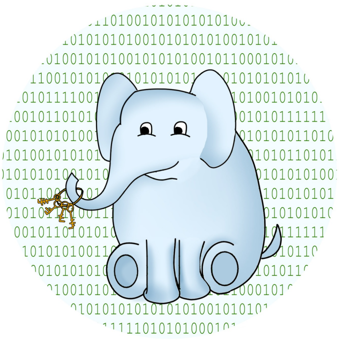
Symmetric Encryption
The myth of perfect security



Credits to our artist Ella

Presenters:
Longde Huang
Luc Steenbakkers

Group Members:
Catarina P. Loureiro
Diogo Pereira
Ella Salo
Magdalena Mikic
Isa Lamers
Isabella Salvaggio
Ivan Vukovic

Contents

Symmetric Encryption

Key space $\mathcal{K}$
Message space $\mathcal{M}$
Ciphertext space $\mathcal{C}$

Definition

A Symmetric Encryption (SE) algorithm is a tuple $(\texttt{KeyGen}, \texttt{Enc}, \texttt{Dec})$ with

$$
\begin{aligned}
\texttt{KeyGen} : (\cdot) &\to \mathcal{K} \\
\texttt{Enc} : \mathcal{K} \times \mathcal{M} &\to \mathcal{C} \\
\texttt{Dec} : \mathcal{K} \times \mathcal{C} &\to \mathcal{M}
\end{aligned}
$$

Both sender and receiver have the same key

Substitution Cipher

Example

$$\mathcal{K} = S_{26}$$
$$\mathcal{M} = \{A, B, \dots, Z\}^n$$
$$\mathcal{C} = \{A, B, \dots, Z\}^n$$

Substitution Cipher

Example

$$\mathcal{K} = S_{26}$$
$$\mathcal{M} = \{A, B, \ldots, Z\}^n$$
$$\mathcal{C} = \{A, B, \ldots, Z\}^n$$

If we take

$k =$ "shift by three to the right"

$m =$ **ELEPHANT**

Enc	with	k
A	→	D
B	→	E
C	→	F
⋮		⋮
W	→	Z
X	→	A
Y	→	B
Z	→	C

Substitution Cipher

Example

$$\mathcal{K} = S_{26}$$
$$\mathcal{M} = \{A, B, \ldots, Z\}^n$$
$$\mathcal{C} = \{A, B, \ldots, Z\}^n$$

If we take
$k =$ "shift by three to the right"
$m =$ **ELEPHANT**
$c =$ **HOHSKDQW**

We call this shifting a **Caesar Cipher**, which is a substitution cipher since $k \in S_{26}$

Enc with k		
A	$\rightarrow$	D
B	$\rightarrow$	E
C	$\rightarrow$	F
$\vdots$		$\vdots$
W	$\rightarrow$	Z
X	$\rightarrow$	A
Y	$\rightarrow$	B
Z	$\rightarrow$	C

Security Properties

Definition (Correctness)

Let $SE = (\texttt{KeyGen}, \texttt{Enc}, \texttt{Dec})$ be a symmetric encryption scheme with message space $\mathcal{M}$, ciphertext space $\mathcal{C}$ and key space $\mathcal{K}$. We say that SE is (perfectly) correct if

$$\forall m \in \mathcal{M}, \forall k \in \mathcal{K}, \quad \mathbb{P}[\texttt{Dec}_k(\texttt{Enc}_k(m)) = m] = 1.$$

Security Properties

Definition (Correctness)

Let $SE = (\texttt{KeyGen}, \texttt{Enc}, \texttt{Dec})$ be a symmetric encryption scheme with message space $\mathcal{M}$, ciphertext space $\mathcal{C}$ and key space $\mathcal{K}$. We say that SE is (perfectly) correct if

$$\forall m \in \mathcal{M}, \forall k \in \mathcal{K}, \quad \mathbb{P}[\texttt{Dec}_k(\texttt{Enc}_k(m)) = m] = 1.$$

Definition (Perfect Security)

The scheme SE $= (\texttt{KeyGen}, \texttt{Enc}, \texttt{Dec})$ is perfectly secure iff $\forall m_1,\ m_2 \in \mathcal{M}$, $\forall c \in \mathcal{C}$,

$$\mathbb{P}(\texttt{Enc}_k(m_1) = c) = \mathbb{P}(\texttt{Enc}_k(m_2) = c) \text{ taken over all } k \in \mathcal{K}$$

Security properties of the Substitution Cipher

Example (Correctness)

Take any $k \in \mathcal{K} = S_{26}$. Since permutations are always invertible, decryption is just applying k^{-1}. Therefore,

$$\forall m \in \mathcal{M}, \forall k \in \mathcal{K}, \quad \mathbb{P}[\mathtt{Dec}_k(\mathtt{Enc}_k(m)) = m] = 1$$

Security properties of the Substitution Cipher

Example (Correctness)

Take any $k \in \mathcal{K} = S_{26}$. Since permutations are always invertible, decryption is just applying k^{-1}. Therefore,

$$\forall m \in \mathcal{M}, \forall k \in \mathcal{K}, \quad \mathbb{P}[\texttt{Dec}_k(\texttt{Enc}_k(m)) = m] = 1$$

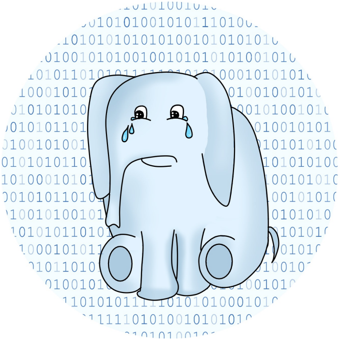
Example (Security)

Consider the messages $m_1 = FUN$ and $m_2 = LOL$. Now imagine that we see the ciphertext $c = \text{QRS}$. Then

$$\mathbb{P}(\texttt{Enc}(k, m_1) = c) > 0$$
$$\mathbb{P}(\texttt{Enc}(k, m_2) = c) = 0$$

Security properties of the Substitution Cipher

So this scheme is not perfectly secure!



Some Examples

Definition (XOR)

For $a, b \in \{0,1\}^N$, $(a \oplus b)_i = \begin{cases} 1, & a_i \neq b_i \\ 0, & a_i = b_i \end{cases}$.

Or equivalently, $a \oplus b = (a+b) \mod 2 = (a+b)_{\mathbb{Z}_2^N}$

Example 1. (One-Time Pad)

Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}$,

$\mathtt{Enc}_k(m) = k \oplus m$, $\mathtt{Dec}_k(c) = k \oplus c$

$$\mathbb{P}(\mathtt{Enc}_k(m) = c) = \frac{1}{2},\ \forall m \in \mathcal{M}, c \in \mathcal{C}$$

Some Examples

Definition (XOR)

For $a, b \in \{0,1\}^N$, $(a \oplus b)_i = \begin{cases} 1, & a_i \neq b_i \\ 0, & a_i = b_i \end{cases}$.

Or equivalently, $a \oplus b = (a + b) \mod 2 = (a + b)_{\mathbb{Z}_2^N}$

Example 1. (One-Time Pad)

Let $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0,1\}$,

$\texttt{Enc}_k(m) = k \oplus m$, $\texttt{Dec}_k(c) = k \oplus c$

$$\mathbb{P}(\texttt{Enc}_k(m) = c) = \frac{1}{2},\ \forall m \in \mathcal{M}, c \in \mathcal{C}$$

$$|\mathcal{K}| = |\mathcal{M}|$$

Shannon's Theorem

Theorem

Let SE$= (\mathtt{KeyGen}, \mathtt{Enc}, \mathtt{Dec})$ *be a perfectly secure and correct encryption scheme, let* $\mathcal{M}$ *be the message space and* $\mathcal{K}$ *be the key space, then*

$$|\mathcal{K}| \geq |\mathcal{M}|.$$

Imperfect Correctness

Definition (Imperfect Correctness)

An SE is $t-$imperfectly correct if

$$\forall m \in \mathcal{M}, \mathbb{P}(\texttt{Dec}_k\texttt{Enc}_k(m) = m) \geq 2^{-t}.$$

We trade some accuracy for efficiency (by trying to make $\mathcal{K}$ small)

Assignments

Problem 1.

Devise a $t-$imperfectly correct scheme that achieves perfect security with $|\mathcal{K}| < |\mathcal{M}|$ when $t \geq 1$.

Problem 2.

(Bonus question) Prove that for any $t-$imperfectly correct scheme that achieves perfect security it must be the case that $|\mathcal{K}| \geq |\mathcal{M}| \cdot 2^{-t}$.

Problem 1.

Scheme 1

$\mathcal{M} = \{0, 1, 2, 3\}$, $\mathcal{K} = \{0, 1\} = \mathcal{C}$.

$$\texttt{Enc}_k(m) = ((k+m) \mod 2)$$
$$\texttt{Dec}_k(c) = ((k+c) \mod 2) + 2k$$

$$\Rightarrow \texttt{Dec}_k\texttt{Enc}_k(m) = (m \mod 2) + 2k$$

$$\Rightarrow \mathbb{P}(\texttt{Enc}_K(m) = c) = \frac{1}{2},$$

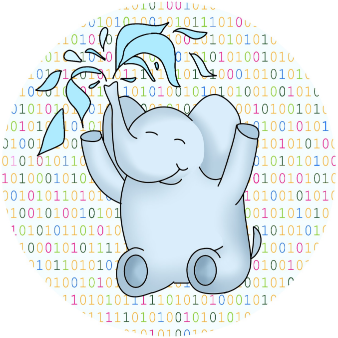
$$\mathbb{P}(\texttt{Dec}_K\texttt{Enc}_K(m) = m) = \frac{1}{2},$$

$\forall m \in \mathcal{M}, c \in \mathcal{C}$.

Table of Encryption-Decryption

k	m	$\to$	c	$\to$	m
0	0		0		0
0	1		1		1
0	2		0		0
0	3		1		1
1	0		1		2
1	1		0		3
1	2		1		2
1	3		0		3

Kiitos - Dankjewel - Tack - Dankeschön - Thank you - Grazie - Obrigado



Hvala - Благодаря ти - Дякую - Tusen takk - Gracias - Merci - Köszönöm