Introduction

Chanathip Namprempre

Computer Science
Reed College

Agenda: Symmetric Encryption

- Caesar cipher: what is it
- One-time Pad (OTP): what is it
- Symmetric encryption schemes: what is it (syntax and correctness condition)
    - Examples
    - Non-examples
- Perfect secrecy
    - OTP provides perfect secrecy

Caesar cipher

$$\texttt{cat} \Rightarrow \texttt{fdw}$$

We can analyze the frequency of letters (and digrams and trigrams) to break substitution ciphers.

One-Time Pad (OTP)

Suppose $K = 00101000$.

$$\begin{aligned} \mathtt{00011101} &\Rightarrow \mathtt{00011101} \oplus \mathtt{K} \\ &\Rightarrow \mathtt{00011101} \oplus \mathtt{00101000} \\ &\Rightarrow \mathtt{00110101} \end{aligned}$$

One-time Pad (OTP)

A stateful, deterministic encryption scheme

idea

- To **encrypt** M with a key K, just do $M \oplus K$

  [but we also need to know which key bits in the key stream we have used so far.]

- To **decrypt** C with a key K, just do $C \oplus K$

  [using the right bits in the key stream.]

More formally

Symmetric Encryption

For simplicity, we assume here that plaintexts, ciphertexts, and keys are bitstrings.

Syntax

A symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a triple of algorithms.

alg	input	output	notation	maybe randomized?	maybe stateful?
$\mathcal{K}$	-	key K	$K \xleftarrow{\$} \mathcal{K}$	yes	no
$\mathcal{E}$	$K \in Keys(\mathcal{SE})$ $M \in \{0,1\}^*$	ciphertext $C \in \{0,1\}^* \cup \{\perp\}$	$C \xleftarrow{\$} \mathcal{E}_K(M)$	yes	yes
$\mathcal{D}$	$K \in Keys(\mathcal{SE})$ $C \in \{0,1\}^*$	plaintext $M \in \{0,1\}^* \cup \{\perp\}$	$M \leftarrow \mathcal{D}_K(C)$	no	no

Correctness

For all $K \in Keys(\mathcal{SE})$ and all $M \in \{0,1\}^*$,

$$\Pr\left[C = \perp \text{ OR } \mathcal{D}_K(C) = M \;:\; C \xleftarrow{\$} \mathcal{E}_K(M) \right] = 1 .$$

Symmetric Encryption

For simplicity, we assume here that plaintexts, ciphertexts, and keys are bitstrings.

Syntax

A symmetric encryption scheme $\mathcal{SE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is a triple of algorithms.

alg	input	output	notation	maybe randomized?	maybe stateful?
$\mathcal{K}$	-	key K	$K \xleftarrow{\$} \mathcal{K}$	yes	no
$\mathcal{E}$	$K \in Keys(\mathcal{SE})$ $M \in \{0,1\}^*$	ciphertext $C \in \{0,1\}^* \cup \{\bot\}$	$C \xleftarrow{\$} \mathcal{E}_K(M)$	yes	yes
$\mathcal{D}$	$K \in Keys(\mathcal{SE})$ $C \in \{0,1\}^*$	plaintext $M \in \{0,1\}^* \cup \{\bot\}$	$M \leftarrow \mathcal{D}_K(C)$	no	no

Correctness

For all $K \in Keys(\mathcal{SE})$ and all $M \in \{0,1\}^*$,

$$\Pr\left[\, C = \bot \text{ OR } \mathcal{D}_K(C) = M \;:\; C \xleftarrow{\$} \mathcal{E}_K(M) \,\right] = 1\,.$$

Symmetric Encryption

- Secret key K is somehow shared a priori.
- Sender and receiver do not share states.
- The term "randomized/stateful" symmetric encryption refers to the property of the encryption algorithm only.
- "plaintext space" $=$ set of messages that $\mathcal{E}$ will encrypt [i.e. $\mathcal{E}$ won't return $\perp$]
- $\mathcal{E}$ returns $\perp$ when
  - $M \notin$ plaintext space or
  - say, a counter reaches the maximum value

We'll look at some encryption schemes. All are correct but may or may not be secure.

One-time Pad: definition

Let $n \in \mathbf{N}$ be the parameter of the scheme. Hereafter, we assume that the key stream is of length exactly n bits.

$\mathcal{K}$: $K \xleftarrow{\$} \{0,1\}^n$;return K

$\mathcal{E}_K(M)$:	$\mathcal{D}_K(C)$:
If $\lvert M\rvert \neq n$ then return $\perp$	If $\lvert C\rvert \neq n$ then return $\perp$
$C \leftarrow M \oplus K$	$M \leftarrow C \oplus K$
return C	return M

Try encrypting $M = 101$ with $K = 010$ and decrypting the resulting ciphertext.

One-time Pad: limitation

Key bits cannot be reused if one wants to maintain security!

Non-Examples

Non-example 1

Let (E, D) be the following functions:

$$\forall x \in \mathbf{N}, E(x) = x^2$$
$$\forall y \in \mathbf{N}, D(y) = y^{\frac{1}{2}} \ .$$

There are many problems with this!

Non-Examples (cont.)

Non-example 2

Let $n \in \mathbf{N}$ be the parameter of the scheme.

$\mathcal{K} : K \xleftarrow{\$} \{0,1\}^n$;return K

$\mathcal{E}_K(M)$:	$\mathcal{D}_K(C)$:
If $M = 0^n$ then return 1^n	If $C = 1^n$ then return 0^n
If $\lvert M\rvert \neq n$ then return $\perp$	If $\lvert C\rvert \neq n$ then return $\perp$
$C \leftarrow M \oplus K$	$M \leftarrow C \oplus K$
return C	return M

Try decrypting 1^n.

Perfect Secrecy

Definition

Let	n	$\in \mathbf{Z}^+$.
Let	K	be a shared secret chosen at random from $\{0,1\}^n$ (for simplicity).
Let	M	be a random variable denoting a plaintext chosen according to some public distribution.
Let	C	be a random variable denoting a ciphertext obtained from M and K.

A symmetric encryption scheme provides **perfect secrecy** iff, for any $a, b \in \{0,1\}^n$,

$$\Pr[\, M = a \mid C = b \,] = \Pr[\, M = a \,] \ .$$

Theorem

OTP provides perfect secrecy.

Proof: OTP provides perfect secrecy

$$
\begin{aligned}
\Pr[\, M = a \mid C = b \,] &= \frac{\Pr[\, M = a \wedge C = b \,]}{\Pr[\, C = b \,]} \\
&= \frac{\Pr[\, M = a \wedge C = b \,]}{\sum_{x \in \{0,1\}^n} \Pr[\, M = x \wedge C = b \,]} \\
&= \frac{\Pr[\, M = a \wedge K = (a \oplus b) \,]}{\sum_{x \in \{0,1\}^n} \Pr[\, M = x \wedge C = b \,]} \\
&= \frac{\Pr[\, M = a \,] \cdot \Pr[\, K = (a \oplus b) \,]}{\sum_{x \in \{0,1\}^n} \Pr[\, M = x \wedge C = b \,]} \\
&= \frac{\Pr[\, M = a \,] \cdot 2^{-n}}{\sum_{x \in \{0,1\}^n} \Pr[\, M = x \wedge C = b \,]}
\end{aligned}
$$

Proof: OTP provides perfect secrecy (cont.)

$$
\begin{aligned}
\Pr[\, M = a \mid C = b \,] &= \frac{\Pr[\, M = a \,] \cdot 2^{-n}}{\sum_{x \in \{0,1\}^n} \Pr[\, M = x \wedge C = b \,]} \\
&= \frac{\Pr[\, M = a \,] \cdot 2^{-n}}{\sum_{x \in \{0,1\}^n} \Pr[\, M = x \,] \cdot 2^{-n}} \\
&= \frac{\Pr[\, M = a \,] \cdot 2^{-n}}{2^{-n} \cdot \sum_{x \in \{0,1\}^n} \Pr[\, M = x \,]} \\
&= \frac{\Pr[\, M = a \,] \cdot 2^{-n}}{2^{-n} \cdot 1} \\
&= \Pr[\, M = a \,] \; .
\end{aligned}
$$

That's nice. But what does it actually say again?

Definition

... A symmetric encryption scheme provides **perfect secrecy** iff, for any $a, b \in \{0,1\}^n$,

$$\Pr\left[\, M = a \mid C = b \,\right] = \Pr\left[\, M = a \,\right] .$$

Consider the following scheme.

Key generation:	Choose one at random from $\{0,1\}^{16}$
Encryption of M with key K:	Return M
Decryption of C with key K:	Return C

Suppose the message space is $\{0,1\}^{16}$, and the samples follow the uniform distribution. Does this scheme provide perfect secrecy?

- What is $\Pr\left[\, M = 0^{16} \mid C = 1^{16} \,\right]$?
- What is $\Pr\left[\, M = 0^{16} \,\right]$?
- What is $\Pr\left[\, M = 0^{16} \mid C = 0^{16} \,\right]$?

And just to make sure you understand the notation and the RVs

Consider the following scheme.

Key generation:	Choose one at random from $\{0,1\}^{64}$
Encryption of M with key K:	Return $M \oplus K$
Decryption of C with key K:	Return $C \oplus M$

Suppose we know that $\Pr\left[\, M = 0^{64} \,\right] = \Pr\left[\, M = 1^{64} \,\right] = 0.5$ and no other values of M are possible.

- What is $\Pr\left[\, M = 01^{63} \,\right]$?
- What is $\Pr\left[\, C = 0^{64} \,\right]$?
- What is $\Pr\left[\, C = 0^{60}1^{4} \,\right]$?