Perfectly Secret Encryption

(Katz & Lindell)

Last Class

- Classical Ciphers
- Cryptanalysis with Ciphertext-only model

Weak

Strong

Security Goal

- Key Recovery
- Message Recovery
- Partial Message Recovery
- Meaningfull information Recovery
- Ciphertext should not reveal anything about plaintext. (*)

Some Basic Notations

{ Distribution of M & K are independent

Encryption Scheme

$\mathcal{M}, \mathcal{K}$

$\Pi = (Gen, Enc, Dec)$

{ chosen uniformly at random

$k \leftarrow Gen$ $\quad (k \xleftarrow{\$} \mathcal{K})$

$c \leftarrow Enc_k(m)$, where $m \in \mathcal{M}$ // may be probabilistic

$m := Dec_k(c)$ // deterministic

$Pr[K = k]$

R.V.

Distribution of $\mathcal{M}$ & $\mathcal{K}$ are given.

// use Enc

Distribution of C.

Exercise

Shift Cipher $(k \xleftarrow{\$} \mathcal{K})$

Suppose $\mathcal{M} = \{a, z\}$ $\quad \Pr[M = a] = 0.7$

$\mathcal{K} = \{0, 1, \ldots, 25\}$ $\quad \Pr[M = z] = 0.3$

Suppose I obtain a ciphertext B. What is the probability that the corresponding plaintext is a?

$$\Pr[M = a \mid C = B] = \frac{\Pr[C = B \mid M = a] \cdot \Pr[M = a]}{\Pr[C = B]}$$

$$\Pr[C = B] = \Pr[M = a \wedge K = 1] + \Pr[M = z \wedge K = 2]$$

$$= \frac{1}{26} \cdot 0.7 + \frac{0.3}{26}$$

$$= \frac{1}{26}$$

$$= \frac{\Pr[K = 1] \cdot \Pr[M = a]}{\Pr[C = B]} = 0.7$$

Perfect Secrecy (Def 1)

Given an encryption scheme $\Pi = (Gen, Enc, Dec)$ with message space $\mathcal{M}$, key space $\mathcal{K}$, we call it perfectly secure if for all $m \in \mathcal{M}$, $c \in C$ (for any distributions on M)

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

[Ciphertext provides no additional information about the plaintext]

Alternate Representation (Def 2)

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

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

$$\Pr_k[Enc_k(m_0) = c] = \Pr_k[Enc_k(m_1) = c]$$

Equivalence of Two Definitions

Def 1 ⇒ Def 2
Home Work

Def 2 ⇒ Def 1

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

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

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

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

$$= \Delta_c$$

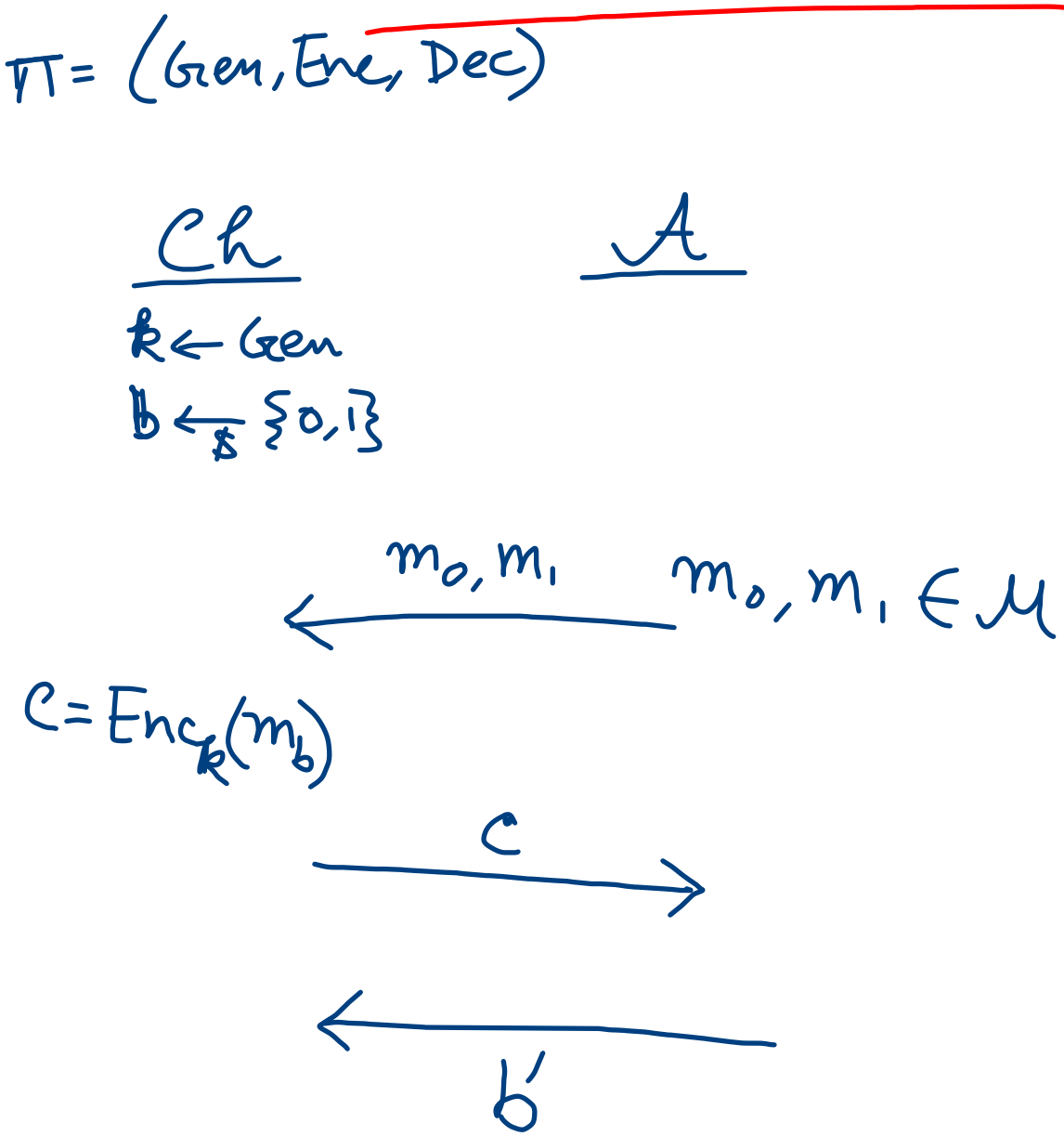
$$= \frac{\Delta_c \cdot \Pr[M=m]}{\sum_{m' \in \mathcal{M}} \Pr[C=c \mid M=m'] \cdot \Pr[M=m']}$$

$$= \frac{\Delta_c \cdot \Pr[M=m]}{\Delta_c \cdot \sum_{m' \in \mathcal{M}} \Pr[M=m']}$$

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

Perfect Indistinguishability

$\Pi = (Gen, Enc, Dec)$



Suppose this experiment outputs 1, i.e.

$$PI_{\pi,A}\ PrivK^{eav}_{\pi,A} = 1$$

if $b = b'$.

We call π to be perfectly indistinguishable if

$$Pr[PrivK^{eav}_{A,\pi} = 1] = \frac{1}{2}$$

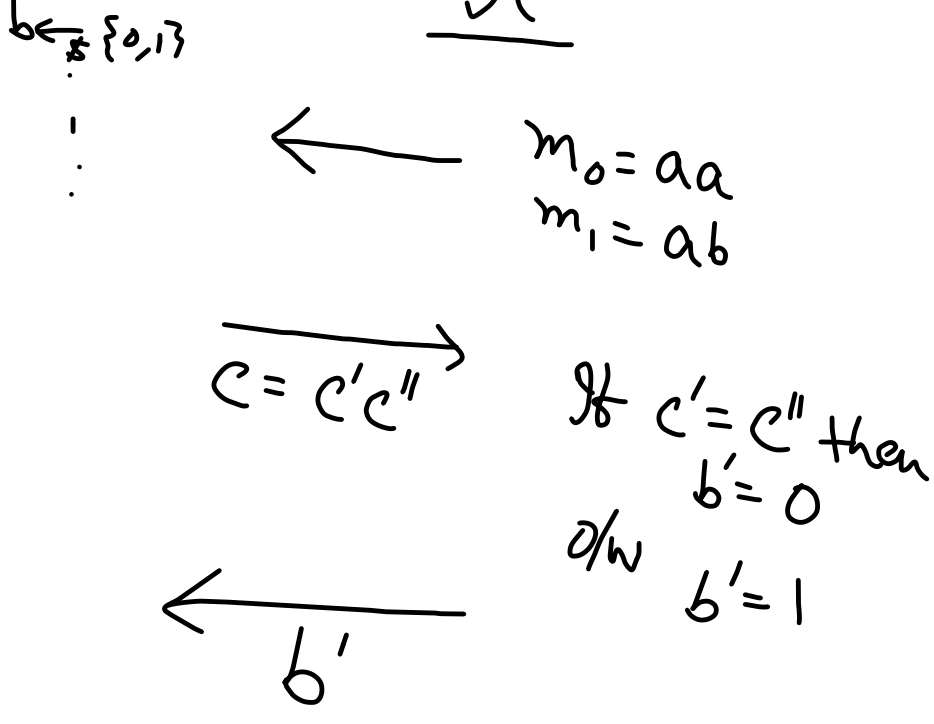
Thm. Π is perfectly secure if and only if Π is perfectly indistinguishable.

Show Vigenere Cipher is not Perfectly Indistinguishable.

a	a
k_1	k_2
c^*	c^{**}

Assumptions:

- Each message is two character long.
- $m = 1/2$ w.p $\frac{1}{2}$.



$$\Pr\left[\text{PrivK}^{eav}_{\pi,A} = 1\right]$$

$$= \frac{1}{2}\Pr\left[\text{PrivK}^{eav}_{\pi,A} = 1 \mid b=0\right] + \frac{1}{2}\Pr\left[\text{Priv}^{eav}_{\pi,A} = 1 \mid b=1\right]$$

$$= \frac{1}{2}\left(\left(\underbrace{\frac{1}{2}\cdot 1}_{m=1} + \underbrace{\frac{1}{2}\cdot\frac{1}{26}}_{m=2}\right) + \frac{1}{2}\left(1 - \frac{1}{2}\cdot\frac{1}{26}\right)\right) = \frac{3}{4}$$

When both the keys are same

Check

One-Time Pad (OTP)

$\mathcal{M} \leftarrow \{0,1\}^n$

$\mathcal{K} \leftarrow \{0,1\}^n$

$m = m_1 \ldots m_n$

$k = k_1 \ldots k_n$

$c = m_1 \oplus k_1 \ldots m_n \oplus k_n$

$k_1 \ldots k_n \xleftarrow{\$} Gen$

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

a	b	a⊕b
0	0	0
0	1	1
1	0	1
1	1	0

Lemma. OTP achieves perfect secrecy.

$$\Pr[M = m \mid C = c]$$
$$= \Pr[K = m \oplus c]$$
$$= \frac{1}{2^n}$$

Limitations of Perfect Secrecy

Th^m For any perfectly secret encryption scheme, $|\mathcal{K}| \geq |\mathcal{M}|$

Proof Let us assume $|\mathcal{K}| < |\mathcal{M}|$.

- Take a message m & encrypt it with any k. Let $c = Enc_k(m)$ (c is a valid ciphertext)
- $\mathcal{M}(c) := \{ m' \mid Dec_k(c) = m' \}$
- $|\mathcal{M}(c)| \leq |\mathcal{K}| < |\mathcal{M}|$
- $\exists m_0$ s.t. $m_0 \in \mathcal{M}$, $m_0 \notin \mathcal{M}(c)$

$$Pr[M = m_0 \mid C = c] = 0 \neq Pr[M = m_0]$$

Shannon's Theorem

$|\mathcal{M}| = |\mathcal{C}| = |\mathcal{K}|$. — (Assumption)

Π is perfectly secure if and only if

(i) $Pr[K = k] = \frac{1}{|\mathcal{K}|}$.

(ii) $\forall m \in \mathcal{M}, c \in \mathcal{C}$, $\exists$ unique $k \in \mathcal{K}$ s.t. $Enc_k(m) = c$

$m, c \rightarrow k$

$Enc_k(m) = c$