No ~~efficiently~~ non-trivial computable function of the message should be revealed by looking at the ciphertext.

**Plaintext:** $\{01, 00\}$

$$\mathrm{Enc}(k, \cdot) = c$$

Looking at the ciphertext, $\mathcal{A}$ can predict the following:

"the first bit of the plaintext is 0".

**Textbook:**

Introduction to Modern Cryptography:

Katz & Lindell

CRC Press.

---

**10 Jan 25**

**Recap:** What is a (secure) secret encryption?

$\mathcal{P}$ = set of plaintexts $= \{m_1, m_2, \ldots\ldots m_\ell\}$

$\mathcal{C}$ = set of ciphertexts $= \{c_1, c_2, \ldots\ldots c_{\ell'}\}$

(obviously: $\ell' \geq \ell$)

$\mathcal{K}$ = set of keys $= \{k_1, k_2, \ldots k_t\}$

## Functions:

(i) Key Gen : every time the function is run, it produces a random secret key $k \in \mathcal{K}$

initial part of this course
$$\mathcal{K} = \{ x \in \{0,1\}^n \}$$

Binary strings of length n bits

Key Gen in this case = produce a $k \in \mathcal{K}$ with prob. $= 1/2^n$

in practice, $n \simeq 128$ bits, for higher level of security (paranoid / quantum comps) — 256 bits

IOT devices - 64 bits

(ii) Enc $(k \in \mathcal{K}, m \in \mathcal{P})$
$$\longrightarrow c \in \mathcal{C}$$

possibility:

$$\text{Enc}(k, m_1) \longrightarrow c$$
$$\text{Enc}(k, m_1) \longrightarrow c' \quad \Rightarrow \quad |\mathcal{C}| = 2 \cdot |\mathcal{P}|$$

Enc(·,·) can be deterministic or randomized

(iii) Dec $(k \in \mathcal{K}, c \in \mathcal{C})$
$$\longrightarrow m \in \mathcal{P}$$

deterministic

Valid Encryption : $\forall m \in \mathcal{P}, \forall k \in \mathcal{K}$

$$\text{Dec}(k, \text{Enc}(k, m)) = m$$

# Secure Encryption ?

## Trivial attack 1

Given a challenge ciphertext $c$, aim is to find $m$

- guess the key $k$
  then $Dec(k, c) \rightarrow$

Prob of success of the adv.
$= 1/|K|$

(Ex) $= 1/2^n$

attack cost $= 1$

## Trivial attack 2

Brute force the keys

effort $= 2^n$ decryption calls

Success prob $= 1$

$\rightarrow$ $n$ should be sufficiently large

Given a ciphertext $c$, an attacker should not get some non-trivial info about the plaintext

information

## Claude Shannon :

information $\propto \frac{1}{\text{prob.}}$

Event $\rightarrow$ $t$ outcomes
prob.
$p_1, p_2, \ldots p_t$ $\rightarrow$ information contained

$= -\sum p \cdot \log p$

Entropy $= \sum p \,(\log 1/p)$

Even against infinite computational power of the adv, no advantage to her.

$$\Pr(\text{plaintext} = m \mid \text{ciphertext} = c) = \Pr(\text{plaintext} = m)$$

$\forall m \in \mathcal{P}, \quad \forall c \in \mathcal{C}$

## Perfectly secure Encryption

## Adversarial setting:

Adv. Dove soap

$\boxed{\text{Adv Game}}$

**Challenger** | **Adversary**

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

$m_0, m_1 \in \mathcal{P}$

$m_0 \neq m_1$

& $|m_0| = |m_1|$

$\xleftarrow{m_0, m_1}$

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

$c = Enc(k, m_b)$

$\xrightarrow{c}$

Some computations
- at the end produce $b' \in \{0,1\}$ guess

Adv wins if $b' = b$

Pr of attacker wins $= 1/2 \implies$ Perfectly secure Encryption

## Is it possible to achieve this strong security notion?

## Vernam Cipher / OTP (one time pad)

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

Key Gen : $\longrightarrow$ uniformly randomly produce a key $k \in \{0,1\}^n$

$$\Pr(k = k^*) = 1/2^n$$

$$Enc(k, m) = k \oplus m$$

$$Dec(k, c) = k \oplus c$$

XOR

| | | XOR |
|---|---|---|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

note: $\alpha \oplus \alpha = 000\cdots0$ for all $\alpha$

To prove : for this encryption algo.

$\forall c, \forall m$ $\quad \Pr(\mathcal{P} = m \mid \mathcal{C} = c) = \Pr(\mathcal{P} = m)$

Notice:

$\mathcal{P}$

$m_1 \longrightarrow \Pr = p_1$

$m_2 \longrightarrow \Pr = p_2$

$\vdots$

$m_{2^n} \longrightarrow \Pr = p_{2^n}$

$\longrightarrow$ determines the RHS above

LHS: $\Pr(P=m \mid C=c)$

$$= \frac{\Pr(P=m \cap C=c)}{\Pr(C=c)}$$

$$= \frac{\Pr(P=m \cap m \oplus k = c)}{\sum_{m} \Pr(P=m) \times \Pr(C=c \mid P=m)}$$

$$= \frac{\Pr(P=m \cap k = c \oplus m)}{\sum (\ldots) \times \Pr(k=(m \oplus c))} \quad \Pr(k=(m \oplus c)) \rightarrow 1/2^n$$

$$= \frac{\Pr(P=m) \times 1/2^n}{1 \times 1/2^n}$$

$$= \Pr(P=m)$$

Used in Hotline between US & USSR during cold-war.

USSR army / spies — they used OTP

## One-Time Pad ?

if the same key is used twice

Two time pad $\longrightarrow$

$$c_1 = m_1 \oplus k \Rightarrow c_1 \oplus c_2$$
$$c_2 = m_2 \oplus k \quad = m_1 \oplus m_2$$

# Project Venona — wikipedia

14 Jan 2025

## Information theoretic security

**Shannon Security**

$\forall m, c$ : $Pr(\mathcal{P} = m \mid C = c) = Pr(\mathcal{P} = m)$

Equivalent

**Perfect Indistinguishability**

- $m_1, m_2$ picked by Adv.
- one of them randomly encrypted by the challenger
- Adv's advantage in distinguishing which of the two messages produced $c$ $= 0$

$\forall m_1, m_2, \forall c$

$Pr(\mathcal{P} = m_1 \mid C = c) = Pr(\mathcal{P} = m_2 \mid C = c)$

① Shannon security $\Rightarrow$ Perfect indistinguishability

$Pr(\mathcal{P} = m_1 \mid C = c) = Pr(\mathcal{P} = m_1)$ for any $m_1, c$

defn of conditional prob

$$\frac{Pr(\mathcal{P} = m_1 \cap Enc(k, m_1) = c)}{Pr(C = c)} = Pr(\mathcal{P} = m_1)$$

$$\frac{\cancel{Pr(\mathcal{P} = m_1)} \cdot Pr(Enc(k, m_1) = c)}{Pr(C = c)} = \cancel{Pr(\mathcal{P} = m_1)}$$

$$\underset{k, c}{Pr}(Enc(k, m_1) = c) = \underset{c}{Pr}(C = c)$$

$$= Pr(Enc(k, m_2) = c) \quad //$$