

AN TOÀN VÀ BẢO MẬT HỆ THÔNG THÔNG TIN

Giáo viên: Trần Hồng Diệp

Bộ môn: Tin học

Email: diepth18@yahoo.com
diepth18@gmail.com



Nội dung môn học

Đại cương về AT & BM hệ thống thông tin

Mật mã học

An toàn phần mềm

An toàn hệ điều hành

An toàn cơ sở dữ liệu

An toàn mạng

CHƯƠNG 2.

Mật mã học

- Mật mã học (Cryptology)
 - Mật mã (Cryptography)
 - Mã thám (Cryptanalysis)
- Mật mã
 - Phép mã hóa (Cypher): tăng cường tính bí mật và toàn vẹn thông tin.
 - Giao thức mật mã (Cryptographic Protocol): xây dựng các giao thức trao đổi thông tin bí mật.
- Mã thám
 - Phá mã

Mục tiêu an toàn của mật mã

- Bí mật (Confidentiality)
- Toàn vẹn (Integrity)
- Xác thực (Authentication)
- Chống phủ nhận (Non – repudiation)
- ...

Hệ mật mã

Hệ mật mã là bộ gồm 5 thành phần (K,M,C,E,D)

- K: Không gian khóa (key)
- M: Không gian Tin (Message/Plaintext)
- C: Không gian mã (Cipher)
- E: Hàm mã hóa (Encryption)
 - $E: K \times M \rightarrow C$
- D: Hàm giải mã (Decryption)
 - $D: K \times C \rightarrow M$

Nội dung cơ bản

- Mật mã không khóa
- Mật mã khóa bí mật
- Mật mã khóa công khai
- Chữ ký điện tử và hàm băm
- Quản lý khóa
- Giao thức mật mã

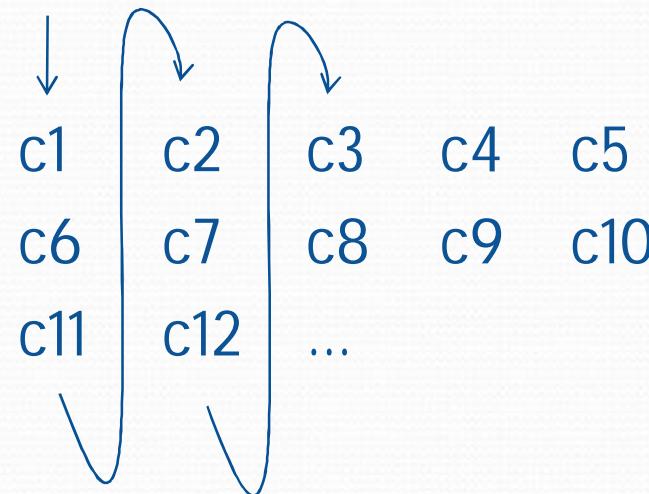
2.1. Mật mã không khóa

Mô hình mã hóa và giải mã:



Mã hoán vị

Hoán vị cột:



Chuyển thành:

c1	c6	c11	c2	c7
c12	c3	c8	...	

Mã hoán vị: ví dụ

Tin:

T H I S I
S A M E S
S A G E S
O S H O W
H O W A C
O L U M N
A R T R A
N S P O S
I T I O N
W O R K S

Mã hoán vị: ví dụ

Tin:

T H I S I
S A M E S
S A G E S
O S H O W
H O W A C
O L U M N
A R T R A
N S P O S
I T I O N
W O R K S

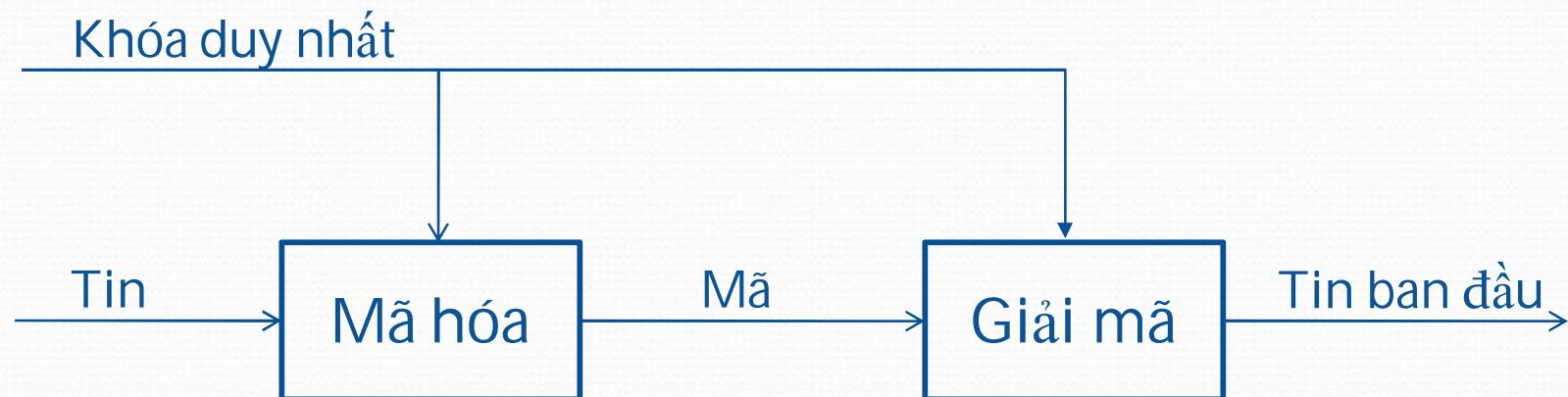
Mã:

t s s o h
o a n i w
h a a s o
l r s t o
i m g h w
u t p i r
s e e o a
m r o o k
l s t w c
n a s n s

2.2. Mật mã khóa bí mật

Còn được gọi là mật mã đối xứng.

Mô hình mã hóa và giải mã:



Mật mã khóa bí mật

- Duy nhất một khóa chung cho cả hai quá trình:
Mã hóa và Giải mã
 - $C = E(K, M)$
 - $M = D(K, C)$
- Khóa phải được giữ bí mật

Các hệ mật mã khóa bí mật

- Mã luồng
 - Mã Ceasar
 - Mã Vigenere
 - Mã Vernam
- Mã khối
 - **DES**
 - AES
 - Bài tập (DES)

Mã luồng

- Đơn vị mã hóa cơ bản là các ký tự
 - Các ký tự trong Tin gốc được mã hóa tách biệt

Mã Ceasar

- Hàm mã hóa: $c = m + n$
 - m : ký tự trong Tin gốc
 - c : ký tự tương ứng trong Mã
 - n : độ dịch chuyển
 - $+$: phép cộng modulo 26

- Ví dụ:
 - $n = 3$
 - Tin: ABCDEFGHIJKLMNOPQRSTUVWXYZ
 - Mã: defghijklmnopqrstuvwxyzabc



Mã Ceasar

□ Tin gốc:

TREATY
IMPOSSIBLE

Mã Ceasar

Tin gốc:

TREATY
IMPOSSIBLE

Mã:

WUHDWB
LPSRVVLEOH

Mã Vigenère

Khóa

Tin

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Mã Vigenère: Ví dụ

❑ Khóa:

- BENCH

❑ Tin gốc:

- A LIMERICK PACKS LAUGHS ANATOMICAL

❑ Nối dài khóa:

- B ENCHBEC HBENC HBENCH BENCHBENCH

❑ Mã hóa:

- Khóa: B ENCHBEC HBENC HBENCH BENCHBENCH

- Tin gốc: A LIMERICK PACKS LAUGHS ANATOMICAL

- Mã: B PVOLSMPM WBGXU SBYTJZ BRNVVNMPGS

Mã Vernam

- Ký tự là các bit
- Khóa
 - $K = K_1K_2K_3\dots K_n$
 - Số ngẫu nhiên
- Tin gốc
 - $M = M_1M_2M_3\dots M_n$
- Mã
 - $C = C_1C_2C_3\dots C_n$

Trong đó: $C_i = K_i \text{ xor } M_i$

Mã khối

- Đơn vị mã hóa cơ bản là các khối ký tự
- Các tham số bao gồm: kích thước khối và chiều dài khóa
 - Kích thước khối lớn để chống tấn công bằng thống kê
 - Chiều dài khóa lớn để chống tấn công vét cạn



Cảm ơn!

