}|$

Π is perfectly secure <u>if and only if</u>

(i) Gen function chooses each key <u>uniformly at random</u>.

(ii) $\forall\, m \in \mathcal{M},\ c \in \mathcal{C},\ \exists$ <u>unique key</u> $k \in \mathcal{K}$ such that

$$Enc_k(m) = c$$