MẬT MÃ ỨNG DỤNG TRONG AN TOÀN THÔNG TIN

(Applied Cryptography In Secure Information System)

ThS. Bùi Hữu Đông
buihuudong19@gmail.com
0903.82.36.46

Học viện Kỹ thuật Mật mã, khoa An toàn thông tin

Ngày 23 tháng 10 năm 2020

Buổi 02

MÃ HÓA ĐỐI XỨNG
(Symmetric Cryptography)

MÃ HÓA ĐỐI XỨNG CĂN BẢN
(Basic Symmetric Cryptography)

Giới thiệu

- Khái niệm: Mã hóa đối xứng (còn gọi là mã hóa khóa đồng bộ) là một thuật toán mà trong đó cả hai quá trình mã hóa và giải mã đều dùng một khóa.
- Đặc điểm:
  - Tốc độ lập mã và giải mã khá nhanh, được cải tiến rất an toàn. Hiện nay, có nhiều phần mềm thương mại hỗ trợ thuật toán mã hóa đối xứng rất hiệu quả. Ví dụ: AES, 3-DES...
  - Vấn đề lớn là chuyển giao khóa giữa bên nhận và gửi
  - Mã hóa đối xứng *không đảm bảo* tính toàn vẹn dữ liệu
  - Mã hóa đối xứng thường dùng cho *single user*. Tức là sử dụng với mục đích mã hóa dữ liệu của cá nhân hoặc tổ chức riêng lẻ để chống xâm nhập của kẻ xấu (Spyware, Trojan hay các phần mềm độc)

Giới thiệu

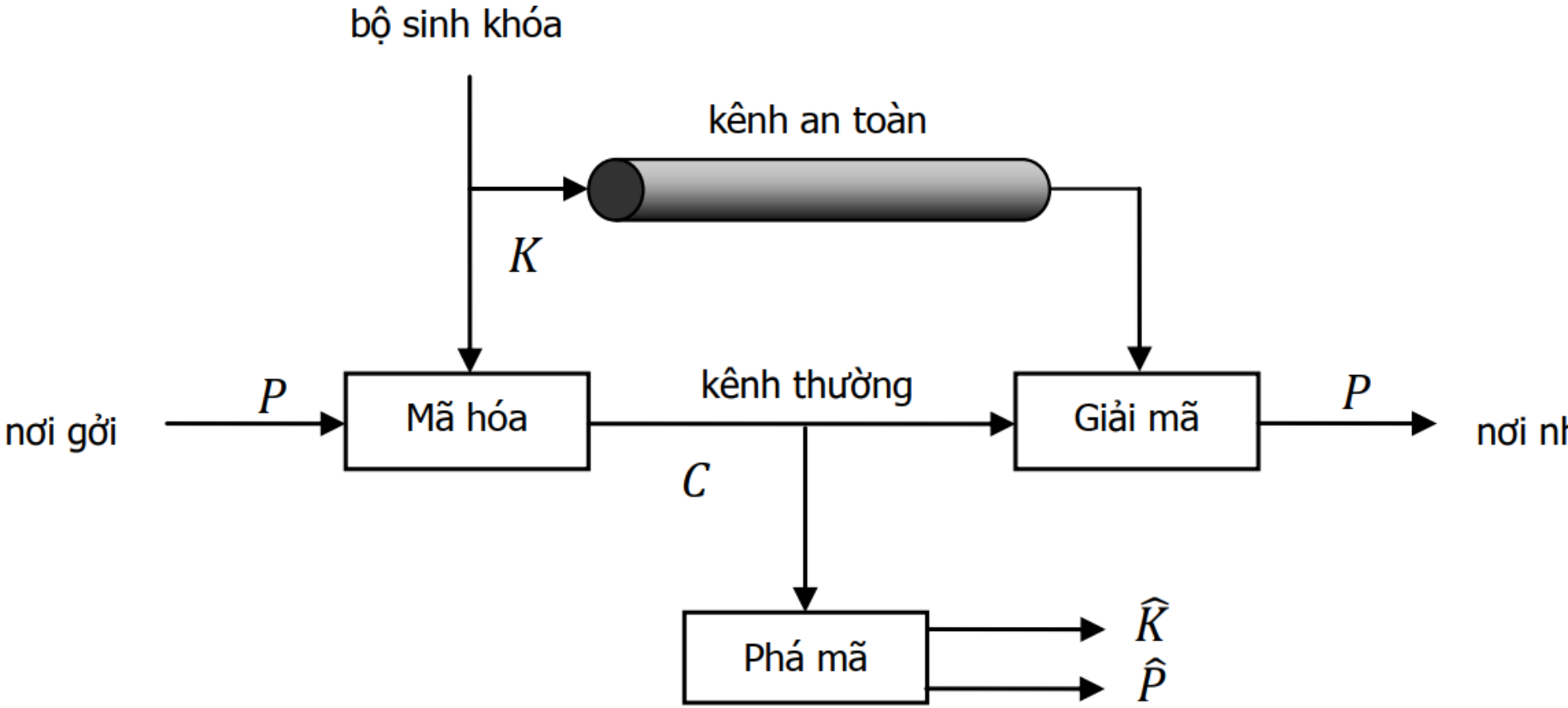
- Một số phần mềm mã hóa đối xứng:
  - **Blowfish**: là một thuật toán mã hóa đối xứng (64 bit cipher) do Bruce Schneier thiết kế năm 1993. Blowfish có các độ dài khóa từ 32 đến 448 bit
  - **CAST** - Carlisle Adams và Stafford Tavares: là một thuật toán mã hóa rất phổ biến, mã hóa khối cipher 64 bit và cho phép độ dài khóa lên đến 128 bit
  - **IDEA** - International Data Encryption Algorithm: là một thuật toán mã hóa đối xứng do TS. X. Lai và GS. J. Massey xây dựng nhằm thay thế thuật toán DES chuẩn. IDEA cũng sử dụng khóa có độ dài là 128 bit.

Giới thiệu

- **RC2:** là một thuật toán mã hóa có kích thước khóa thay đổi do Ron Rivest tạo ra
- **RC4:** cũng là một thuật toán do Ron Rivest phát triển năm 1987. Đây là một thuật toán mã hóa dòng với khóa có kích thước thay đổi. Kích thước khóa của RC4 có thể đạt tới 2048 bit (thông thường là 256 bit)
- **RC6:** là thuật toán do Ron Rivest, Matt Robshaw, Ray Sidney, và Yiqun Lisa Yin thiết kế nhằm đáp ứng yêu cầu của cuộc thi AES (Advanced Encryption Standard).
- **Twofish** - do do Bruce Schneier, John Kelsey, Chris Hall, Niels Ferguson, David Wagner and Doug Whiting thiết kế. Là một thuật toán mã hóa đối xứng khối, có kích thước khối là 128 và chấp nhận các khóa có mọi độ dài cho đến 256 bit.

Giới thiệu

- Mô hình mã hóa đối xứng (Symmetric Ciphers):



Hình: Mô hình mã hóa đối xứng

Giới thiệu

Mô hình mã hóa trên gồm 05 yếu tố:

- Bản rõ P (Plaintext)
- Thuật toán mã hóa E (encrypt algorithm)
- Khóa bí mật K (secret key)
- Bản mã C (ciphertext)
- Thuật toán giải mã D (decrypt algorithm)

  Trong đó:

  $$C = E(P, K)$$

  $$P = D(C, K)$$

  Có thể viết gọn: $P = K(K(P))$

Giới thiệu

- Phá mã: là hành động tấn công vào bản mã để tìm ra bản rõ mà không cần khóa. Do đó, mật mã đối xứng gọi là an toàn khi nó không thể phá mã hoặc thời gian phá mã lâu.

Kích thước khóa (bít)	Số lượng khóa	Thời gian thực hiện (tốc độ thử: 10^3 khóa/giây)	Thời gian thực hiện (tốc độ thử: 10^9 khóa/giây)
32	$2^{32} \approx 4.3 \times 10^9$	35.8 phút	2.15 mili giây
56	$2^{56} \approx 7.2 \times 10^{16}$	1142 năm	10.01 giờ
128	$2^{128} \approx 3.4 \times 10^{38}$	5.4×10^{24} năm	5.4×10^{18} năm
168	$2^{168} \approx 3.7 \times 10^{50}$	5.9×10^{36} năm	5.9×10^{30} năm
hoán vị 26 ký tự	$26! \approx 4 \times 10^{26}$	6.4×10^{12} năm	6.4×10^{6} năm

Hình: Thời gian phá mã ứng với kích thước khóa

Phương pháp mã hóa Ceasar

- Phương pháp: là cách mã hóa bản tin gốc bằng cách thay thế mỗi chữ trong bản tin bằng chữ đứng sau nó k vị trí trong bảng chữ cái
- Thí dụ: giả sử ta chọn $k = 3$ ta có:

Ban đầu: 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

Thay thế: 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

Giả sử có bản rõ là: *meet me after the toga party*

Bản mã hóa sẽ là: PHHW PH DIWHU WKH WRJD SDUWB

- Chỉ số tương ứng:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Phương pháp mã hóa Ceasar

- Mã hóa và giải mã Ceasar:

Quá trình mã hóa: $C = (p + k) mod(26)$. Tức mỗi chữ cái p sẽ được thay thế bằng c

Quá trình giải mã: $p = (C - k) mod(26)$. Trong đó k là khóa.

Mã hóa Ceasar không thật an toàn, do hacker có thể thử tất cả 25 khóa để tìm bản rõ có nghĩa.

Phương pháp mã hóa Ceasar

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	**meet me after the toga party**
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

- Khi thử tất các khóa (Bruce force) Hacker sẽ tìm thấy bản rõ có ý nghĩa nhất.
- Trong thí dụ này $k = 3$ cho bản rõ có ý nghĩa hơn cả.

Phương pháp mã hóa đơn bảng

• Phương pháp: là phương pháp mã hóa không phải là phép dịch k vị trí của các chữ cái $A, B, C...$ mà là một hoán vị của 26 chữ cái này và mỗi hoán vị tương ứng với một khóa.

• Thí dụ: giả sử ta có hoán vị sau:

Chữ ban đầu: 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

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

Theo đó bản rõ: *meet me after the toga party*

Được mã hóa: *NJJU NJ ZRUJM UKJ UVSZ DZMUE*

• Nhận xét: Việc mã hóa được tiến hành bằng cách thay thế một chữ cái trong bản rõ thành một chữ cái trong bản mã. Số lượng hoán vị của 26 chữ cái là 26! => số lượng khóa.

Phương pháp mã hóa đa bảng

(Polyalphabetic Substitution Cipher)

- Mô tả:

◦ Với phương pháp đơn bản thì mỗi ký tự sẽ được ánh xạ vào một ký tự duy nhất.

◦ Phương pháp này do nhà ngoại giao tên Blaise de Vigenère - thế kỷ XVI đưa ra.

◦ Theo phương pháp này thì chiều dài của khóa sẽ bằng chiều dài bản tin rõ.

◦ Vigenère định ra một bảng mã như sau:

Phương pháp mã hóa đa bảng

(Polyalphabetic Substitution Cipher)

key	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

Phương pháp mã hóa đa bảng

(Polyalphabetic Substitution Cipher)

- Thí dụ: Giả sử cần mã hóa bản rõ *"We are discovered, save yourself"* với khóa k = "DECEPTIVE".

  ▷ Quá trình mã hóa:

plaintext:	wearediscoveredsaveyourself
key:	DECEPTIVEDECEPTIVEDECEPTIVE
ciphertext:	ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Trong thí dụ trên, các chữ cái e trong bản rõ được mã hóa tương ứng thành I, T, G, T, H, M trong bản mã. Do vậy, nếu dùng phương pháp thám mã dựa trên thống kê tần suất chữ cái là không khả thi.

Phương pháp mã hóa đa bảng

(Polyalphabetic Substitution Cipher)

- Quá trình giải mã:

  Để giải mã ta làm ngược lại. Tức là, bắt đầu từ trái qua phải với mỗi ký tự *(*key) làm *dòng* ta tìm cột mà khi dóng xuống ta có giá trị là ký tự trong chuỗi đã mã hóa. Ký tự trong cột đó chính là ký tự của chuỗi ban đầu.

  Lưu ý: Trên thực tế, bảng mã không bắt buộc là 26 ký tự alphabet mà có thể tùy ý tùy vào người mã hóa, ví dụ như sử dụng ký tự tiếng Việt, tiếng Nhật.

Phương pháp mã hóa đa ký tự - Mã Hill

- Mô tả mã Hill:
  - Là một dạng mã hóa đa bảng khác do Lester S.Hill đưa ra năm 1929
  - Mã Hill dùng 26 chữ cái được đánh số từ 0 đến 25 như sau:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

  - Thực hiện mã hóa một lần m ký tự bản rõ (kí hiệu: $p_1, p_2, \ldots p_m$) thay thế thành m ký tự trong bản mã (ký hiệu: $c_1, c_2, \ldots, c_m$)
  - Việc thay thế này được thực hiện bằng m phương trình tuyến tính. Giả sử $m = 3$ ta có:

$$c_1 = k_{11}p_1 + k_{12}p_2 + k_{13}p_3 mod(26)$$

$$c_2 = k_{21}p_1 + k_{22}p_2 + k_{23}p_3 mod(26)$$

$$c_3 = k_{31}p_1 + k_{32}p_2 + k_{33}p_3 mod(26)$$

Phương pháp mã hóa đa ký tự - Mã Hill

Các phương trình trên được biểu diễn thành vector và phép nhân ma trận như sau:

$$\begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} \quad mod(26)$$

Tổng quát: $C = (KP)mod(26)$. Trong đó K là ma trận khóa.

Phương pháp mã hóa đa ký tự - Mã Hill

- Thí dụ: với bản rõ là P: *paymoremoney* và khóa K là:

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

▷ *Quá trình mã hóa:* Ba chữ cái đầu tiên trong P ứng với vector $(15, 0, 24)$ ta có:

$$\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} mod(26) = \begin{bmatrix} 11 \\ 13 \\ 18 \end{bmatrix} = LNS$$

Thực hiện tương tự ta có bản mã đầy đủ là *LNSHDLEWMTRW*

Phương pháp mã hóa đa ký tự - Mã Hill

▷ *Quá trình giải mã*: để giải mã ta cần sử dụng ma trận nghịch đảo của K là K^{-1}. Tức là $K^{-1}K \ mod \ 26 = \mathrm{I}$ - ma trận đơn vị.

Ma trận nghịch đảo của ma trận trên là:

$$K^{-1} = \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix}$$

vì:

$$\begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} = \begin{bmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{bmatrix} mod(26) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Khi đó bảng giải mã là: $K^{-1}C \ mod \ 26 = K^{-1}KP \ mod \ 26 = P$

Phương pháp mã hóa đa ký tự - Mã Hill

- Nhận xét:
  - Một cách tổng quát ta có thể lấy một ma trận vuông có kích thước $m \times m$ làm khóa.
  - Nếu một phần tử ở hàng i và cột j của K là k_{ij} thì ta có thể viết $K = (k_{ij})$, với $p = (p_1, p_2, ...p_m) \in P$ và $K \in$ K. Ta tính $c = e_K(p) = (c_1, c_2, ...c_m)$

    Một cách khác: $c = pK$
  - Ta thấy, bản mã nhận được từ bản rõ nhờ phép biến đổi tuyến tính
  - Cách giải mã, ta sẽ phải dùng ma trận nghịch đảo K^{-1} để giải mã. Cụ thể bằng công thức: cK^{-1}

Phương pháp mã hóa đa ký tự - Mã Hill

- Một số kiến thức cần thiết từ số học theo modulo:
  - *Phép đồng dư:* Giả sử a và b là các số nguyên và m là số nguyên dương. Ta viết $a \equiv b(mod\, m)$ nếu m chia hết cho $b - a$. Mệnh đề $a \equiv b(mod\, m)$ được gọi là a đồng dư với b theo modulo m. Số nguyên m được gọi là mudulus
  - *Không gian Z_m:* Một miền giá trị nguyên và không âm, chính là tập hợp $\{0, m-1\}$ có trang bị hai phép toán cộng và nhân, kí hiệu là Z_m

Phương pháp mã hóa đa ký tự - Mã Hill

- Thí dụ rút gọn theo modulo: tính 13×11 trong Z_{16}
  $11 \times 13 = 143 = 8 \times 16 + 15 => 143\ mod\ m = 15$ trong Z_{16}
- Một số tính chất của phép cộng và nhân trong Z_m:
  - Phép cộng là đóng, tức với $a, b \in Z_m$ thì $a + b \in Z_m$
  - Phép cộng có tính chất giao hoán, tức là $a + b = b + a$
  - Phép cộng có tính chất kết hợp, với $a, b, c \in Z_m$ ta có: $(a + b) + c = a + (b + c)$
  - 0 là phần tử đơn vị của phép cộng, tức là: $0 + a = a + 0 = a$
  - Phần tử nghịch đảo của phép cộng của phần tử a bất kỳ là $m - a$, tức là $a + (m - a) = (m - a) + a = 0$
  - Phép nhân là đóng, tức với $a, b \in Z_m$ thì $ab \in Z_m$

Phương pháp mã hóa đa ký tự - Mã Hill

- Phép nhân có tính chất giao hoán
- Phép nhân có tính chất kết hợp
- 1 là phần tử đơn vị của phép nhân, tức là với bất kỳ $a \in Z_m, a \times 1 = 1 \times a$
- Phép nhân có tính chất phân phối với phép cộng. Tức là, $a, b, c \in Z_m$ ta có: $a(b + c) = ab + ac, (a + b)c = ac + bc$

Phương pháp mã hóa đa ký tự - Mã Hill

- Một số kiến thức cần thiết từ đại số tuyến tính:
  - Nếu $A = (a_{i,j})$ là một ma trận cấp $1 \times m$ và $B = (b_{1,k})$ là một ma trận cấp $m \times n$ thì tích ma trận $AB = (c_{1,k})$ được xác định bằng công thức:

$$c_{1,k} = \sum_{j=1}^{m} a_{i,j} b_{j,k} \tag{1}$$

    Để ý: AB là ma trận cấp $1 \times n$
  - Phép nhân ma trận có tính chất kết hợp, tức là $(AB)C = A(BC)$ nhưng không có tính chất giao hoán.

Phương pháp mã hóa đa ký tự - Mã Hill

- Ma trận đơn vị kí hiệu là I_m có kích thước $m \times m$
- I_m là ma trận đơn vị vì $AI_m = A$ với mọi ma trận cấp $1 \times m$ và $I_m B = B$ với mọi ma trận cấp $m \times n$
- Ma trận nghịch đảo của ma trận A cấp $m \times m$ (nếu tồn tại) là ma trận A^{-1} sao cho $AA^{-1} = A^{-1}A = I_m$.

  Nếu ma trận A tồn tại ma trận nghịch đảo thì nó là duy nhất

Phương pháp mã hóa đa ký tự - Mã Hill

- Với các kiến thức trên ta có thể xây dựng công thức giải mã đã nêu.

  Vì $c = pK$ ta nhân hai vế với K^{-1} và được:

$$cK^{-1} = p(KK^{-1}) = pI_m = p$$

  (ta sử dụng tính chất kết hợp)

Phương pháp mã hóa đa ký tự - Mã Hill

- Thực tế, phép giải mã thực hiện được khi K là khả nghịch. Tính khả nghịch của ma trận vuông phụ thuộc vào định thức của nó. Ta có:

  Định nghĩa: Định thức của ma trận $A = (a_{i,j})$ cấp 2×2 là giá trị $det(A) = a_{11}a_{22} - a_{12}a_{21}$.

  Tính chất của định thức:

  - $det(I_m) = 1$
  - Quy tắc nhân $det(AB) = det(A) \times det(B)$

- Một ma trận thức K là có nghịch đảo khi và chỉ khi định thức của nó khác 0

Phương pháp mã hóa đa ký tự - Mã Hill

- Kết quả tương ứng là ma trận K có nghịch đảo theo modulo 26 khi và chỉ khi UCLN(det K,26) $= 1$.
- Theo công thức này, chỉ thích hợp với với m là nhỏ. Nếu m lớn ta xác định ma trận nghịch đảo phải dựa vào các phép toán hằng sơ cấp

One-Time Pad

- Mô tả:

▷ Với phương pháp mã hóa thay thế thì các từ trong khóa có thể bị lặp lại vì thế vẫn sẽ tạo ra một mối liên quan giữa bản rõ và bản mã => tận dụng phá mã.

▷ Vì thế, phải làm sao để bản rõ và bản mã thực sự là *ngẫu nhiên*. **Joseph Mauborgne**, giám đốc viện nghiên cứu mật mã của quân đội Mỹ đề xuất phương án dùng khóa ngẫu nhiên.

Khóa ngẫu nhiên có size bằng size của bản rõ và chỉ sử dụng một lần.

One-Time Pad

- Thí dụ: Cần mã hóa bản tin: *wearediscoveredsaveyourself*

Bản rõ P: *wearediscoveredsaveyourself*

Khóa K_1: *FHWYKLVMKVKXCVKDJSFSAPXZCVP*

Bản mã C: *BLWPOODEMJFBTZNVJNJQOJORGGU*

Tuy nhiên, giả sử ta giải mã với hai khóa K_2 và K_3 lần lượt như sau:

Trường hợp 1:	Bản mã C:	`BLWPOODEMJFBTZNVJNJQOJORGGU`
	Khóa K_2:	`IESRLKBWJFCIFZUCJLZXAXAAPSY`
	Bản giải mã:	`theydecidedtoattacktomorrow`
		(*they decided to attack tomorrow*)
Trường hợp 2:	Bản mã C:	`BLWPOODEMJFBTZNVJNJQOJORGGU`
	Khóa K_3:	`FHAHDDRAIQFIASJGJWQSVVBJAZB`
	Bản giải mã:	`wewillmeetatthepartytonight`
		(*we will meet at the party tonight*)

One-Time Pad

- Nhận xét:
  - Trong cả hai trường hợp trên thì bản giải mã đều có ý nghĩa. Có nghĩa phá mã thực hiện phá mã vét cạn thì sẽ tìm được nhiều khóa ứng với nhiều bản tin có ý nghĩa, do đó sẽ không biết được bản tin nào là bản rõ $=>$ rất an toàn
  - Phương pháp One-Time Pad là an toàn tuyệt đối thì mỗi khóa chỉ được sử dụng một lần
  - One-time pad không được dùng nhiều trong thực tế vì chiều dài khóa bằng với bản rõ.

Luyện tập

1. Giải mã bản mã sau, giả sử mã hóa Ceasar được sử dụng để mã hóa với $k = 3$: *IRXUVFRUHDQGVHYHQBHDUVDJR*
2. Mã hóa bản rõ sau: "enemy coming", dùng phương pháp mã hóa thay thế đơn bảng với khóa hoán vị K là: *IAUTMOCSNREBDLHVWYFPZJXKGQ*
3. Xét phương pháp Vigenere. Giả sử biết bản mã *"PVRLHFMJCRNFKKW"* có bản rõ tương ứng là "networksecurity". Hãy tìm khóa K
4. Mã hóa từ "explanation" bằng phương pháp Vigenere, từ khóa là LEG
5. Nghiên cứu thêm bài tập về mã hóa bằng phương pháp mã hóa Hill (về nhà)