Perfectly Secure Encryption

Recap

- Classical Cipher
- Modern Crypto
  - Security definition
  - Assumptions
  - Security Proof

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

$\mathcal{M}$ → message space, $\mathcal{K}$ → key space
$\mathcal{C}$ → ciphertext space. distribution of $\mathcal{K}$ & $\mathcal{M}$ are independent

- $k \leftarrow Gen \;\|\; k \in \mathcal{K}$
- $c \leftarrow Enc(m, k)$
- $m := Dec(c, k)$

Correctness $\forall m \in \mathcal{M}, k \in \mathcal{K}$,
$Dec(Enc(m,k),k) = m$

Gen, Enc → Probabilistic
Dec → Deterministic

1. Consider Shift cipher.

Suppose, $Pr[K = k] = \frac{1}{26}$, for all $k \in \mathcal{K}$

Distribution of M, K ↓ Independent

Consider the following distribution:

$$Pr[M = a] = 0.7, \quad Pr[M = z] = 0.3.$$

(i) What is the probability that the ciphertext is B?

$Pr[C = B]$

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

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

1. Consider Shift cipher.

Suppose, $Pr[K = k] = \frac{1}{26}$, for all $k \in \mathcal{K}$

Distribution of M, K ↓ Independent

Consider the following distribution:

$$Pr[M = a] = 0.7, \quad Pr[M = z] = 0.3.$$

(i) What is the probability that the ciphertext is B?

$Pr[C = B]$

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

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

(ii) Assume $C = B$. What is the probability that the underlying message is "a"?

$$\Pr[M = a \mid C = B]$$

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

(Using Bayes' rule)

$$= \frac{\frac{1}{26} \times 0.7}{\frac{1}{26}} = 0.7$$

$$\Pr[C = B \mid M = a]$$
$$= \Pr[M + K = B \mid M = a]$$
$$= \Pr[a + K = B \mid M = a]$$
$$= \Pr[K = 1] = \frac{1}{26}$$

Perfect Secrecy

$\Pi = (Gen, Enc, Dec)$ is called perfectly secure Encryption if for all $m \in \mathcal{M}$ (any distribution) and $c \in \mathcal{C}$,

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

$(Pr[C = c] \neq 0)$

Shift Cipher with length 2

$$Pr[M = aa] = 0.1, \quad Pr[M = bc] = 0.9$$

- $Pr[M = aa \mid C = BB] = ?$

$$Pr[M = aa \mid C = BB] = \frac{Pr[C = BB \mid M = aa] \cdot Pr[M = aa]}{Pr[C = BB]}$$

$$= \frac{Pr[k = 1] \cdot 0.1}{\frac{0.1}{26}} = 1$$

Index of coincidence

$$I_C = \sum_{i=1}^{26} p_i^2$$

$p_1 \to q_1$

$p_2 \to q_2$

$\vdots$

$p_n \to q_n$

$p_1 q_1 + \cdots + p_n q_n = I_C$

$p_1, \ldots, p_n$

① $p_1 = \cdots = p_n = \frac{1}{n}$

$$I_C = n\left(\frac{1}{n}\right)^2 = \frac{1}{n}$$

② $p_1 = 1, \; p_2 = \cdots = p_n = 0$

$I_C = 1$

Index of coincidence

$$I_C = \sum_{i=1}^{26} p_i^2$$

$p_1 \to q_1$

$p_2 \to q_2$

$\vdots$

$p_n \to q_n$

$p_1 q_1 + \cdots + p_n q_n = I_C$

$p_1, \ldots, p_n$

① $p_1 = \cdots = p_n = \frac{1}{n}$

$$I_C = n\left(\frac{1}{n}\right)^2 = \frac{1}{n}$$

② $p_1 = 1, \; p_2 = \cdots = p_n = 0$

$I_C = 1$

Shift Cipher

Plaintext/msg: c r y p t o

key → + 1 1 1 1 1 1

d s z q u p

- Substitution Cipher
- Vigenere Cipher

Kerchoff's Principle

- Only Key is the secret.

1970 - 78

↓

Classical Crypto → Modern Crypto

Shift Cipher

Plaintext/msg: c r y p t o

key → + 1 1 1 1 1 1

d s z q u p

- Substitution Cipher
- Vigenere Cipher

Kerchoff's Principle

- Only Key is the secret.

1970 - 78

↓

Classical Crypto → Modern Crypto

Security goal

- Break the key $E_k(m) = m$
- Recover the complete plaintext
- (No information should be leaked from the ciphertext)

Security goal

- Break the key $E_k(m) = m$
- Recover the complete plaintext
- (No information should be leaked from the ciphertext)

8 people

- uniformly at random choose 1.

$P(H) = P(T) = \frac{1}{2}$

HHH → Person 1
⋮
TTH → Person 7
TTT → Repeat the experiment

HHH → Person 1
⋮
TTT → Person 8

Probability that the experiment terminates

$= \frac{7}{8} + \frac{1}{8}\times\frac{7}{8} + \left(\frac{1}{8}\right)^2 \times \frac{7}{8} + \cdots$

$= \frac{7}{8}\left(1 + \frac{1}{8} + \left(\frac{1}{8}\right)^2 + \cdots\right) = \frac{7}{8}\cdot\frac{8}{7} = 1$

$Pr[H] = p, \quad Pr[T] = (1-p)$

Choose one out of 2

2 toss

- $\to HH \to p^2 \to$ Repeat
- $\to HT \to p(1-p) \to$ choose P1
- $\to TH \to (1-p)p \to$ choose P2
- $\to TT \to (1-p)^2 \to$ Repeat

$2p.(1-p) = \alpha$

$Pr[$This experiment terminates$] = ?$