



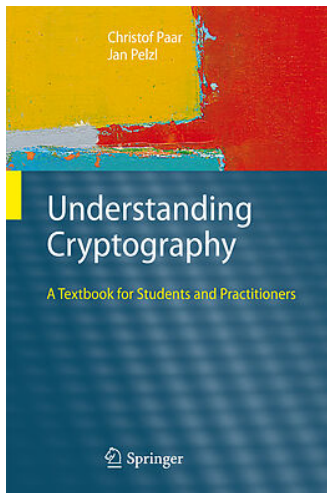
ĐẠI HỌC BÁCH KHOA HÀ NỘI  
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

# Nhập môn An toàn Thông tin

## Giới thiệu về mật mã

# Tài liệu

<https://www.crypto-textbook.com>

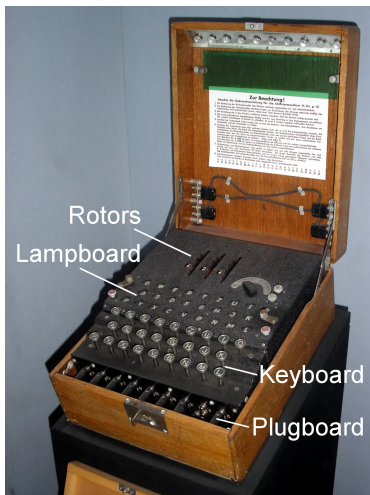


# Nội dung

- 1 Tổng quan
- 2 Mã hóa
- 3 Thăm mã
- 4 One-time Pad

# Thế chiến II

## Máy Enigma của Đức

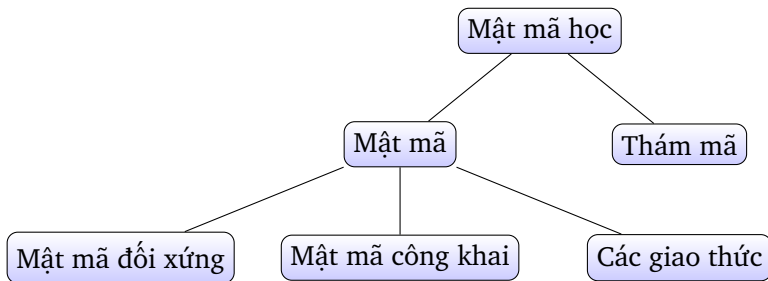


# Mật mã cổ đại

Ổng tròn của người Hy Lạp



## Phân loại



# Nội dung

1 Tổng quan

2 Mã hóa

3 Thăm mã

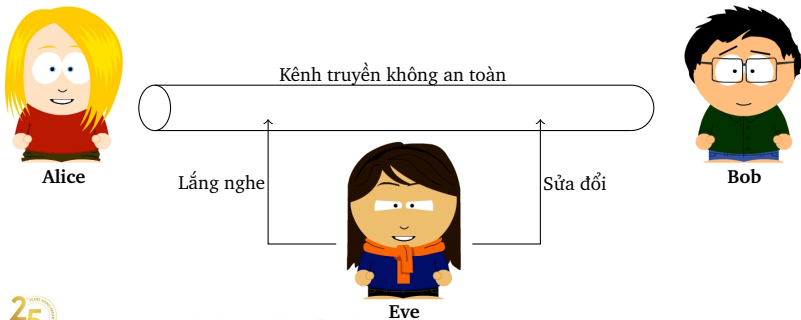
4 One-time Pad

# Mã hóa

**Mục tiêu:** Đảm bảo **tính bí mật** cho các thông điệp được gửi đi (hoặc lưu trữ).

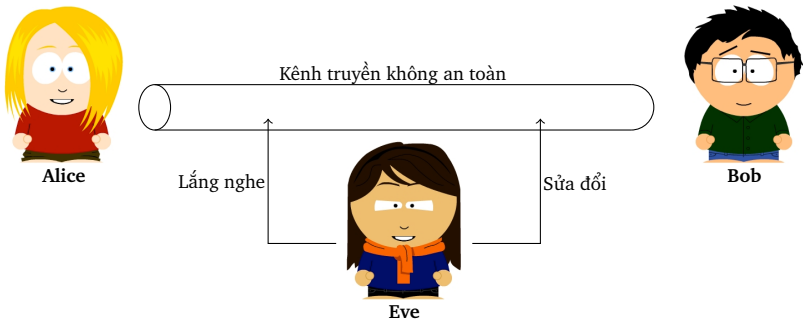
**Nhân vật** tham gia trò chơi:

- Alice, Bob là người “tốt” (theo Wikipedia)
- Oscar là kẻ “nghe trộm”, “tấn công”





## Cách tiếp cận của mật mã



- Bob biết **khóa**  $k$  mà Eve không biết.
- Alice có thể **mã hóa** thông điệp  $x$  sao cho người biết khóa  $k$  có thể giải mã.
- Oscar có bản mã  $y$ , nhưng **không biết thông tin** gì về  $x$ .

## Ký hiệu

- $x, m$  là bản rõ;
- $y, c$  là bản mã;
- $k$  là khoá;
- Enc là hàm mã hoá;
- Dec là hàm giải mã;
- Gen là hàm sinh khoá.

# Mật mã khóa đối xứng

Alice & Bob đã có chung **khóa chia sẻ**

## Thuật toán:

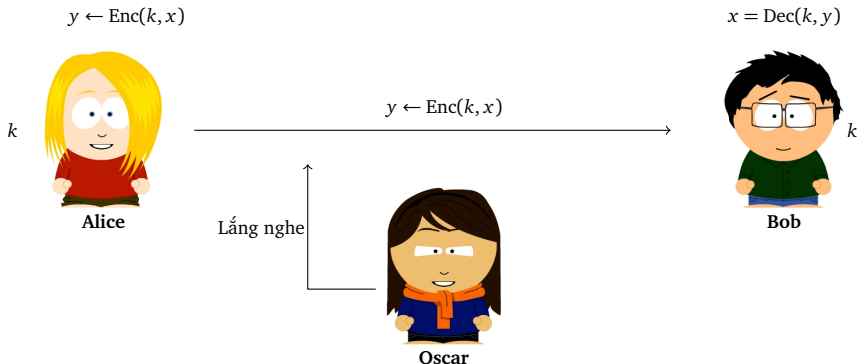
$k \leftarrow \text{Gen}(1^\lambda)$     sinh khóa độ dài  $\lambda$   
 $y \leftarrow \text{Enc}(k, x)$     mã hóa thông điệp  $x$  với khóa  $k$ , kết quả là bản mã  $y$   
 $x = \text{Dec}(k, y)$     giải mã  $y$  dùng khóa  $k$  để lấy được  $x$ .

## Thực hiện:

- Ai đó (có thể là Alice hoặc Bob) tính  $k \leftarrow \text{Gen}(1^\lambda)$ .
- Đảm bảo rằng Alice & Bob cả hai đều có  $k$  (và Oscar không có) **(Làm thế nào !?)**

# Mật mã khóa đối xứng

Trao đổi thông tin



# Nguyên lý Kerckhoffs

*Hệ mật phải an toàn cả khi kẻ tấn công (Oscar) biết mọi chi tiết về hệ thống, ngoại trừ khoá bí mật. Cụ thể, hệ thống phải an toàn cả khi kẻ tấn công biết rõ hàm mã hoá và hàm giải mã.*

## Bài tập thực tế

- Tìm hiểu thư viện NaCl (Networking and Cryptography library)
- Để bắt đầu, hãy xem wikipedia  
[https://en.wikipedia.org/wiki/NaCl\\_\(software\)](https://en.wikipedia.org/wiki/NaCl_(software))
- Xem thêm về tác giả của NaCl (Daniel J. Bernstein)

# Hệ mã thay thế

## Ví dụ

$A \rightarrow k$

$B \rightarrow d$

$C \rightarrow w$

...

Xâu ABBA sẽ được mã hoá thành kddk.

Khoá  $k$  của hệ mã trên là gì?

Xét bản mã được mã hoá bởi hệ mã thay thế

```
1 iq ifcc vqqr fb rdq vfllcq na rdq cfjwhwz hr bnnb  
2 hcc hwwhbsqvqbrev hwq vhlq
```

### Câu hỏi

- Bạn có thể đoán được bản rõ là gì không?
- Hệ mã này có an toàn?



# Nội dung

1 Tổng quan

2 Mã hóa

3 Thám mã

4 One-time Pad

## Tấn công vét cạn khoá

- Xem hệ mã như một hộp đen
- Cần ít nhất một cặp bản rõ, bản mã  $(x_0, y_0)$
- Kiểm tra mọi khoá  $k$  cho đến khi thoả mãn điều kiện:

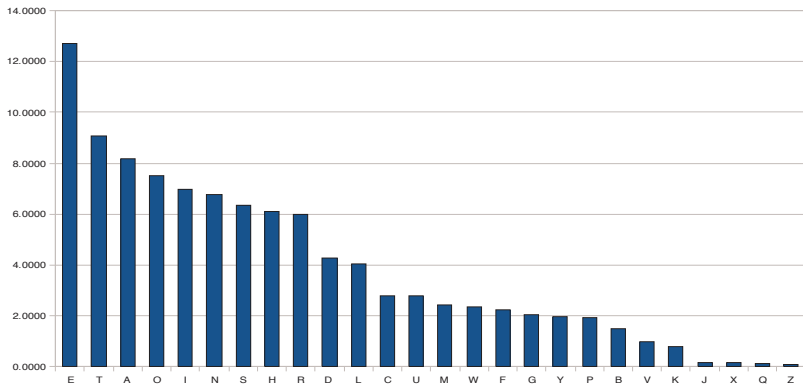
$$\text{Dec}(k, y_0) = x_0.$$

### Câu hỏi

Không gian khoá của hệ mã thay thế là gì?

# Tần công bằng Phân tích tần suất

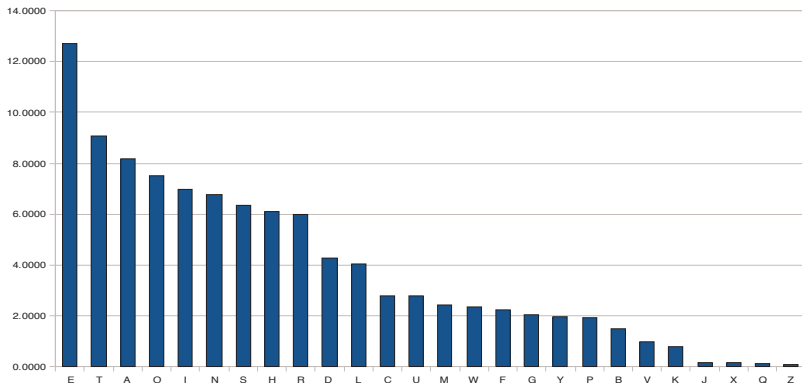
**Tính chất:** Hai chữ giống nhau trong bản rõ ánh xạ thành hai chữ giống nhau trong bản mã.



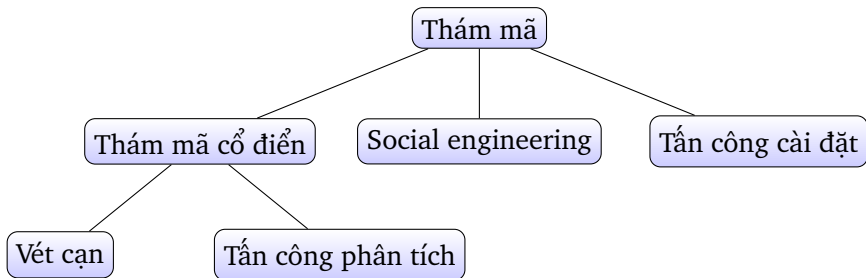
Hình: Bảng tần suất của chữ cái Tiếng Anh

## Bài tập: Giải mã

1 iq ifcc vqqr fb rdq vlllcq na rdq cfjwhwz hr bnnb  
2 hcc hwwhbsqvqbre hwq vhlq



# Phân loại các kiểu tấn công



# Thế nào là an toàn?

**Mục tiêu an toàn:** Không phân biệt được bản mã hay còn gọi là an toàn ngữ nghĩa

- Oscar không thể phân biệt được  $y_1 = \text{Enc}(k, x_1)$  với  $y_2 = \text{Enc}(k, x_2)$  kể cả khi chị ta biết (hoặc chọn)  $x_1$  và  $x_2$  có cùng độ dài.

**Các kiểu tấn công:**

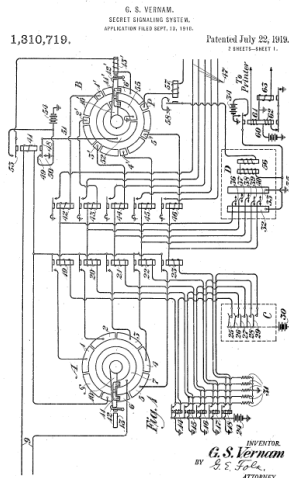
- Biết bản mã
- Biết một số cặp bản mã/bản rõ
- Chọn bản rõ
- Chọn bản mã
- v.v.

# Nội dung

- 1 Tổng quan
- 2 Mã hóa
- 3 Thăm mã
- 4 One-time Pad

# One-Time Pad hay OTP

- Vernam 1917. Bằng phát minh.
- Thông điệp, khóa, và bản mã có cùng độ dài ( $\lambda$  bit).
- Khóa  $k$  cũng được gọi là pad; là ngẫu nhiên và chỉ biết bởi Alice & Bob.





## Phép toán XOR

XOR của hai chuỗi trên  $\{0, 1\}^n$  là tổng từng bit theo mô đun 2.

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

$$\begin{array}{r} 1\ 0\ 1\ 1\ 0\ 0 \\ \oplus\ 0\ 1\ 1\ 0\ 1\ 0 \\ \hline 1\ 1\ 0\ 1\ 1\ 0 \end{array}$$

# Một tính chất quan trọng của XOR

## Định lý

Xét  $x$  là một biến ngẫu nhiên trên  $\{0, 1\}^n$ , và xét  $k$  là một biến ngẫu nhiên **đều** trên  $\{0, 1\}^n$ . Khi đó

$$y = x \oplus k$$

là biến ngẫu nhiên **đều** trên  $\{0, 1\}^n$ .

## Chứng minh.

Khi  $n = 1$ , ta có:

$x$	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	$p_1/2$
1	0	$p_0/2$
1	1	$p_1/2$

## Mã hóa OTP

- **Gen:** sinh dãy bit ngẫu nhiên độ dài  $\lambda$ .
- **Enc:** Biểu diễn thông điệp như xâu nhị phân và cộng theo mod 2 với khóa.

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

- **Dec:** Giống như mã hóa, chỉ cộng với  $k$ .

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

## Bài tập

Hãy liệt kê các ưu nhược điểm của hệ OTP.



25  
SOICT

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG  
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Cảm ơn!



[soict.hust.edu.vn/](http://soict.hust.edu.vn/)



[fb.com/groups/soict](https://fb.com/groups/soict)

