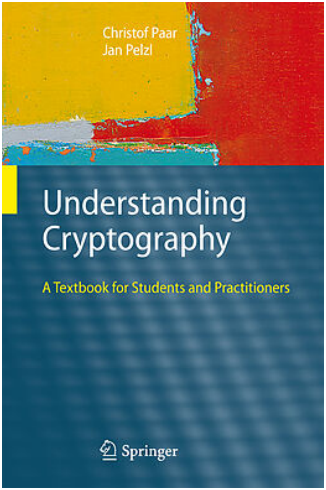
HA NOI UNIVERSITY OF SCIENCE AND TECHNOLOGY
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Introduction to Cryptography and Security

Introduction

Textbook

https://www.crypto-textbook.com


Christof Paar
Jan Pelzl
Understanding Cryptography
A Textbook for Students and Practitioners
Springer

Outline

1. Introduction

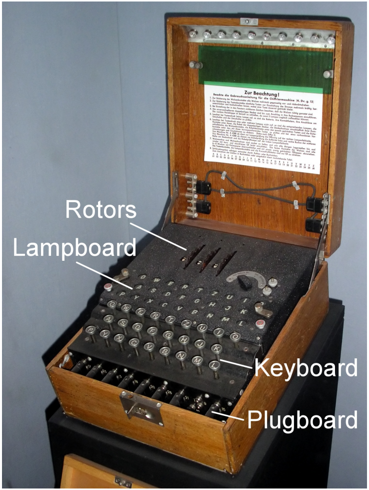
2. Symmetric Cryptography

3. Cryptanalysis

4. One-time Pad

World War II

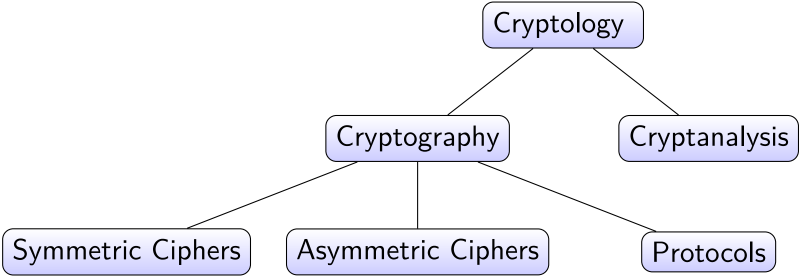
German Enigma encryption machine



Back to about 2000 B.C

Scytale of Sparta

Classification



Outline

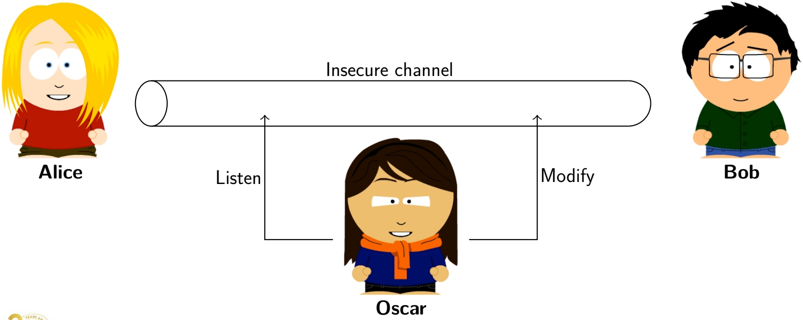
1. Introduction
2. Symmetric Cryptography
3. Cryptanalysis
4. One-time Pad

Encryption

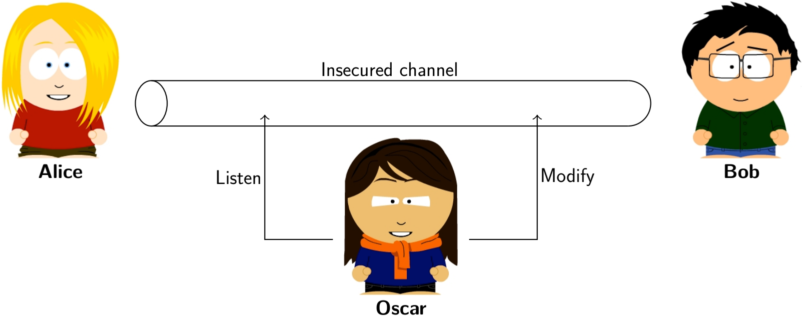
Goal: Confidentiality of transmitted (or stored) message.

Characters in the game :

- Alice, Bob are "good guys" (by Wikipedia)
- Oscar is "eavesdropper", "adversary"



Cryptography Approach



- Bob knows a key k that Oscar doesn't (Oscar know the system).
- Alice can encrypt x such that knowledge of k allows for decryption.
- Oscar sees ciphertext y, but learns nothing about x.

Notation

- x, m are plaintext or message;
- y, c are ciphertexts;
- k is the key;

- Enc is the encryption function;
- Dec is the decryption function;
- Gen is the key generation function.

Symmetric Cryptography

Alice & Bob both know key k. shared symmetric key

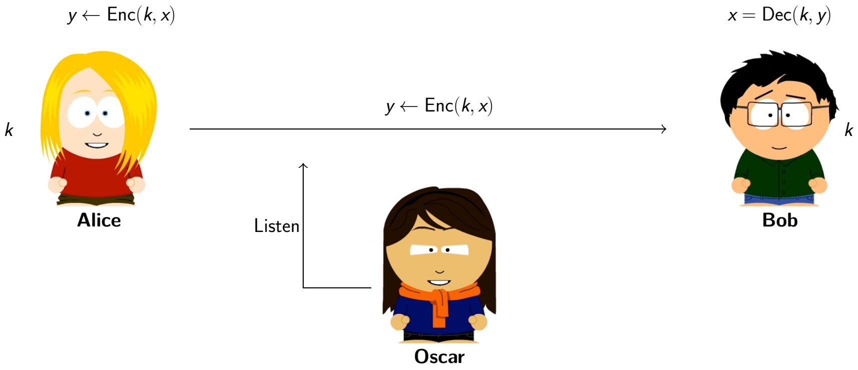
Algorithms:

$k \leftarrow \mathsf{Gen}(1^\lambda)$	generate key of length λ
$y \leftarrow \mathsf{Enc}(k, x)$	encrypt message x with key k, result is y
$x = \mathsf{Dec}(k, y)$	decrypt y using k to obtain x.

Setup:

- Someone (may be Alice or Bob) computes $k \leftarrow \mathsf{Gen}(1^\lambda)$.
- and ensures that Alice & Bob both have k (and Oscar doesn't) (How?!)

Symmetric-key cryptosystem



$y \leftarrow \mathrm{Enc}(k, x)$

$x = \mathrm{Dec}(k, y)$

k

$y \leftarrow \mathrm{Enc}(k, x)$

k

Alice

Bob

Listen

Oscar

Questions

- Can Oscar know the encryption and decryption functions?
- Yes. She knows.

- Why not hide the encryption and decryption functions?
- Because it's safer to make the functions public!

Kerckhoffs' Principle

> *A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.*

Remark: Kerckhoffs' Principle is is counterintuitive.

NaCl (Networking and Cryptography library)

- NaCl (pronounced "salt") is a new easy-to-use high-speed software library for network communication, encryption, decryption, signatures, etc.
- NaCl's goal is to provide all of the core operations needed to build higher-level cryptographic tools.
- NaCL in Wikipedia https://en.wikipedia.org/wiki/NaCl_(software)
- NaCl was created by the mathematician and programmer Daniel J. Bernstein (Daniel J. Bernstein)

Substitution Cipher

Ví dụ

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

For instance, the pop group ABBA would be encrypted as kddk.

What is the key *k* of this cipher?

Exercise

Consider the ciphertext that is encrypted by the substitution cipher.

```
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb
      hcc hwwhbsqvqbre hwq vhlq
```

Question

- Can you guess what the plaintext is?
- Is the substitution cipher secure?

Outline

1. Introduction

2. Symmetric Cryptography

3. Cryptanalysis

4. One-time Pad

First Attack: Brute-Force or Exhaustive Key Search

- Let (x, y) denote the pair of plaintext and ciphertext,
- and let $K = \{k_1, \ldots, k_n\}$ be the key space of all possible keys k_i.
- A brute-force attack now checks for every $k_i \in K$ if

$$\mathrm{Dec}(k_i, y) = x.$$

- If the equality holds, a possible correct key is found; if not, proceed with the next key.

Brute-Force Attack for Substitution Cipher

Question

What is the key space of the cipher?

Second Attack: Letter Frequency Analysis

The major weakness of the substitution cipher is that each plaintext symbol always maps to the same ciphertext symbol.

Ví dụ

$$\begin{aligned} &\texttt{A} \longrightarrow \texttt{k} \\ &\texttt{B} \longrightarrow \texttt{d} \\ &\texttt{C} \longrightarrow \texttt{w} \\ &\quad \ldots \end{aligned}$$

For instance, the pop group `ABBA` would be encrypted as `kddk`.

Second Attack: Letter Frequency Analysis

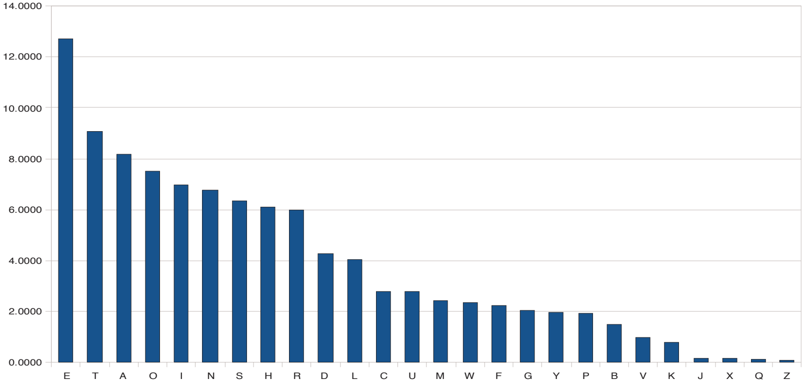
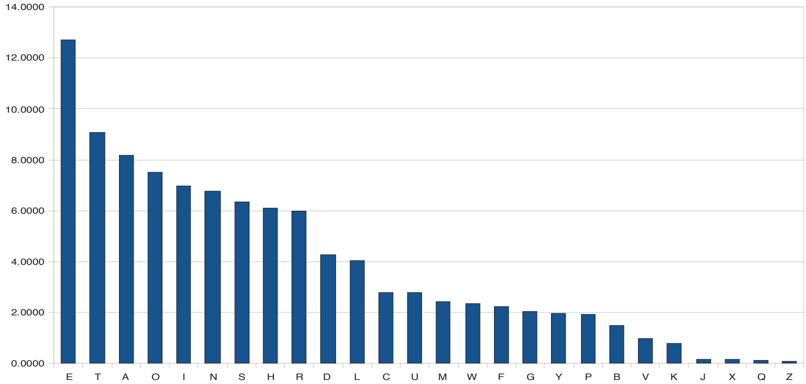


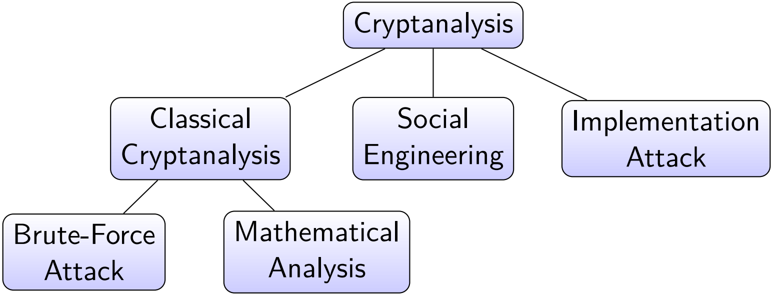
Figure: Relative letter frequencies of the English language

Exercise: Decrypt the ciphertext

```
iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb
       hcc hwwhbsqvqbre hwq vhlq
```



Overview of Cryptanalysis



Security Objective

- Oscar cannot distinguish

$$y_1 = \mathsf{Enc}(k, x_1) \quad \text{and} \quad y_2 = \mathsf{Enc}(k, x_2)$$

  even if she know (or choose) x_1, x_2 (of same length). Encryption typically does not hide the message length.
- The security notion is called "ciphertext indistinguishability" or "semantic security".

Attacks

- Known ciphertext
- Know ciphertext/plaintext pairs
- chosen plaintext
- chosen ciphertext

Assume *k* is reused.

Outline

1 Introduction

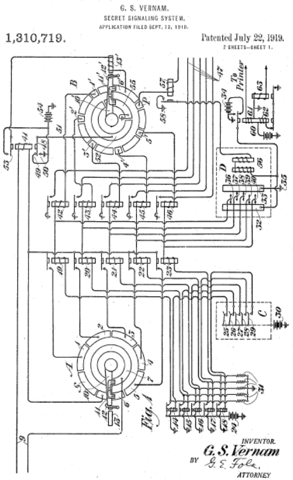
2 Symmetric Cryptography

3 Cryptanalysis

4 One-time Pad

One-Time Pad or OTP

- Vernam 1917. Paper-tape based (patent)
- Message, key, ciphertext have the same length (λ bit).
- Key k also called pad; it is random and known only by Alice & Bob.



XOR Operation

XOR of two strings in $\{0,1\}^n$ is their bit-wise addition $\mod 2$.

x	y	$\oplus$
0	0	0
0	1	1
1	0	1
1	1	0

$$\begin{array}{cc} & 1\ 0\ 1\ 1\ 0\ 0 \\ \oplus & 0\ 1\ 1\ 0\ 1\ 0 \\ \hline & 1\ 1\ 0\ 1\ 1\ 0 \end{array}$$

An important property of XOR

Theorem

Let x a random variable $\{0,1\}^n$, and k an independent uniform variable on $\{0,1\}^n$.
Then $y = x \oplus k$ is uniform variable on $\{0,1\}^n$.

Proof.

For $n = 1$, we have:

x	$\Pr$
0	p_0
1	p_1

k	$\Pr$
0	$1/2$
1	$1/2$

x	k	$\Pr$
0	0	$p_0/2$
0	1	$p_0/2$
1	0	$p_1/2$
1	1	$p_1/2$

□

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.

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

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

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

Exercise

List the advantages and disadvantages of OTP.

Thank you!