HA NOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Introduction to Cryptography and Security

Perfect Security

Slides are taken from

- https://cseweb.ucsd.edu/~mihir/cse107/slides.html

Outline

1. Definition
2. One-Time Pad Security

A measure of security

Let $(\mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme. For any message m and ciphertext c we are interested in

$$\Pr[\mathsf{Enc}(k, m) = c]$$

where the probability is over the random choice $k \leftarrow \mathcal{K}$ and over the coins tossed by Enc if any.

Example

Consider the symmetric encryption scheme as follows.

messages:

keys:		00	01	10	11
	00	01	10	11	00
	01	01	11	10	00
	10	00	11	01	11
	11	11	10	01	11

The table entry in row k and column m is $\mathsf{Enc}(k, m)$,

- $\Pr[\mathsf{Enc}(k, 00) = 01] = 2/4 = 1/2$
- $\Pr[\mathsf{Enc}(k, 01) = 01] = 0$
- $\Pr[\mathsf{Enc}(k, 10) = 11] = 1/4$

Perfect Security

Definition

Let $\Pi = (\mathsf{Enc}, \mathsf{Dec})$ be a symmetric encryption scheme. We say that Π is perfectly secure if for any two messages m_1, m_2 and any ciphertext c

$$\Pr[\mathsf{Enc}(k, m_1) = c] \quad = \quad \Pr[\mathsf{Enc}(k, m_2) = c].$$

In both cases, the probability is over the random choice $k \leftarrow \mathcal{K}$ and over the coins tossed by Enc if any.

Intuitively: Given c, and even knowing the message is either m_1 or m_2 the adversary cannot determine which.

Definition requires that

For all $m_1,\ m_2,\ c$ we have

$$\Pr[\mathsf{Enc}(k, m_1) = c] \quad = \quad \Pr[\mathsf{Enc}(k, m_2) = c].$$

If we want to show the definition is not met, we need to show that

There exists m_1, m_2, c such that

$$\Pr[\mathsf{Enc}(k, m_1) = c] \quad \neq \quad \Pr[\mathsf{Enc}(k, m_2) = c].$$

Example

		messages:			
		00	01	10	11
	00	01	10	11	00
keys:	01	01	11	10	00
	10	00	11	01	11
	11	11	10	01	11

The table entry in row k and column m is $\mathsf{Enc}(k, m)$.

- $\Pr[\mathsf{Enc}(k, 00) = 01] = 2/4 = 1/2$
- $\Pr[\mathsf{Enc}(k, 01) = 01] = 0$

Question: Is this encryption scheme perfectly secure? No, because for $m_1 = 00, m_2 = 01$ and $c = 01$ we have

$$\Pr[\mathsf{Enc}(k, m_1) = c] \quad \neq \quad \Pr[\mathsf{Enc}(k, m_2) = c].$$

Perfect security of substitution ciphers

Claim

A substitution cipher is NOT perfectly secure.

Example

$$\begin{aligned} \texttt{A} &\rightarrow \texttt{k} \\ \texttt{B} &\rightarrow \texttt{d} \\ \texttt{C} &\rightarrow \texttt{w} \\ &\cdots \end{aligned}$$

Perfect security of substitution ciphers

Claim

Let $\Pi = (Enc, Dec)$ be a substitution cipher over the alphabet Σ consisting of the 26 English letters. Assume that k picks a random permutation over Σ as the key. That is, its code is

$$k \leftarrow \textsc{Perm}(\Sigma); \quad \text{return } k.$$

Let Plaintexts be the set of all three letter English words. Then Π is not perfectly secure.

Proof of claim

To show: there exist m_1, m_2, c such that

$$\Pr[\mathsf{Enc}(k, m_1) = c] \quad \neq \quad \Pr[\mathsf{Enc}(k, m_2) = c].$$

Let

- $c = \mathtt{xyy}$
- $m_1 = \mathtt{FEE}$
- $m_2 = \mathtt{FAR}$

Then

$$\begin{aligned} \Pr[\mathsf{Enc}(k, m_2) = c] &= \Pr[\mathsf{Enc}(k, \mathtt{FAR}) = \mathtt{xyy}] \\ &= 0 \end{aligned}$$

Why?

Proof of claim

$$
\begin{aligned}
\Pr[\mathsf{Enc}(k, m_1) = c] &= \Pr[\mathsf{Enc}(k, \mathtt{FEE}) = \mathtt{xyy}] \\
&= \frac{|\{k \in \textsc{Perm}(\Sigma) \ : \ k(\mathtt{F})k(\mathtt{E})k(\mathtt{E}) = \mathtt{xyy}\}|}{|\textsc{Perm}(\Sigma)|} \\
&= \frac{24!}{26!} \\
&= \frac{1}{650}.
\end{aligned}
$$

Outline

1. Definition
2. One-Time Pad Security

One Time Pad

- Gen: Generates a random bit sequence of length λ.
- Enc: Represent the message as a binary string and XOR with the key.

$$\begin{array}{rrl} & x & = 101100.. \\ \oplus & k & = 011010.. \\ \hline & y & = 110110.. \end{array}$$

- Dec: Same as encryption, just XOR with k.

$$\begin{aligned}(x_i \oplus k_i) \oplus k_i &= x_i \oplus (k_i \oplus k_i) \\ &= x_i \oplus 0 = x_i\end{aligned}$$

Intuition for OTP security

Suppose adversary gets ciphertext $c = 101$ and knows the plaintext m is either $m_1 = 010$ or $m_2 = 001$. Can it tell which?

No, because $c = k \oplus m$ so

- $m = 010$ iff $k = 111$
- $m = 001$ iff $k = 100$

but k is equally likely to be 111 or 100 and adversary does not know k.

Perfect security of OTP

Claim

Let $\Pi = (Enc, Dec)$ *be the OTP scheme with key-length* $\lambda \geq 1$*.*
Then Π *is perfectly secure.*

Proof Idea.

Want to show that for any m_1, m_2, c

$$\Pr[\mathsf{Enc}(k, m_1) = c] \quad = \quad \Pr[\mathsf{Enc}(k, m_2) = c].$$

That is

$$\Pr[k \oplus m_1 = c] \quad = \quad \Pr[k \oplus m_2 = c]$$

when $k \leftarrow \{0,1\}^\lambda$. $\square$

Example: $\lambda = 2$

messages:

keys:		00	01	10	11
	00	00	01	10	11
	01	01	00	11	10
	10	10	11	00	01
	11	11	10	01	00

The table entry in row k and column m is $\mathsf{Enc}(k, m) = k \oplus m$.

- $\Pr[\mathsf{Enc}(k, 00) = 01] = 1/4$
- $\Pr[\mathsf{Enc}(k, 10) = 01] = 1/4$

Proof of Claim

$$\begin{aligned}\Pr[\mathsf{Enc}(k, m) = c] &= \Pr[k \oplus m = c] \\ &= \frac{\left|\{k \in \{0,1\}^\lambda : k \oplus m = c\}\right|}{|\{0,1\}^\lambda|} \\ &= 1/2^\lambda.\end{aligned}$$

Perfect security: Plusses and Minuses

$+$

- Very good privacy

$-$

- Key needs to be as long as message

Project 1: Many-time pad attack

https://www.coursera.org/learn/crypto/

- Let us see what goes wrong when an OTP key is used more than once.
- Given eleven hex-encoded ciphertexts that are the result of encrypting eleven plaintexts with an OTP scheme, all with the same OTP key.
- Your goal is to decrypt the last ciphertext, and submit the secret message within it as solution.

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Thank you!

soict.hust.edu.vn/ fb.com/groups/soict