

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

Plaintext: $\{01, 00\}$

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

Looking at the ciphertext, 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 ^(secret) secret encryption?

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

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

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

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

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

$$\mathcal{K} = \{w \in \{0,1\}^n\}$$

Binary strings of
length n bits

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

in practice. $n \geq 128$ bits, for higher level of security
(paraivoid/quantum comp)
— 256 bits

IoT devices - 64 bits

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

possibility:

$$\begin{aligned} \text{Enc}(k, m_1) &\longrightarrow c \\ \text{Enc}(k, m_1) &\longrightarrow c' \end{aligned} = |\mathcal{C}| = 2 \cdot |\mathcal{P}|$$

$\text{Enc}(\cdot)$ can be deterministic or randomized

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

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 $\text{Dec}(k, c) \rightarrow$

Prob of success of the adv.
 $= \frac{1}{|K|}$

$$(Ex) = \frac{1}{2^n}$$

attack cost = 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
 \downarrow prob.

p_1, p_2, \dots, p_t

\rightarrow information contained

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

$$= \sum p (\log \frac{1}{p})$$

Entropy

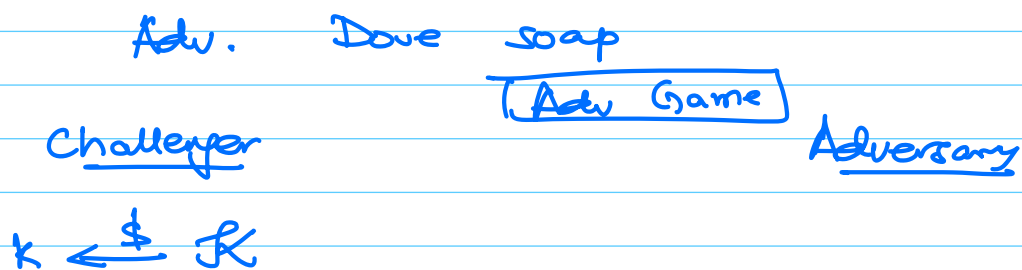
Even against
infinite computational power
of the adv,
no advantage to
her.

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

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

Perfectly Secure Encryption

Adversarial setting:



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

$$m_0 \neq m_1$$

$$\xleftarrow{m_0, m_1 \text{ \& } |m_0| = |m_1|}$$

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

$$c = \text{Enc}(k, m_b)$$

$$\xrightarrow{c}$$

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

Adv wins if $b' = b$

\Pr of attacker winning $= 1/2 \Rightarrow$ 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 : \rightarrow ^{uniformly} ^{randomly} produce a key
 $k \in \{0, 1\}^n$

$$\Pr(k = k^*) = \frac{1}{2^n}$$

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

$$\text{Dec}(k, c) = k \oplus c$$

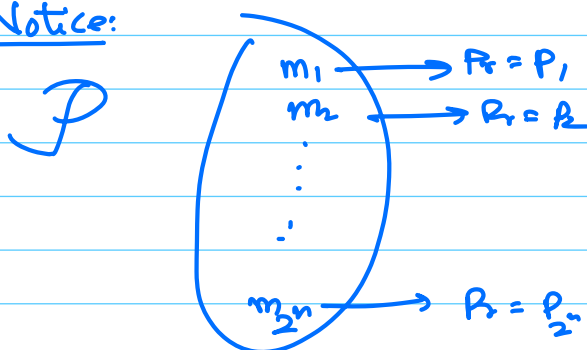
XOR		
0	0	0
0	1	1
1	0	1
1	1	0

note: $\alpha \oplus \alpha = 000\dots 0$ for all α

To prove: for this encryption algo.

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

Notice:



\rightarrow determines the RHS above

$$\text{LHS: } \Pr(P=m | C=c)$$

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

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

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

$$\leq (\dots) \times \Pr(K=(m \oplus c)) \rightarrow \frac{1}{2^n}$$

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

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

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 →

$$\begin{aligned} C_1 &= m_1 \oplus K \\ C_2 &= m_2 \oplus K \Rightarrow C_1 \oplus C_2 = m_1 \oplus m_2 \end{aligned}$$

Project Venona — wikipedia

14 Jan 2025

Information theoretic security

Shannon Security

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

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 $c = 0$

$$\forall m_1, m_2, \forall c$$

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

① Shannon Security \Rightarrow Perfect indistinguishability

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

(defn of conditional prob)

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

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

$$\Pr_{k, c}(\text{Enc}(k, m_1) = c) = \Pr_c(\mathcal{C} = c)$$

$$= \Pr(\text{Enc}(k, m_2) = c)$$