



TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN ĐIỆN TỬ - VIỄN THÔNG

BỘ MÔN ĐIỆN TỬ HÀNG KHÔNG VŨ TRỤ


Môn học:

LÝ THUYẾT MẬT MÃ

Giảng viên: TS. Hán Trọng Thanh
Email: httbkhn@gmail.com

3/21/2016

1



Mục tiêu học phần

Cung cấp kiến thức cơ bản về mật mã đảm bảo an toàn và bảo mật thông tin:

- ✓ Các phương pháp mật mã khóa đối xứng; Phương pháp mật mã khóa công khai;
- ✓ Các hệ mật dòng và vấn đề tạo dãy giả ngẫu nhiên;
- ✓ Lược đồ chữ ký số Elgamal và chuẩn chữ ký số ECDSA;
- ✓ Độ phức tạp xử lý và độ phức tạp dữ liệu của một tấn công cụ thể vào hệ thống mật mã;
- ✓ Đặc trưng an toàn của phương thức mã hóa;
- ✓ Thăm mã tuyến tính, thăm mã vi sai và các vấn đề về xây dựng hệ mã bảo mật cho các ứng dụng.

2



Nội Dung

1. Chương 1. Tổng quan
2. Chương 2. Mật mã khóa đối xứng
3. Chương 3. Mật mã khóa công khai
4. Chương 4. Hàm băm và chữ ký số
5. Chương 5. Dây giả ngẫu nhiên và hệ mật dòng
6. Chương 6. Kỹ thuật quản lý khóa

3/21/2016

3



Tài liệu tham khảo

1. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press 1998.
2. B. Schneier, *Applied Cryptography*. John Wiley Press 1996.
3. M. R. A. Huth, *Secure Communicating Systems*, Cambridge University Press 2001.
4. W. Stallings, *Network Security Essentials, Applications and Standards*, Prentice Hall. 2000.

4



Nhiệm vụ của Sinh viên

1. Chấp hành nội quy lớp học
2. Thực hiện đầy đủ bài tập
3. Nắm vững ngôn ngữ lập trình Matlab




5



Chương 2. Mật mã khóa đối xứng

- 2.1. Giới thiệu sơ lược mật mã khóa đối xứng cổ điển
- 2.2. Một số hệ mật mã khóa đối xứng cổ điển
- 2.3. Sơ lược hệ mật mã dòng và hệ mật mã khối

6



2.1. Giới thiệu sơ lược hệ mật mã khóa đối xứng cổ điển

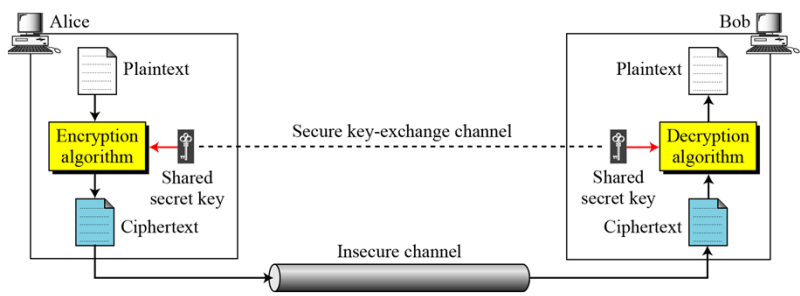




Figure shows the general idea behind a symmetric-key cipher. The original message from Alice to Bob is called plaintext; the message that is sent through the channel is called the ciphertext. To create the ciphertext from the plaintext, Alice uses an encryption algorithm and a shared secret key. To create the plaintext from ciphertext, Bob uses a decryption algorithm and the same secret key.

7



2.1. Giới thiệu sơ lược hệ mật mã khóa đối xứng cổ điển

- Based on **Kirchhoff's** principle, one should always assume that the adversary, Eve, knows the encryption/decryption algorithm. The resistance of the cipher to attack **must be based only on the secrecy of the key**.



Locking and unlocking with the same key

8



2.2. Một số hệ mật mã khóa đối xứng cổ điển

2.2.1. Hệ mật mã khóa đối xứng thay thế

- Đây là hệ mật mã thay thế một ký tự này thành một ký tự khác.
- Phân loại:
 - Mật mã thay thế đơn ký tự - monoalphabetic
 - Mật mã thay thế đa ký tự - polyalphabetic

A substitution cipher replaces one symbol with another.

9



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

In monoalphabetic substitution, the relationship between a symbol in the plaintext to a symbol in the cipher text is always one-to-one.

10



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

- The simplest monoalphabetic cipher is the **additive cipher**. This cipher is sometimes called a **shift cipher** and sometimes a **Caesar cipher**, but the term additive cipher better reveals its mathematical nature.

Plaintext →	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
Ciphertext →	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
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

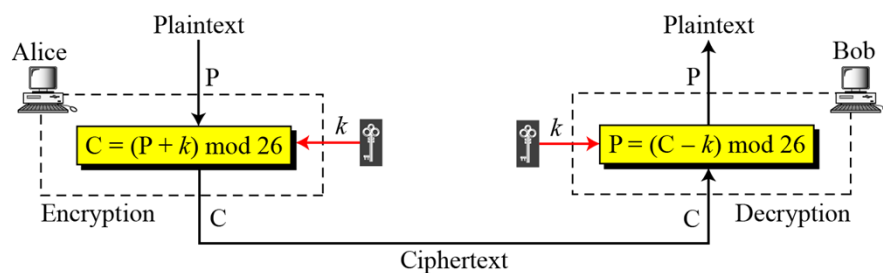
Plaintext and ciphertext in Z_{26}

11




2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic



12



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

- Ví dụ 1:** Hãy sử dụng mã cộng để mã hóa chữ **hello** với khóa $K = 15$.


Plaintext: hello

➔
Additive cipher

Ciphertext: WTAAD

Plaintext: h → 07	Encryption: $(07 + 15) \bmod 26$	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: $(04 + 15) \bmod 26$	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: $(11 + 15) \bmod 26$	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: $(11 + 15) \bmod 26$	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: $(14 + 15) \bmod 26$	Ciphertext: 03 → D

13



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

- Ví dụ 2:** Hãy sử dụng mã cộng để giải mã chữ **WTAAD** với khóa $K = 15$.

Plaintext: WTAAD

➔
Additive cipher

Ciphertext: hello

Ciphertext: W → 22	Decryption: $(22 - 15) \bmod 26$	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: $(19 - 15) \bmod 26$	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: $(00 - 15) \bmod 26$	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: $(00 - 15) \bmod 26$	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: $(03 - 15) \bmod 26$	Plaintext: 14 → o

14



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

- Historically, additive ciphers are called **shift ciphers**. Julius Caesar used an additive cipher to communicate with his officers. For this reason, additive ciphers are sometimes referred to as the **Caesar cipher**. Caesar used a key of 3 for his communications.

Additive ciphers are sometimes referred to as shift ciphers or Caesar cipher.

15



2.2. Một số hệ mật mã khóa đối xứng cổ điển


a. Hệ mật thay thế đơn ký tự - monoalphabetic

- Ví dụ 3:** Hacker lấy được đoạn mã “UVACLYFZLJBYL”, khi đó anh ta làm thế nào để giải mã được đoạn mã đó??
- He tries keys from 1 to 25. With a key of 7, the plaintext is “not very secure”, which makes sense

Ciphertext: UVACLYFZLJBYL

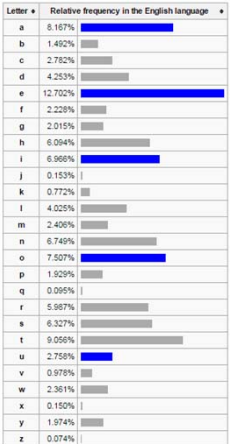
K = 1	→	Plaintext: tuzbkxeykiaxk
K = 2	→	Plaintext: styajwdxjhzwj
K = 3	→	Plaintext: rsxzivcwigyvi
K = 4	→	Plaintext: qrwyhubvhfxuh
K = 5	→	Plaintext: pqvxgtaugewtg
K = 6	→	Plaintext: opuwfsztfdvsv
K = 7	→	Plaintext: notverysecure

16



2.2. Một số hệ mật mã khóa đối xứng cổ điển


a. Hệ mật thay thế đơn ký tự - monoalphabetic



Letter	Frequency	Letter	Frequency	Letter	Frequency	Letter	Frequency
E	12.7	H	6.1	W	2.3	K	0.08
T	9.1	R	6.0	F	2.2	J	0.02
A	8.2	D	4.3	G	2.0	Q	0.01
O	7.5	L	4.0	Y	2.0	X	0.01
I	7.0	C	2.8	P	1.9	Z	0.01
N	6.7	U	2.8	B	1.5		
S	6.3	M	2.4	V	1.0		

Digram	TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, OF
Trigram	THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR, DTH

17



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic


- Ví dụ:** Hacker lấy được đoạn mã

XLILSYWIMWRSJASVWEPIJSVJSYVQMPPMSRHSPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPVIVIGIMZIWQSVISJJIVW

- Số lần xuất hiện chữ cái I = 14 là nhiều nhất, do đó I tương ứng với chữ e tức là đã dịch đi 4 đơn vị hay K = 4, từ đó ta có

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers

18

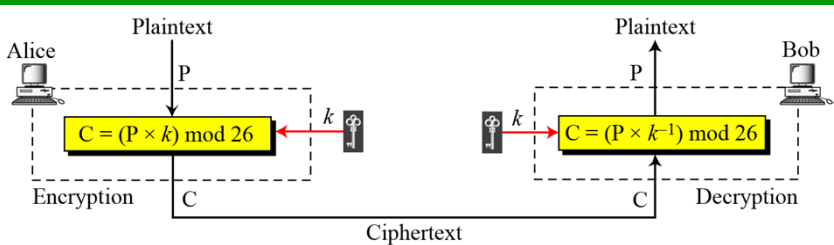


2.2. Một số hệ mật mã khóa đối xứng cổ điển


a. Hệ mật thay thế đơn ký tự - monoalphabetic

Multiplicative Ciphers

In a multiplicative cipher, the plaintext and ciphertext are integers in Z_{26} ; the key is an integer in Z_{26}^* .



19



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

- Ví dụ 4:** What is the key domain for any multiplicative cipher?

Tập các thặng dư thu gọn theo $mod\ n$ được định nghĩa là tập $Z_n^* = \{a \in Z_n: \gcd(a, n) = 1\}$, tức Z_n^* là tập con của Z_n bao gồm tất cả các phần tử nguyên tố với n

The key needs to be in Z_{26}^* . This set has only 12 members: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

20



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

Ví dụ 5: Hãy sử dụng mã nhân để giải mã hóa chữ “hello” với $K = 7$?

Plaintext: h $\rightarrow 07$	Encryption: $(07 \times 07) \bmod 26$	ciphertext: 23 $\rightarrow X$
Plaintext: e $\rightarrow 04$	Encryption: $(04 \times 07) \bmod 26$	ciphertext: 02 $\rightarrow C$
Plaintext: l $\rightarrow 11$	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow Z$
Plaintext: l $\rightarrow 11$	Encryption: $(11 \times 07) \bmod 26$	ciphertext: 25 $\rightarrow Z$
Plaintext: o $\rightarrow 14$	Encryption: $(14 \times 07) \bmod 26$	ciphertext: 20 $\rightarrow U$

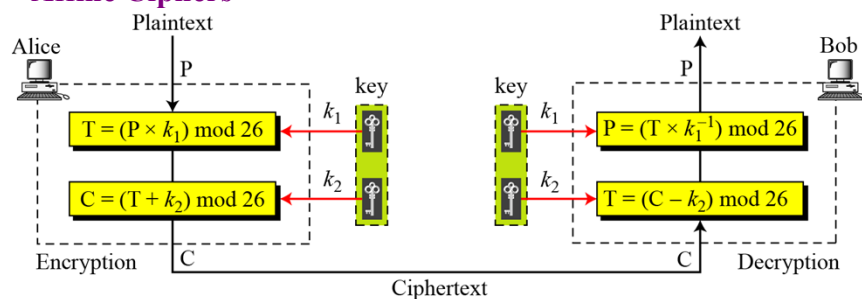
21



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

Affine Ciphers



$$C = (P \times k_1 + k_2) \bmod 26$$

$$P = ((C - k_2) \times k_1^{-1}) \bmod 26$$

where k_1^{-1} is the multiplicative inverse of k_1 and $-k_2$ is the additive inverse of k_2

22



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - *monoalphabetic* Affine Ciphers

The affine cipher uses a pair of keys in which the first key is from Z_{26}^* and the second is from Z_{26} . What is the size of the key domain?

The size of the key domain is $26 \times 12 = 312$.



23



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - *monoalphabetic*

Ví dụ 6: Hãy sử dụng mã Affine để mã hóa chữ “hello” với $K = (7, 2)$?

P: h \rightarrow 07	Encryption: $(07 \times 7 + 2) \bmod 26$	C: 25 \rightarrow Z
P: e \rightarrow 04	Encryption: $(04 \times 7 + 2) \bmod 26$	C: 04 \rightarrow E
P: l \rightarrow 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 \rightarrow B
P: l \rightarrow 11	Encryption: $(11 \times 7 + 2) \bmod 26$	C: 01 \rightarrow B
P: o \rightarrow 14	Encryption: $(14 \times 7 + 2) \bmod 26$	C: 22 \rightarrow W

24



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - *monoalphabetic*

Ví dụ 7: Hãy sử dụng mã Affine để giải mã hóa chữ “ZEBBW” với $K = (7, 2)$?

C: Z \rightarrow 25	Decryption: $((25 - 2) \times 7^{-1}) \bmod 26$	P: 07 \rightarrow h
C: E \rightarrow 04	Decryption: $((04 - 2) \times 7^{-1}) \bmod 26$	P: 04 \rightarrow e
C: B \rightarrow 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P: 11 \rightarrow l
C: B \rightarrow 01	Decryption: $((01 - 2) \times 7^{-1}) \bmod 26$	P: 11 \rightarrow l
C: W \rightarrow 22	Decryption: $((22 - 2) \times 7^{-1}) \bmod 26$	P: 14 \rightarrow o

25



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - *monoalphabetic*


Hãy so sánh Affine Cipher với Additive Cipher?

The additive cipher is a special case of an affine cipher in which $k_1 = 1$.

Hãy so sánh Affine Cipher với multiplicative Cipher?

The multiplicative cipher is a special case of affine cipher in which $k_2 = 0$.

26



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic


Monoalphabetic Substitution Cipher

Because additive, multiplicative, and affine ciphers have small key domains, they are very vulnerable to brute-force attack.

A better solution is to create a mapping between each plaintext character and the corresponding ciphertext character. Alice and Bob can agree on a table showing the mapping for each character.

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

27




2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật thay thế đơn ký tự - monoalphabetic

Monoalphabetic Substitution Cipher

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

this message is easy to encrypt but hard to find the key



ICFVQRVVNEFVRNVSIYRGASLJOJCNHTIYBFGTICRXRS

28



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic

In polyalphabetic substitution, each occurrence of a character may have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is one-to-many.

Autokey Cipher

$$P = P_1 P_2 P_3 \dots$$

$$C = C_1 C_2 C_3 \dots$$

$$k = (k_1, P_1, P_2, \dots)$$

$$\text{Encryption: } C_i = (P_i + k_i) \bmod 26$$

$$\text{Decryption: } P_i = (C_i - k_i) \bmod 26$$

29



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic

Assume that Alice and Bob agreed to use an autokey cipher with initial key value $k_1 = 12$. Now Alice wants to send Bob the message “Attack is today”. Enciphering is done character by character.

Plaintext:	a	t	t	a	c	k	i	s	t	o	d	a	y
P's Values:	00	19	19	00	02	10	08	18	19	14	03	00	24
Key stream:	12	00	19	19	00	02	10	08	18	19	14	03	00
C's Values:	12	19	12	19	02	12	18	00	11	7	17	03	24
Ciphertext:	M	T	M	T	C	M	S	A	L	H	R	D	Y

30



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic *Vigenere Cipher*

$$P = P_1P_2P_3 \dots \quad C = C_1C_2C_3 \dots \quad K = [(k_1, k_2, \dots, k_m), (k_1, k_2, \dots, k_m), \dots]$$

$$\text{Encryption: } C_i = P_i + k_i$$

$$\text{Decryption: } P_i = C_i - k_i$$

We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	15	00	18	02	00	11	15	00	18	02	00	11	15	00
C's values:	07	07	22	10	18	22	23	18	11	6	13	19	02	06
Ciphertext:	H	H	W	K	S	W	X	S	L	G	N	T	C	G

31



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic *Vigenere Cipher*

We can encrypt the message “She is listening” using the 6-character keyword “PASCAL”.

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	15	00	18	02	00	11	15	00	18	02	00	11	15	00
C's values:	07	07	22	10	18	22	23	18	11	6	13	19	02	06
Ciphertext:	H	H	W	K	S	W	X	S	L	G	N	T	C	G

The initial key stream is (15, 0, 18, 2, 0, 11)

32

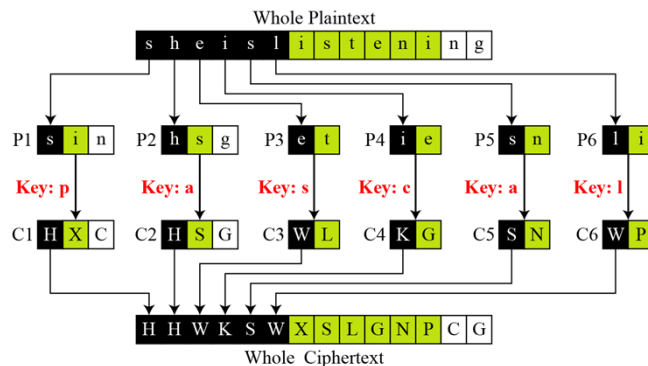


2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic

Hãy so sánh Vigenere cipher với Additive Cipher?

A Vigenere cipher as a combination of m additive ciphers



33



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic

Hãy so sánh Vigenere cipher với Additive Cipher?

Ngược lại: the additive cipher is a special case of Vigenere cipher in which $m = 1$.

	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

34



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic Thám mã Vigenere Cipher

Giả sử hacker nhận được bản tin mật sau:

LIOMWGFEGGDVWGHHCQUCRHRWAGWIOWQLKGZETKKMEVLWPCZVGTH-
VTSGXQOVGCSVETQLTJSUMVWVEUVLXEWSLGFZMVVWLGYHCUSWXQH-
KVGSHEEVFLCFDGVSUMPHKIRZDMPHHBVVWVJWIXGFWLTSHGJOUEEHH-
VUCFVGOWICQLTJSUXGLW

Làm thế nào để
giải mã????

Theo phương pháp Kasiski, từng cụm 3 chữ liên tiếp được khảo sát trong cả đoạn để tìm khoảng cách ngắn nhất mà cụm đó xuất hiện lặp lại

35



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic Thám mã Vigenere Cipher

Giả sử hacker nhận được bản tin mật sau:

Theo phương pháp Kasiski, từng cụm 3 chữ liên tiếp được khảo sát trong cả đoạn để tìm khoảng cách ngắn nhất mà cụm đó xuất hiện lặp lại

String	First Index	Second Index	Difference
JSU	68	168	100
SUM	69	117	48
VWV	72	132	60
MPH	119	127	8

36



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic Thám mã Vigenere Cipher

The greatest common divisor of differences is 4, which means that the key length is multiple of 4. First try $m = 4$.

37



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic Hill Cipher

Key in the Hill cipher

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

$$\begin{aligned} C_1 &= P_1 k_{11} + P_2 k_{21} + \dots + P_m k_{m1} \\ C_2 &= P_1 k_{12} + P_2 k_{22} + \dots + P_m k_{m2} \\ &\dots \\ C_m &= P_1 k_{1m} + P_2 k_{2m} + \dots + P_m k_{mm} \end{aligned}$$

The key matrix in the Hill cipher needs to have a multiplicative inverse.

38



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic Hill Cipher

Ví dụ 9: Hãy mã hóa bản tin “code is ready” bằng hệ mật Hill với khóa K

$$K = \begin{bmatrix} 09 & 07 & 11 & 13 \\ 04 & 07 & 05 & 06 \\ 02 & 21 & 14 & 09 \\ 03 & 23 & 21 & 08 \end{bmatrix}$$

39



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic Hill Cipher

$$P = \begin{bmatrix} 02 & 14 & 03 & 04 \\ 08 & 18 & 17 & 04 \\ 00 & 03 & 24 & 25 \end{bmatrix} = \begin{bmatrix} 14 & 07 & 10 & 13 \\ 08 & 07 & 06 & 11 \\ 11 & 08 & 18 & 18 \end{bmatrix} K^{-1} = \begin{bmatrix} 02 & 15 & 22 & 03 \\ 15 & 00 & 19 & 03 \\ 09 & 09 & 03 & 11 \\ 17 & 00 & 04 & 07 \end{bmatrix}$$

40



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic *Thám mã hệ mật Hill*

- Việc thám mã hệ mật Hill bằng cách dò lần lượt các từ khóa là dường như không thực hiện được.
- Hệ mật này gần như chỉ có thể bị phá được khi biết được giá trị m và các cặp chữ tương ứng giữa bản mật và bản rõ.
- Ví dụ: với $m = 3$

$$\begin{bmatrix} 05 & 07 & 10 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 03 & 06 & 00 \end{bmatrix}$$

$$\begin{bmatrix} 13 & 17 & 07 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 14 & 16 & 09 \end{bmatrix}$$

$$\begin{bmatrix} 00 & 05 & 04 \end{bmatrix} \longleftrightarrow \begin{bmatrix} 03 & 17 & 11 \end{bmatrix}$$

P C

41



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật thay thế đa ký tự - Polyalphabetic *Thám mã hệ mật Hill*

- Do P là ma trận khả nghịch, nên người thám mã sẽ tìm ma trận P^{-1} , rồi tìm khóa K

$$\begin{bmatrix} 02 & 03 & 07 \\ 05 & 07 & 09 \\ 01 & 02 & 11 \end{bmatrix} = \begin{bmatrix} 21 & 14 & 01 \\ 00 & 08 & 25 \\ 13 & 03 & 08 \end{bmatrix} \begin{bmatrix} 03 & 06 & 00 \\ 14 & 16 & 09 \\ 03 & 17 & 11 \end{bmatrix}$$

K P^{-1} C

Từ đó, người thám mã sẽ phá được tất cả các bản mật sử dụng khóa K nói trên

42



2.2. Một số hệ mật mã khóa đối xứng cổ điển

2.2.2. Hệ mật mã khóa đối xứng dịch chuyển vị trí – Transposition Ciphers

A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.

A transposition cipher reorders symbols.

- a. Hệ mật dịch chuyển không khóa - Keyless Transposition Ciphers
- b. Hệ mật dịch chuyển có khóa - Keyed Transposition Ciphers
- c. Hệ mật dịch chuyển kết hợp - Combination of Two Approaches

43




2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật dịch chuyển không khóa

- Đây là hệ mật mã cổ điển đơn giản, được sử dụng từ lâu.
- Hệ mật mã dựa trên sự hoán vị của các ký tự trong bản rõ để có được bản mật.
- Có 2 phương pháp:
 - Chia cột – ghép hàng
 - Chia hàng – ghép cột

44




2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật dịch chuyển không khóa

- A good example of a keyless cipher using the first method is the *rail fence cipher*.
- The plaintext is arranged in 2 lines as a zigzag pattern.
- The ciphertext is created by reading the pattern row by row.

45



2.2. Một số hệ mật mã khóa đối xứng cổ điển

a. Hệ mật dịch chuyển không khóa

- Alice and Bob can agree on the number of columns and use the second method.
- Alice writes the same plaintext, row by row, in a table of four columns.

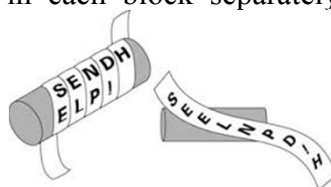
46



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật dịch chuyển có khóa

- The keyless ciphers permute the characters by using writing plaintext in one way and reading it in another way.
- The permutation is done on the whole plaintext to create the whole ciphertext.
- Another method is to divide the plaintext into groups of predetermined size, called blocks, and then use a key to permute the characters in each block separately. => **Keyed transposition ciphers**



47



2.2. Một số hệ mật mã khóa đối xứng cổ điển

b. Hệ mật dịch chuyển có khóa

Alice needs to send the message “Enemy attacks tonight” to Bob.

The key used for encryption and decryption is a permutation key.

e n e m y a t t a c k s t o n i g h t z

Key

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

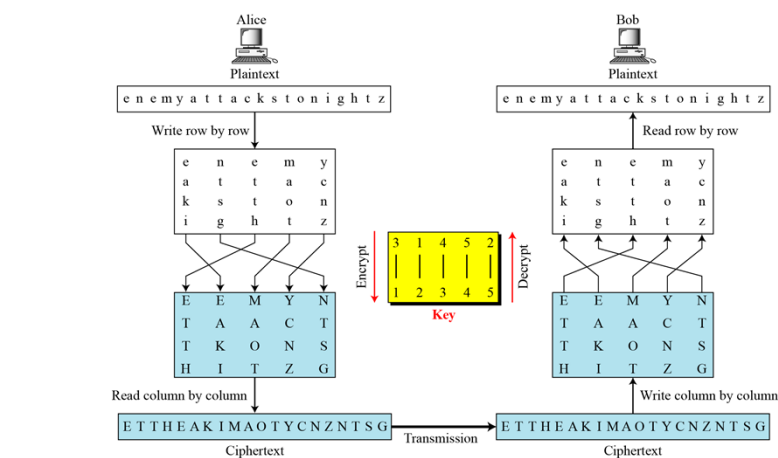
E E M Y N T A A C T T K O N S H I T Z G

48



2.2. Một số hệ mật mã khóa đối xứng cổ điển

c. Hệ mật dịch chuyển kết hợp

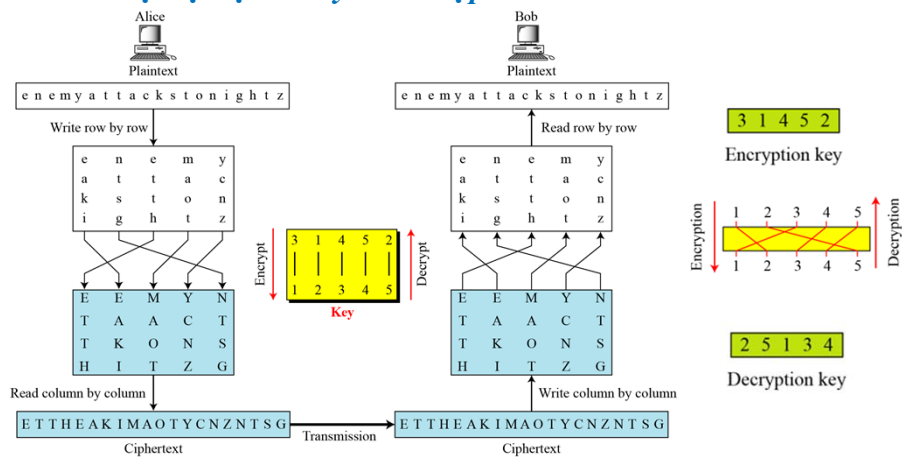


49



2.2. Một số hệ mật mã khóa đối xứng cổ điển

c. Hệ mật dịch chuyển kết hợp



50



2.2. Một số hệ mật mã khóa đối xứng cổ điển

Biểu diễn hệ mật dịch chuyển bằng ma trận

$$\begin{bmatrix} 04 & 13 & 04 & 12 & 24 \\ 00 & 19 & 19 & 00 & 02 \\ 10 & 18 & 19 & 14 & 13 \\ 08 & 06 & 07 & 19 & 25 \end{bmatrix} \times \begin{bmatrix} 3 & 1 & 4 & 5 & 2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 04 & 04 & 12 & 24 & 13 \\ 19 & 00 & 00 & 02 & 19 \\ 19 & 10 & 14 & 13 & 18 \\ 07 & 08 & 19 & 25 & 06 \end{bmatrix}$$

Plaintext Encryption key Ciphertext

51




2.3. Sơ lược hệ mật mã dòng và mã khối

- Các hệ mật mã khóa đối xứng có thể được phân loại thành 2 loại hệ mật: Hệ mật mã dòng và hệ mật mã khối



52



2.3. Sơ lược hệ mật mã dòng và mã khối

2.3.1. Hệ mật mã dòng

Với bản rõ dòng P, bản mật dòng C và khóa dòng K, ta có:

$$P = P_1P_2P_3, \dots \quad C = C_1C_2C_3, \dots \quad K = (k_1, k_2, k_3, \dots)$$

$$C_1 = E_{k_1}(P_1) \quad C_2 = E_{k_2}(P_2) \quad C_3 = E_{k_3}(P_3) \dots$$

Ví dụ

Plaintext
p l a i n


$K = (k_1, k_2, k_3, k_4, k_5)$

Ciphertext
S O

$D = E_{k_3}(a)$

Encryption algorithm

53




2.3. Sơ lược hệ mật mã dòng và mã khối

2.3.1. Hệ mật mã dòng


Hệ mật mã cộng có phải là hệ mật dòng hay không?

Hệ mật mã thay thế đơn ký tự có phải là hệ mật dòng hay không?

54



ĐẠI HỌC
BÁCH KHOA

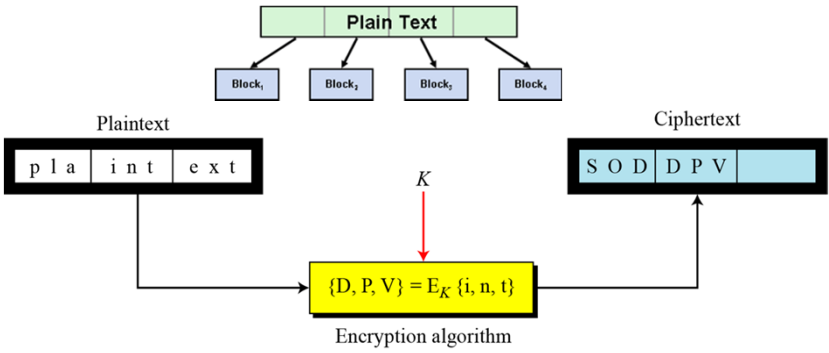


S E T


2.3. Sơ lược hệ mật mã dòng và mã khối

2.3.2. Hệ mật mã khối


A group of plaintext symbols of size m ($m > 1$) are encrypted together creating a group of ciphertext of the same size



55



ĐẠI HỌC
BÁCH KHOA



S E T

2.3. Sơ lược hệ mật mã dòng và mã khối

2.3.2. Hệ mật mã khối

- Hill ciphers are block ciphers.
- A block of plaintext, of size 2 or more is encrypted together using a single key (a matrix).
- In these ciphers, the value of each character in the ciphertext depends on all the values of the characters in the plaintext.
- The key is made of $m \times m$ values, it is considered as a single key.

56



2.3. Sơ lược hệ mật mã dòng và mã khối

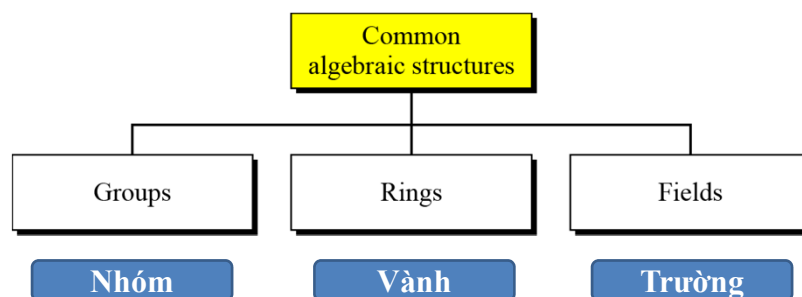
2.3.1. Hệ mật mã khối

- In practice, blocks of plaintext are encrypted individually, but they use a stream of keys to encrypt the whole message block by block.
- In other words, the cipher is a block cipher when looking at the individual blocks, but it is a stream cipher when looking at the whole message considering each block as a single unit.

57



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại



58



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

- A group (G) is a set of elements with a binary operation (\bullet) that satisfies four properties:
 - Closure
 - Associativity
 - Existence of identity
 - Existence of inverse

59



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

- A commutative group satisfies an extra property, commutatively or *abelian* group
 - Closure
 - Commutativity
 - Associativity
 - Existence of identity
 - Existence of inverse

60



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

- A commutative group satisfies an extra property, commutatively or **abelian** group
 - Closure: $a, b \in G$ thì $c = a (\cdot) b \in G$
 - Commutatively: $a (\cdot) b = b (\cdot) a$
 - Associativity: $c (\cdot) (a (\cdot) b) = (c (\cdot) a) (\cdot) b$
 - Existence of identity: $a \cdot e = e \cdot a = a$
 - Existence of inverse: $a \cdot a' = a' \cdot a = e$

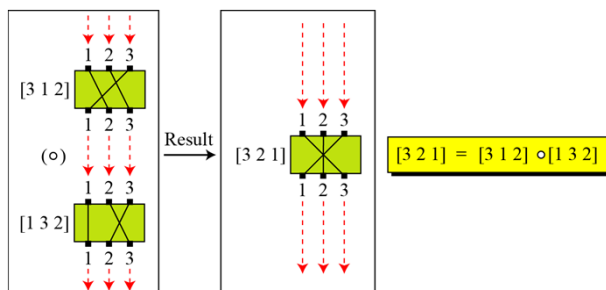
61



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

- A very interesting group is the permutation group. The set is the set of all permutations, and the operation is composition: applying one permutation after another.



62



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

- A very interesting group is the permutation group. The set is the set of all permutations, and the operation is composition: applying one permutation after another.

\circ	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

63



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

• Finite Group

Nhóm hữu hạn là nhóm có số hữu hạn các phần tử

• Order of a Group

Cấp của nhóm là số phần tử của nhóm đó

• Subgroup

Nhóm con của một nhóm G là nhóm bao gồm các phần tử thuộc G đồng thời thỏa mãn phép toán đóng trong G

64



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

• Tính chất của subgroup

1. If a and b are members of both groups, then $c = a \bullet b$ is also a member of both groups.
2. The group share the same identity element.
3. If a is a member of both groups, the inverse of a is also a member of both groups.
4. The group made of the identity element of G , $H = \{e\}$, is a subgroup of G .
5. Each group is a subgroup of itself.

65



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại


2.4.1. Nhóm

Cyclic Subgroups

- Nhóm con Cyclic là nhóm được tạo ra bởi cấp số của 1 phần tử nhóm gốc
- Cấp số của phần tử là số lần thực hiện lặp lại phép toán đối với phần tử đó

$$a^n \rightarrow a \bullet a \bullet \dots \bullet a \quad (n \text{ times})$$

66




2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm

Cyclic Group

- Nhóm G là nhóm Cyclic khi G chính là nhóm con Cyclic $\{e, g, g^2, \dots, g^{n-1}\}$, where $g^n = e$

67



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.1. Nhóm


Lagrange's Theorem

Assume that G is a group, and H is a subgroup of G . If the order of G and H are $|G|$ and $|H|$, respectively, then, based on this theorem, $|H|$ divides $|G|$.

Order of an Element

The order of an element, $\text{ord}(a)$, is the smallest integer that $a^n = e$.

68



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.2. Vành

A ring, $R = \langle \{...\}, \bullet, \blacksquare \rangle$, is an algebraic structure with two operations.

1. Closure
 2. Associativity
 3. Commutativity
 4. Existence of identity
 5. Existence of inverse

1. Closure
 2. Associativity

1. Closure
 2. Associativity
 3. Commutativity


Note:
 The third property is
 only satisfied for a
 commutative ring.

The second operation must be distributed over the first

$$a \blacksquare (b \circ c) = (a \blacksquare b) \circ (a \blacksquare c)$$

$$(a \circ b) \blacksquare c = (a \blacksquare c) \circ (b \blacksquare c)$$

69



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.2. Vành

The second operation must be distributed over the first

$$a \blacksquare (b \circ c) = (a \blacksquare b) \circ (a \blacksquare c)$$

$$(a \circ b) \blacksquare c = (a \blacksquare c) \circ (b \blacksquare c)$$

The set Z with two operations, addition and multiplication, is a commutative ring. We show it by $R = \langle Z, +, \times \rangle$. Addition satisfies all of the five properties; multiplication satisfies only three properties.

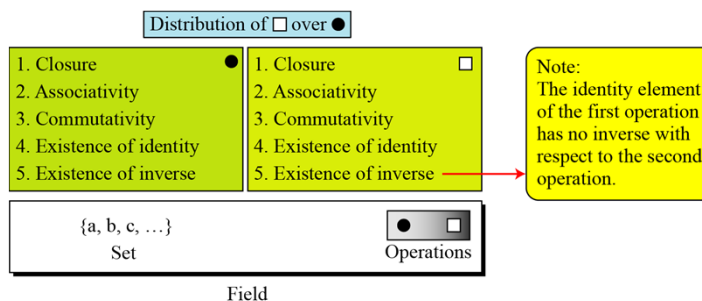
70



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường

A field, denoted by $F = \langle \{...\}, \bullet, \blacksquare \rangle$ is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation has no inverse.



71



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường

- A finite field, a field with a finite number of elements, are very important structures in cryptography.
- Galois showed that for a field to be finite, the number of elements should be p^n , where p is a prime and n is a positive integer.

A Galois field, $GF(p^n)$, is a finite field with p^n elements.

72



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường

A Galois field, $GF(p^n)$, is a finite field with p^n elements.

When $n = 1$, we have $GF(p)$ field. This field can be the set Z_p , $\{0, 1, \dots, p-1\}$, with two arithmetic operations.

A very common field in this category is $GF(2)$ with the set $\{0, 1\}$ and two operations, addition and multiplication.

GF(2)					
<div><div><div>{0, 1}</div><div><div>+</div><div>×</div></div></div></div>					
					</



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$

Let us define a $GF(2^2)$ field in which the set has **four 2-bit words**: {00, 01, 10, 11}. We can **redefine addition** and **multiplication** for this field in such a way that all properties of these operations are satisfied.

Addition						Multiplication					
\oplus	00	01	10	11		\otimes	00	01	10	11	
00	00	01	10	11		00	00	00	00	00	
01	01	00	11	10		01	00	01	10	11	
10	10	11	00	01		10	00	10	11	01	
11	11	10	01	00		11	00	11	01	10	
Identity: 00						Identity: 01					

An example of $GF(2^2)$ field

75



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Polynomials

A **polynomial** of **degree $n - 1$** is an expression of the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x^1 + a_0x^0$$

where x^i is called the **i^{th} term** and a_i is called **coefficient** of the i^{th} term.

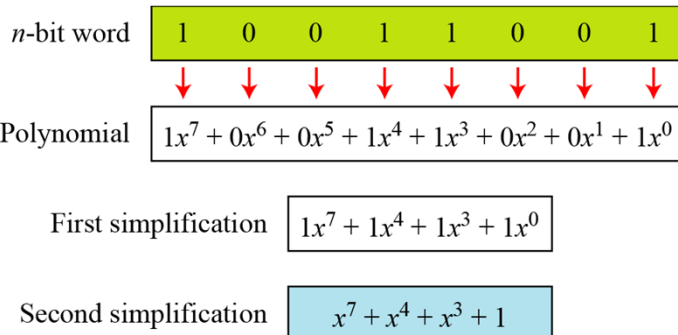
76



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Polynomials

How we can represent the 8-bit word (10011001) using a polynomials?



77



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Polynomials

To find the 8-bit word related to the polynomial $x^5 + x^2 + x$, we first supply the omitted terms. Since $n = 8$, it means the polynomial is of degree 7.

The expanded polynomial is

$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$

This is related to the 8-bit word **00100110**.

78



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Polynomials

Lưu ý:

**Polynomials representing n -bit words
use two fields: $GF(2)$ and $GF(2^n)$**

79



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Modulus

For the sets of **polynomials in $GF(2^n)$** , a **group of polynomials of degree n** is defined as the **modulus**. Such polynomials are referred to as **irreducible polynomials**.

Degree	Irreducible Polynomials
1	$(x + 1), (x)$
2	$(x^2 + x + 1)$
3	$(x^3 + x^2 + 1), (x^3 + x + 1)$
4	$(x^4 + x^3 + x^2 + x + 1), (x^4 + x^3 + 1), (x^4 + x + 1)$
5	$(x^5 + x^2 + 1), (x^5 + x^3 + x^2 + x + 1), (x^5 + x^4 + x^3 + x + 1),$ $(x^5 + x^4 + x^3 + x^2 + 1), (x^5 + x^4 + x^2 + x + 1)$

80



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Modulus

Lưu ý:

Addition and subtraction operations on polynomials are the same operation.

81



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Modulus

Let us do $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$. We use the symbol \oplus to show that we mean **polynomial addition**.

The following shows the procedure:

$$\begin{array}{rcl}
 0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 & \oplus & \\
 0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 & & \\
 \hline
 0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 & \rightarrow & x^5 + x^3 + x + 1
 \end{array}$$

82



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Modulus

There is also another short cut. Because the **addition in $GF(2)$** means the **exclusive-or (XOR) operation**. So **we can exclusive-or the two words, bits by bits, to get the result**. In the previous example, $x^5 + x^2 + x$ is **00100110** and $x^3 + x^2 + 1$ is **00001101**. The result is **00101011** or in polynomial notation **$x^5 + x^3 + x + 1$** .

83



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Multiplication

1. The **coefficient multiplication** is **done in $GF(2)$** .
2. The multiplying x^i by x^j results in x^{i+j}
3. The multiplication may create terms with **degree more than $n - 1$** , which means the result **needs to be reduced using a modulus polynomial**.

84



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Generator

Sometimes it is easier to define the elements of the $GF(2^n)$ field using a generator.

$$\{0, g, g^2, \dots, g^N\}, \text{ where } N = 2^n - 2$$

85



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Generator

Generate the elements of the field $GF(2^4)$ using the irreducible polynomial $f(x) = x^4 + x + 1$.

86



2.4. Cơ sở toán học cho hệ mật mã khóa đối xứng hiện đại

2.4.3. Trường $GF(2^n)$ Summary

The finite field $GF(2^n)$ can be used to define four operations of addition, subtraction, multiplication and division over n -bit words. The only restriction is that division by zero is not defined.