



BÀI GIẢNG

CƠ SỞ MẬT MÃ HỌC

Giảng viên: TS. Ngô Đức Thiện

E-mail: thienptit@gmail.com

Bộ môn: Xử lý tín hiệu và truyền thông

Khoa: KTDT1

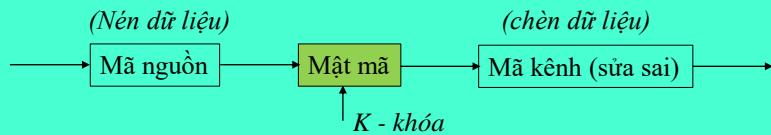
Cơ sở mật mã học

Tài liệu tham khảo

1. Giáo trình: “*Cơ sở mật mã học*” – GS.TS. Nguyễn Bình
2. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone.
Handbook of applied cryptography. CRC Press 1998.
3. B. Schneier. *Applied Cryptography*. John Wiley Press 1996.
4. D. R. Stinson. *Cryptography. Theory and Practice*. CRC Press 1995

Các định nghĩa và khái niệm cơ bản

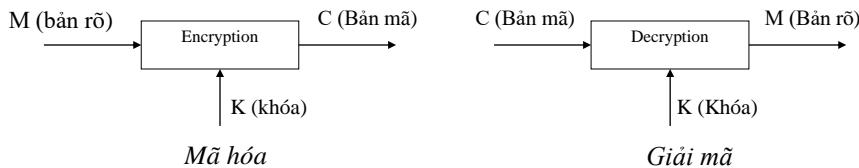
- Các khối mã hóa trong hệ thống số



- Trong mã nguồn và mã kênh gọi **mã hóa** là: Coding



- Trong mật mã học gọi **mã hóa** là: Encryption



Các định nghĩa và khái niệm cơ bản

- **Định nghĩa Mật mã:**

Mật mã là việc nghiên cứu các kỹ thuật toán học liên quan đến các khía cạnh an toàn thông tin như **bảo mật, toàn vẹn dữ liệu, xác thực...**

- **Mục tiêu của mật mã**

1. **Bảo mật (Confidentiality):** là một dịch vụ nhằm bảo vệ thông tin cho những các bên có thẩm quyền. **Bí mật** là thuật ngữ đồng nghĩa với bảo mật và quyền riêng tư. Có nhiều cách để thực hiện bảo mật, từ bảo vệ vật lý đến các thuật toán làm cho dữ liệu trở nên không hiểu được.

2. **Toàn vẹn dữ liệu (Data integrity):** là dịch vụ xử lý các thay đổi trái phép dữ liệu. Để đảm bảo tính toàn vẹn, phải phát hiện được các thay đổi lên dữ liệu của các đối tượng không có thẩm quyền. Thay đổi dữ liệu có thể là chèn, xóa và thay thế.

Các định nghĩa và khái niệm cơ bản

• Mục tiêu của mật mã

3. **Xác thực (Authentication):** là dịch vụ liên quan đến nhận dạng. Chức năng này liên quan đến cả chủ thể nội dung và nội dung. Hai bên liên lạc cần phải có cơ chế nhận dạng nhau. Nội dung gửi trên kênh liên lạc phải được xác thực về nguồn gốc, ngày phát hành, nội dung, thời gian gửi... Vì các lý do này, mà mật mã thường chia thành 2 loại xác thực chính là: **xác thực chủ thể nội dung và xác thực nguyên bản của nội dung.** Xác thực tính nguyên ban liên quan đến tính toàn vẹn của dữ liệu.
4. **Không thể chối bỏ (Non-repudiation):** là dịch vụ ngăn chặn các chủ thể từ chối cam kết hoặc các hoạt động trước đó. Điều này là cần thiết khi xảy ra tranh chấp nếu một bên chối bỏ các hoạt động trước đó. Ví dụ một bên ủy quyền cho mua tài sản cho một bên khác sau đó lại phủ nhận sự ủy quyền này. Khi đó cần có một thủ tục liên quan đến bên thứ 3 đáng tin cậy để giải quyết các tranh chấp này.

Các định nghĩa và khái niệm cơ bản

- Môn học là một bộ phận của khoa học mật mã (Cryptology), được chia thành 2 bộ phận chính:

- + **Mật mã học (Cryptography):** chia thành 3 nội dung:
 - Mật mã khóa bí mật (Khóa đối xứng)
 - Mật mã khóa công khai (khóa bất đối xứng)
 - Hàm băm, xác thực và chữ ký số
- + **Phân tích mật mã (Cryptanalysis):** Dành riêng cho các trường nghiên cứu chuyên sâu về mật mã. Có nhiều phương pháp thám mã:
 - Phương pháp tấn công tổng lực (tìm khóa vét cạn)
 - Phương pháp thống kê
 - Phương pháp phân tích cấu trúc
 - ...

Các định nghĩa và khái niệm cơ bản

Các phương pháp xử lý thông tin số trong các hệ thống mật mã:

- **Mật mã khóa bí mật:**

- + Hoán vị
- + Thay thế
- + Xử lý bit (chủ yếu trong các ngôn ngữ lập trình).
- + Phương pháp hỗn hợp (hay mật mã tích – là sự kết hợp của hoán vị và thay thế; điển hình là chuẩn mã hóa dữ liệu – DES, AES của Mỹ)

- **Mật mã khóa công khai:** (Xây dựng trên một số bài toán):

- + **Bài toán logarithm rời rạc**
- + **Bài toán phân tích thừa số**
- + Bài toán xếp ba lô
- + Bài toán mã sửa sai
- + **Bài toán đường cong Elliptic**

Các định nghĩa và khái niệm cơ bản

- **Mật mã khối:**

Quá trình xử lý thông tin được thực hiện trong các **khối có độ dài xác định**.

- **Mật mã dòng:**

Quá trình xử lý thông tin thực hiện trên từng **bit**.



BÀI GIẢNG

CƠ SỞ MẬT MÃ HỌC

Giảng viên: TS. Ngô Đức Thiện

E-mail: thienptit@gmail.com

Bộ môn: Xử lý tín hiệu và truyền thông

Khoa: KTDT1

Bài giảng: Cơ sở mật mã học

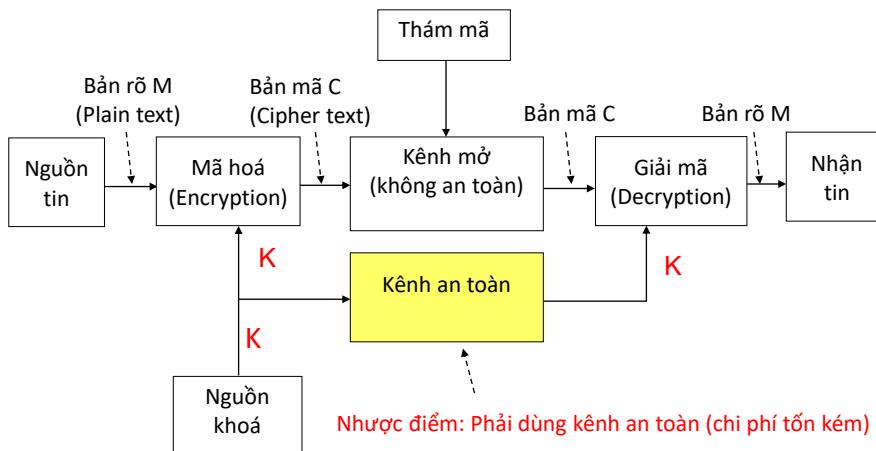
CHƯƠNG I

MẬT MÃ KHÓA BÍ MẬT

(Mật mã khóa đối xứng)

1.1. Sơ đồ khái niệm hệ mật khẩu bí mật

1.1. Sơ đồ khái niệm hệ mật khẩu bí mật



1.1. Sơ đồ khái niệm hệ mật khẩu bí mật

- Một hệ mật là một bộ (P, C, K, E, D) thoả mãn các điều kiện sau:

- + P (hoặc M) là một tập hữu hạn các **bản rõ** có thể.
- + C là một tập hữu hạn các **bản mã** có thể.
- + K là một tập hữu hạn **các khoá** có thể (không gian khoá)
- + Đối với mỗi $k \in K$ có một quy tắc mã hóa: $e_k \in E$

$$e_k : P \rightarrow C$$

và một quy tắc giải mã tương ứng $d_k \in D$

$$d_k : C \rightarrow P$$

- sao cho: $d_k(e_k(x)) = x \quad \text{với } \forall x \in P$

1.2. Các hệ mật thay thế

1.2. Các hệ mật thay thế

1.2.1. Các hệ mật thay thế đơn biểu

a) Mật mã dịch vòng (MDV)

Giả sử $P = C = K = Z_n$ với $1 \leq k \leq n-1$, ta định nghĩa:

- + Mã hóa: $C \equiv M + K \pmod{n}$
- + Giải mã: $M \equiv C - K \pmod{n}$

- Ví dụ với tiếng Anh, $n = 26$ hoặc $n = 27$, như vậy $M, C, K \in Z_{26}$, hoặc Z_{27} .
- Ta sử dụng MDV (với modulo 26) để mã hóa một văn bản tiếng Anh thông thường bằng cách thiết lập sự tương ứng giữa các ký tự theo mod 26 như sau:

1.2. Các hệ mật thay thế

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25

- Ví dụ: $M = \text{meet_me_at_sunset}$

Chọn $K = 4$ ($1 \rightarrow 25$) ta có:

$M = 12.4.4.19_12.4_0.19_18.20.13.18.4.19$

$C = 16.8.8.23_16.8_4.23_22.24.17.22.8.23$

$C = QIX_QI_EX_WYRWIX$

- Nhận xét: Thám mã có thể tìm bẩn rõ bằng phương pháp tìm khóa vét cạn \rightarrow hệ mật không an toàn (số lượng khóa ít $K = 25$)

1.2. Các hệ mật thay thế

- **Bài tập 3.1:** Thám mã thu được bản mã sau của một hệ mật mã dịch vòng với khóa K chưa biết:

PSZI_QIERW_RIZIV_LEZMRK_XS_WEC_CSY_EVI_WSVVC

Hãy thực hiện thám mã bản mã trên bằng các phương pháp đã biết (tìm khóa vét cạn, thống kê và dựa trên các hiểu biết ngôn ngữ). Giả sử bản rõ là một văn bản tiếng Anh.

- **Nhận xét:** Phân bố của khoảng trống (space) tương tự như 1 bản rõ tiếng Anh, cho nên $n=26$ (không mã hóa khoảng trống). (Nếu không thỏa mãn thì $n=27$, mã hóa cả khoảng trống)

1.2. Các hệ mật thay thế

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25
													Space
													26

- **Phương pháp 1: Tìm khóa vét cạn.**

C = PSZI_QIERW_RIZIV_LEZMRK_XS_WEC_CSY_EVI_WSVVC

Chú ý: với hệ mật dịch vòng: mã hóa: $C \equiv M + K \pmod{n}$

giải mã: $M \equiv C - K \pmod{26}$. Khóa $K = 1 \rightarrow 25$, lần lượt chọn K .

- $K = 1 \rightarrow \text{ORYH}$: Vô nghĩa (loại)
- $K = 2 \rightarrow \text{NQXG}$: Vô nghĩa (loại)
- $K = 3 \rightarrow \text{MPWF}$: Vô nghĩa (loại)
- $K = 4 \rightarrow \text{LOVE}$: Có nghĩa, tiếp tục tìm các từ còn lại ta được:

LOVE MEANS NEVER HAVING TO SAY YOU ARE SORRY

1.2. Các hệ mật thay thế

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25
													Space
													26

• Phương pháp thống kê

$$C = \text{PSZI_QIERW_RIZIV_LEZMRK_XS_WEC_CSY_EVI_WSVVC}$$

Ta biết rằng các ký tự có xác suất xuất hiện lớn trong tiếng Anh được sắp xếp theo thứ tự sau: **_ , E, T, A, H, O, N,...**

Trong bản mã C xác suất hiện của chữ **I** nhiều nhất ($N(I) = 5$); trong bảng văn bản tiếng Anh thì chữ **E** xuất hiện nhiều nhất (không kể khoảng trắng).

Do đó, chữ **I** có thể là dịch vòng của chữ **E**; tức là $K = 4$. Thủ với $K = 4$ ta được bắn rõ như phương pháp vét cạn.

1.2. Các hệ mật thay thế

Ký tự	A	B	C	D	E	F	G	H	I	J	K	L	M
Mã tương ứng	0	1	2	3	4	5	6	7	8	9	10	11	12
Ký tự	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Mã tương ứng	13	14	15	16	17	18	19	20	21	22	23	24	25
													Space
													26

$$C = \text{PSZI_QIERW_RIZIV_LEZMRK_XS_WEC_CSY_EVI_WSVVC}$$

• Phương pháp dựa trên hiểu biết về ngôn ngữ

- Nếu văn bản xuất hiện **ký tự đơn** thì chỉ có thể là “**I**” hoặc “**A**”
- Nếu xuất hiện **2 ký tự** thì có thể là: “**AN**”, “**OF**” hoặc “**TO**”...

Trong văn bản xuất hiện 2 ký tự: **XS** → khoảng cách giữa X và S là: $d(X,S) = 5$; hay bản mã có khoảng cách là 5.

Xét các trường hợp: “**AN**” → $d(A,N) = -13 \rightarrow$ loại

“**OF**” → $d(O,F) = 14 - 5 = 9 \rightarrow$ loại

“**TO**” → $d(T,O) = 19 - 14 = 5 \rightarrow$ thỏa mãn

Ta có: **X** là bản mã của **T** từ đó suy ra **K = 4**

1.2. Các hệ mật thay thế

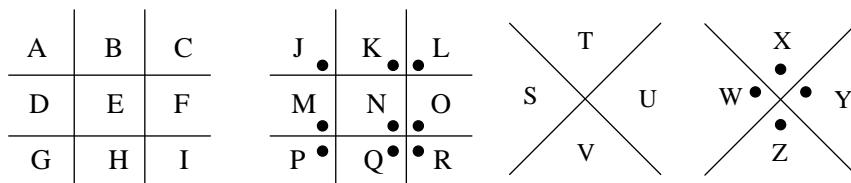
b) Hệ mật dùng bảng thay thế

- Thay thế mỗi ký tự bằng một ký tự khác trong bảng chữ cái. **Như thế số khóa có thể là $|K| = 26! - 1$** ; Với các máy tính hiện nay thì chưa đủ an toàn.
- Khi độ dài bản mã đủ lớn có thể sử dụng phương pháp thống kê để thám mã.

1.2. Các hệ mật thay thế

c) Mật mã “cùi lợn”

- Mỗi một ký tự được “nhốt” vào một “chuồng”, hình ảnh của “chuồng” sẽ đại diện cho ký tự.



Ví dụ: M = MEET ME AT SUNSET

C = ☐☐☐V ☐☐ _V ><☐>☐V

1.2. Các hệ mật thay thế

d) Mật mã Affine

- Mã hóa: $C \equiv aM + b \text{ mod } n$ đây là PT tuyến tính
- Giải mã: $M \equiv (C - b)a^{-1} \text{ mod } n$
- Điều kiện để tồn tại: để có a^{-1} thì $(a, n) = 1$
hay $\text{gcd}(a, n) = 1$; $\text{UCLN}(a, n) = 1$

Nhận xét: Do khoảng trống xuất hiện nhiều lần trong văn bản, nên khi mã hóa nên mã hóa cả khoảng trống để giảm số lần xuất hiện.

1.2. Các hệ mật thay thế

1.2.2. Hệ mật thay thế đa biểu

Hệ mật Vigenère

Sử dụng phép tương ứng $A \leftrightarrow 0, B \leftrightarrow 1, \dots, Z \leftrightarrow 25$ mô tả ở trên, ta có thể gắn cho mỗi khoá K một chuỗi ký tự có độ dài m , được gọi là từ khoá. Mật mã Vigenère sẽ mã hoá đồng thời m ký tự: mỗi phần tử của bản rõ tương đương với m ký tự.

Ví dụ

Giả sử $m = 6$ và từ khoá là **CIPHER**. Từ khoá này tương ứng với dãy số $k = (2, 8, 15, 7, 4, 17)$. Giả sử bản rõ là:

meet me at sunset

Ta sẽ biến đổi các phần tử của bản rõ thành các thặng dư theo mod 26, viết chúng thành các nhóm 6 rồi cộng với từ khoá theo modulo 26 như sau:

1.2. Các hệ mật thay thế

m	e	e	t	m	e	a	t	s	u	n	s	e	t							
12	4	4	19	12	4	0	19	18	20	13	18	4	19	Bản rõ						
2	C	8	I	15	P	7	H	4	E	17	R	2	8	15	7	4	17	2	8	Khoá
14	12	19	0	16	21	2	1	7	1	17	9	6	1	Bản mã						
O	M	T	A	Q	V	C	B	H	B	R	J	G	B							

Như vậy, dãy ký tự tương ứng với xâu bản mã sẽ là:

OMTA QV CB HBRJGB

Chú ý: Để giải mã, ta có thể dùng cùng từ khoá nhưng thay cho cộng, ta trừ nó theo modulo 26.

Ta thấy rằng, số các từ khoá có thể với độ dài m trong mật mã Vigenere là 26^m . Ví dụ, với $m = 6$ thì không gian khoá cũng có kích thước lớn hơn 3.10^8 khoá.

1.3. Các hệ mật hoán vị

1.3. Các hệ mật hoán vị (MHV)

- Khác với mã thay thế, ý tưởng của **mã hoán vị** là **giữ các ký tự của bản rõ không thay đổi**, nhưng sẽ thay đổi **vị trí** của chúng bằng cách sắp xếp lại các ký tự này. Ở đây không có một phép toán đại số nào cần thực hiện khi mã hoá và giải mã.

1.3. Các hệ mật hoán vị

Hệ mật hoán vị độ dài K

Chia bản rõ thành các khối độ dài K và hoán vị các ký tự trong mỗi khối

Ví dụ: Giả sử $m = 6$ và khóa là phép hoán vị sau:

1	2	3	4	5	6
3	5	1	6	4	2

Khi đó, phép hoán vị ngược sẽ là:

1	2	3	4	5	6
3	6	1	5	2	4

Ví dụ bản rõ: $M = \text{asecondclasscarriageonthertrain}$

Trước tiên, ta nhóm bản rõ thành các nhóm 6 ký tự:

a sec on|dclass|carria|geon|th|etrain

Sau đó, mỗi nhóm 6 chữ cái lại được sắp xếp lại theo phép hoán vị:

EOANCS|LSDSAC|RICARA|OTGHNE|RIENAT|

Cuối cùng, ta có bản mã sau:

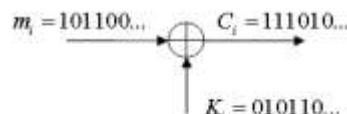
$C = \text{FOANCSLSDSACRICARAOTGHNERIENAT}$

1.4. Các hệ mật mã dòng

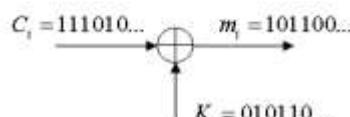
1.4. Các hệ mật mã dòng và việc tạo dãy giả ngẫu nhiên

1.4.1. Các hệ mật mã dòng

+ Mã hóa: $C_i = m_i + k_i \bmod 2$



+ Giải mã: $m_i = C_i + k_i \bmod 2$



Nhận xét:

- Để hệ thống an toàn, dãy bit khóa ngẫu nhiên phải dài hơn bản tin: $|k_i| \geq |m_i|$ (Dãy ngẫu nhiên có $p(0) = p(1) = 0,5$).
- Việc tạo dãy ngẫu nhiên tốn kém và việc lưu trữ không hiệu quả, do đó phải tạo **dãy giả ngẫu nhiên** (có tính tiền định và được xây dựng từ các bit mầm).

1.2.4. Các hệ mã dòng và việc tạo dãy giả ngẫu nhiên

1.4.2. Tạo dãy giả ngẫu nhiên bằng đa thức nguyên thủy

* **Đa thức nguyên thủy:** **Đa thức bất khả quy bậc m được gọi là đa thức nguyên thủy nếu nó là ước của $x^n + 1$ với $n = 2^m - 1$ nhưng không là ước của $x^p + 1$ (với $p < n$).**

(Tức là chia hết cho 1 và chính nó, tương đương số nguyên tố)

Ví dụ: Với $m = 3$ ta có $n = 2^3 - 1 = 7$ và:

$$x^7 + 1 = (x+1)(\underbrace{1+x+x^2}_{\text{Hai đa thức nguyên thủy}})(\underbrace{1+x^2+x^4}_{\text{Hai đa thức không nguyên thủy}})$$

Hai đa thức nguyên thủy

Với $m = 4$ ta có:

$$x^{15} + 1 = (x+1)(1+x+x^2)(1+x+x^4)(1+x^3+x^4)(1+x+x^2+x^3+x^4)$$

↓ ↓
Nguyên thủy Không nguyên thủy
(vì là ước của $x^5 + 1$)

1.4. Các hệ mã dòng và việc tạo dãy giả ngẫu nhiên

Bố đề: Dãy giả ngẫu nhiên (M-dãy) được tạo từ phương trình đồng dư sau:

$$a(x) \equiv b(x) \cdot x^i \pmod{g(x)}; \quad i = \overline{1, 2^m - 1}$$

Với: $g(x)$ - đa thức nguyên thủy bậc m .

$b(x)$ - đa thức mầm, thỏa mãn: $\deg b(x) \leq m-1$ và $b(x) \neq 0$
; chọn ngẫu nhiên ứng với m bit.

Ví dụ: $m = 4$; $g(x) = 1 + x + x^4$

M-dãy được tạo như sau: $a(x) \equiv b(x) \cdot x^i \pmod{1 + x + x^4}$

(Coi $1 + x + x^4 = 0$ hay $x^4 = 1 + x$)

Giả sử: $b(x) = 1 + x \leftrightarrow (1100)$ (4bit)

1.4. Các hệ mã dòng và việc tạo dãy giả ngẫu nhiên

i	$a(x)$	\bar{a}
0	$1+x$	1 1 0 0
1	$x+x^2$	0 1 1 0
2	x^2+x^3	0 0 1 1
3	$1+x+x^3$	1 1 0 1
4	$1+x^2$	1 0 1 0
5	$x+x^3$	0 1 0 1
6	$1+x+x^2$	1 1 1 0
7	$x+x^2+x^3$	0 1 1 1
8	$1+x+x^2+x^3$	1 1 1 1
9	$1+x^2+x^3$	1 0 1 1
10	$1+x^3$	1 0 0 1
11	1	1 0 0 0
12	x	0 1 0 0
13	x^2	0 0 1 0
14	x^3	0 0 0 1
15	$1+x$	1 1 0 0

M-dây

Lấy bất kỳ cột nào ta cũng được 1 M-dây.

Nhận xét:

+ Chu kỳ dây: $i = 2^n - 1$

+ Số con "1" trong dây:

$$N_1 = 2^{n-1}$$

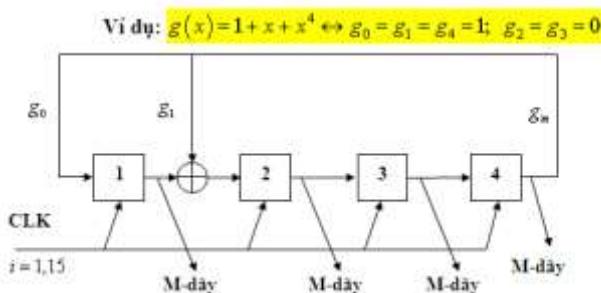
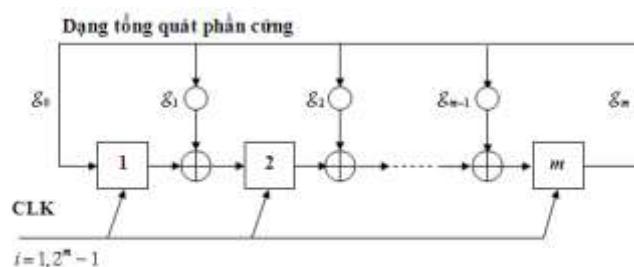
+ Số con "0" trong dây:

$$N_0 = 2^{n-1} - 1$$

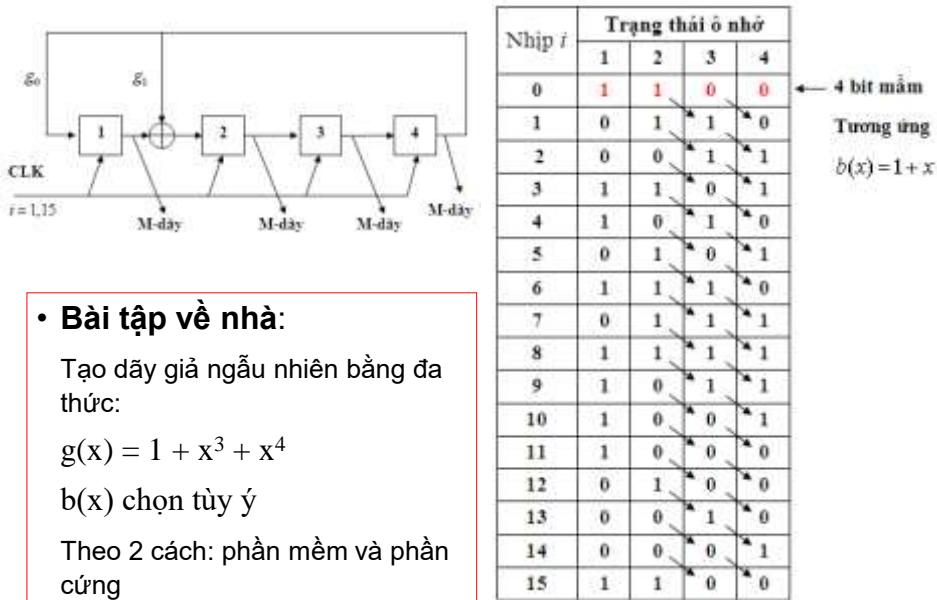
Và do đó:

$$\lim_{n \rightarrow \infty} p(0) = \lim_{n \rightarrow \infty} p(1) = \frac{1}{2}$$

1.4. Các hệ mã dòng và việc tạo dãy giả ngẫu nhiên



1.4. Các hệ mã dòng và việc tạo dãy giả ngẫu nhiên



1.5. Chuẩn mã dữ liệu DES

1.5. Chuẩn mã dữ liệu (DES-Data Encryption Standard)

Đây là mật mã tích (kết hợp Hoán vị và Thay thế) tạo được một hệ mật an toàn từ 2 hệ mật không an toàn.

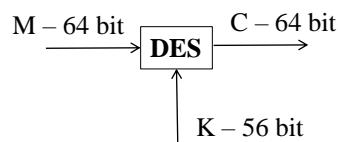
Mô tả đầy đủ của DES được nêu trong Công bố số 46 về các chuẩn xử lý thông tin Liên bang (Mỹ) vào 15/1/1977. DES mã hoá một xâu bit x của bản rõ độ dài 64 bằng một khoá 56 bit. Bản mã nhận được cũng là một xâu bit có độ dài 64.

a) Sơ đồ mã hóa DES

$$C = \text{DES}(M, K)$$

Thuật toán mã hóa (16 vòng)

Theo lược đồ Feistel



1.5. Chuẩn mã dữ liệu (DES)

Thuật toán mã hóa (16 vòng)

For $i = 1$ to 16 do

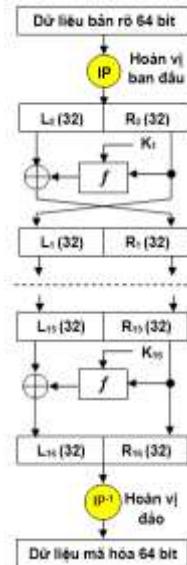
$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

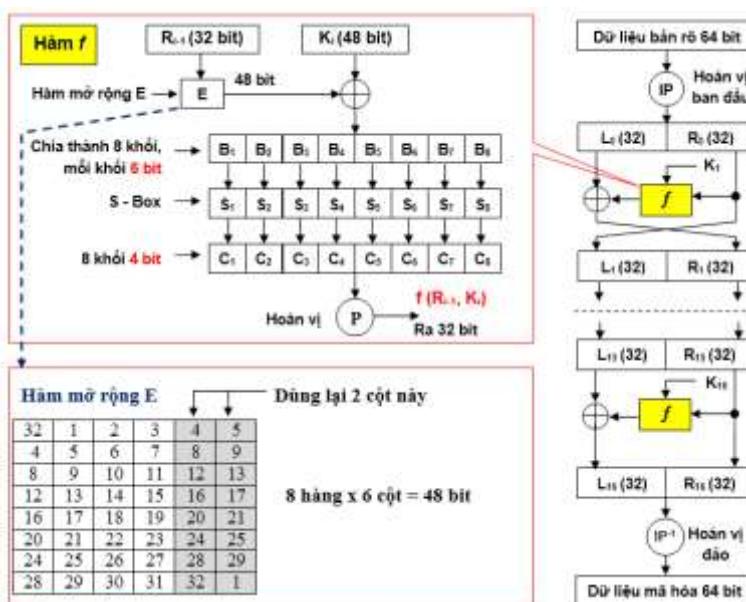
Trong đó: IP (Initial Permutation):

Có **64!** cách chọn bảng IP, DES chọn 1 cách:

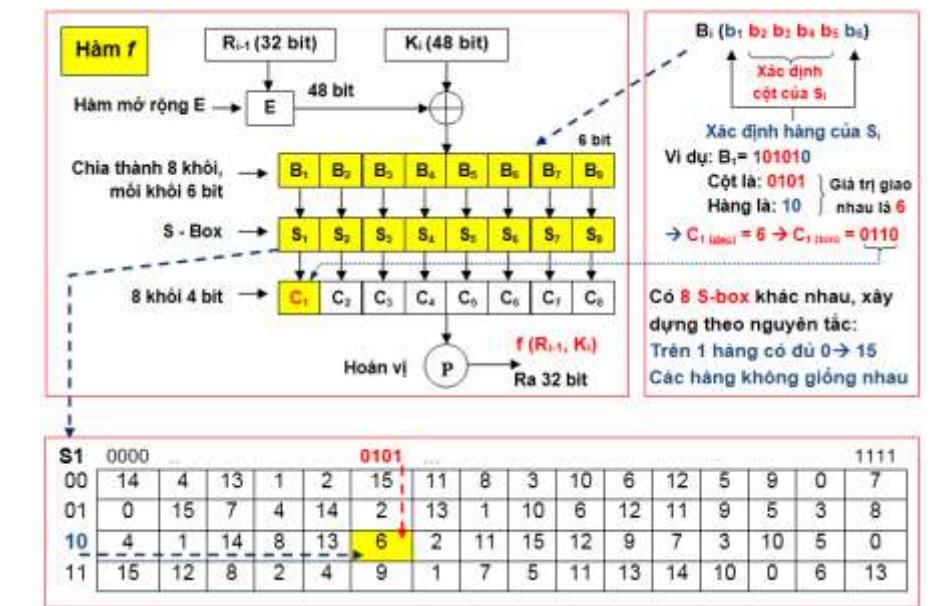
IP															
58	50	42	34	26	18	10	2	40	8	18	16	56	24	64	32
60	52	44	36	28	20	12	4	39	7	47	15	55	23	63	31
62	54	46	38	30	22	14	6	38	6	46	14	54	22	62	30
64	56	48	40	32	24	16	8	37	5	45	13	53	21	61	29
57	49	41	33	25	17	9	1	36	4	44	12	52	20	60	28
59	51	43	35	27	19	11	3	35	3	43	11	51	19	59	27
61	53	45	37	29	21	13	5	34	2	42	10	50	18	58	26
63	55	47	39	31	23	15	7	33	1	41	9	49	17	57	25



1.5. Chuẩn mã dữ liệu (DES)



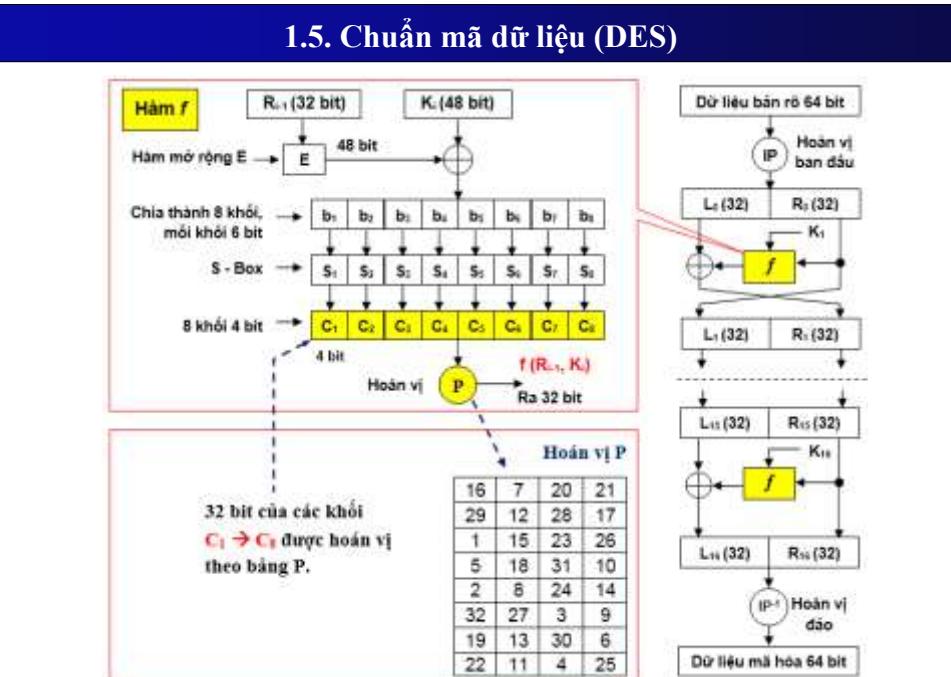
1.5. Chuẩn mã dữ liệu (DES)



Ngô Đức Thiện - PTIT

Chương 1: Mật mã khóa bí mật

27

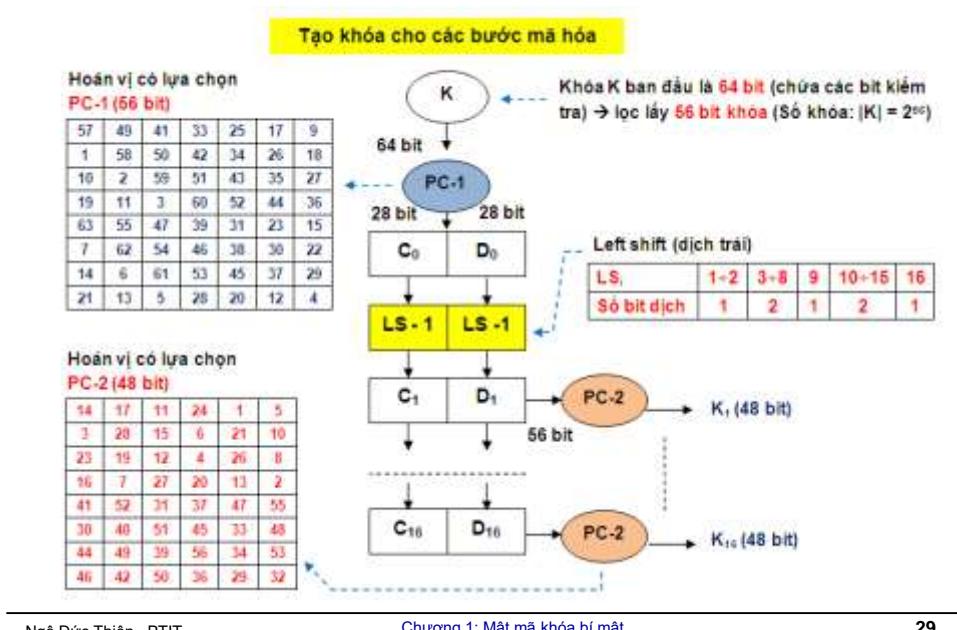


Ngô Đức Thiện - PTIT

Chương 1: Mật mã khóa bí mật

28

1.5. Chuẩn mã dữ liệu (DES)



1.5. Chuẩn mã dữ liệu (DES)

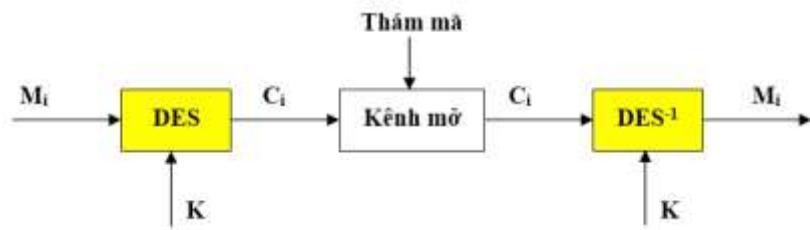
b) Các chế độ hoạt động của DES

- + Các chế độ mã khôi:
 - Chế độ **Quyển mã điện tử ECB** (Electronic Code Book mode).
 - Chế độ **Liên kết mã khôi CBC** (Cipher Block Chaining mode).

- + Các chế độ mã dòng
 - Chế độ **Phản hồi đầu ra OFB** (Output Feedback Mode).
 - Chế độ **Phản hồi mật mã CFB** (Code Feedback Mode)

1.5. Chuẩn mã dữ liệu (DES)

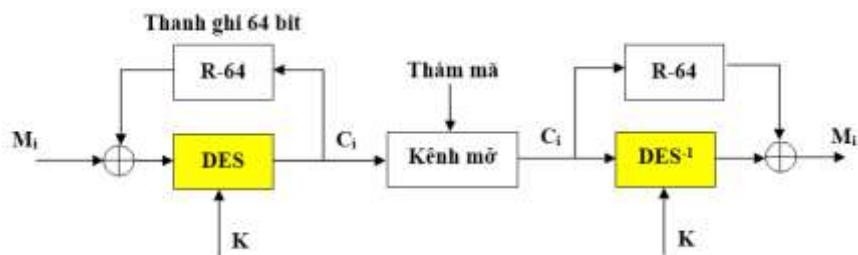
- + Quyển mã điện tử **ECB** (Electronic Code Book mode)
Đây là chế độ hoạt động bình thường của DES



- **Ưu điểm:** Đơn giản
- **Nhược điểm:** Nếu đầu vào giống nhau và cùng khóa thì đầu ra sẽ giống nhau → thám mã có thể phá được.

1.5. Chuẩn mã dữ liệu (DES)

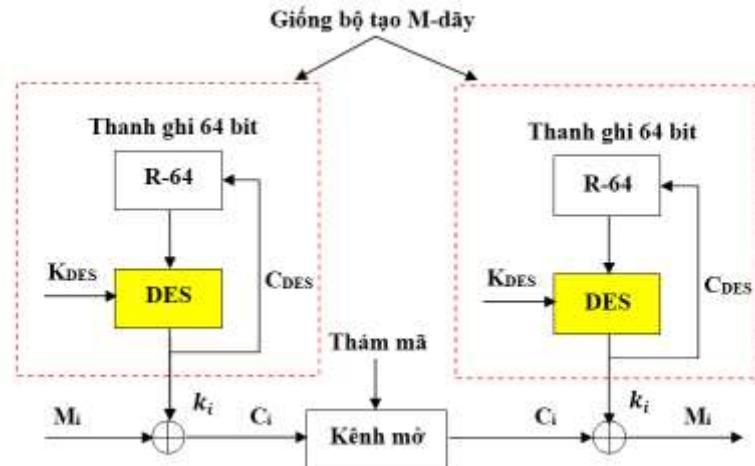
- + Chế độ Liên kết mã khối **CBC** (Cipher Block Chaining mode)
Khắc phục nhược điểm của chế độ ECB



- **Nhược điểm:** Nếu giải mã sai cho khôi nào thì sẽ gây sai toàn bộ các khôi còn lại.

1.5. Chuẩn mã dữ liệu (DES)

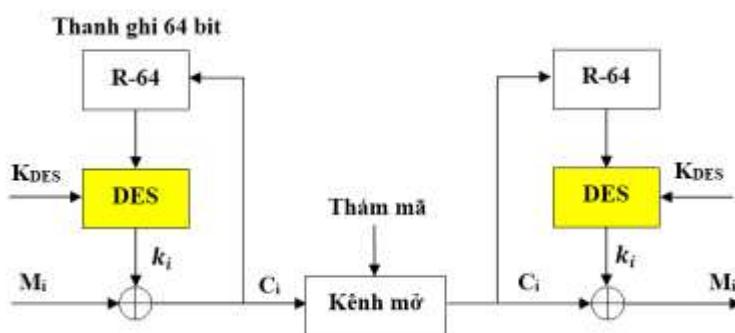
- + Chế độ Phản hồi đầu ra **OFB**



Nhược điểm: giống CBC

1.5. Chuẩn mã dữ liệu (DES)

- + Chế độ Phản hồi mật mã **CFB**



Nhược điểm: giống CBC

1.5. Chuẩn mã dữ liệu (DES)

Nhược điểm của DES:

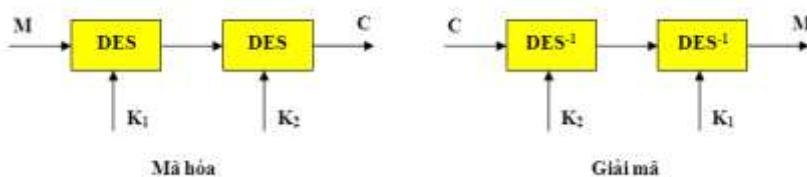
- + Do số lượng của khóa $|K| = 2^{56}$, có thể thám mã phá được với chi phí cao.
- + Để khắc phục phải tăng số lượng khóa hoặc sử dụng các biến thể của DES

1.5. Chuẩn mã dữ liệu (DES)

c) Các biến thể của DES

- + Double DES (DES bội 2)

Thực hiện theo nguyên lý mật mã tích:

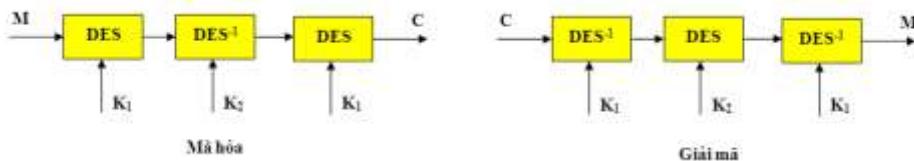


Số lượng khóa: $|K| = |K_1| \cdot |K_2| = 2^{112}$; Cho đến nay thì đảm bảo an toàn (hiện nay với 2^{128} là an toàn) vì khó tóm khóa vét cạn.

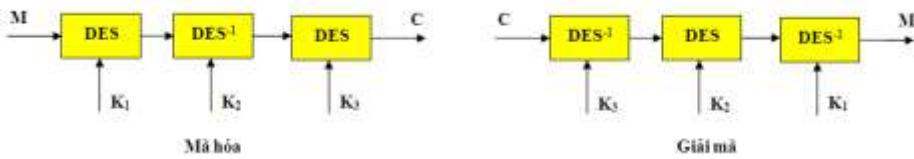
1.5. Chuẩn mã dữ liệu (DES)

- + Triple DES (DES bội 3)

Với 2 khóa: Số lượng khóa: $|K| = 2^{112} \rightarrow$ An toàn hơn
Double DES



Với 3 khóa: $|K| = 2^{168}$



1.6. Ưu, nhược điểm của mật mã khóa bí mật

- + Ưu điểm:
 - Đơn giản (Thời gian xử lý nhanh, phần cứng yêu cầu thấp)
 - Hiệu quả cao (Hệ số mở rộng bản tin R = 1; ví dụ với DES vào 64 bit ra 64 bit)
- Dễ sử dụng cho các ứng dụng nhẹ cảm với trễ và các ứng dụng di động.
- + Nhược điểm:
 - Phải dùng kênh an toàn để truyền khóa (khó thiết lập, tốn kém)
 - Việc tạo, giữ bí mật khóa phức tạp (khi làm việc trên mạng phải tạo nhiều khóa).
 - Khó xây dựng các dịch vụ an toàn khác (như đảm bảo tính toàn vẹn, xác thực và chữ ký số)
- Để khắc phục các nhược điểm này phải sử dụng Hệ mật khẩu công khai.



BÀI GIẢNG

CƠ SỞ MẬT MÃ HỌC

Giảng viên: TS. Ngô Đức Thiện

Điện thoại: 0912.928.928

E-mail: thienptit@gmail.com

Bộ môn: Lý thuyết mạch - Khoa KTDT1

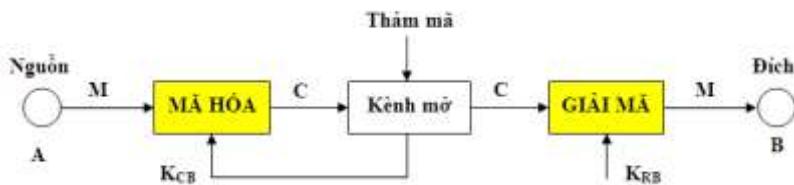
Bài giảng: Cơ sở mật mã học

CHƯƠNG II

CÁC HỆ MẬT KHÓA CÔNG KHAI

(Hệ mật khóa bất đối xứng)

2. 1. Sơ đồ khái niệm



K_{CB} - Khóa công khai của B; K_{RB} - Khóa bí mật của B

Mã hóa: $C = E(M, K_{CB})$; **Giải mã:** $M = E^{-1}(C, K_{RB}) = D(C, K_{RB})$

- Ưu điểm:**
- Không cần 2 khóa bí mật
 - Không cần kênh an toàn riêng.
 - Biết khóa mã hóa trên kênh mở nhưng rất khó giải mã

Yêu cầu: **Dễ mã hóa, khó giải mã** (Hàm 1 chiều, tính thuận đơn giản, tính ngược phức tạp)

2. 1. Sơ đồ khái niệm

- Mật mã khóa công khai ra đời thỏa mãn các yêu cầu bảo mật thông tin ngày càng phát triển
- Từ năm 1976 cho tới nay, trên thế giới đã tìm ra một số hàm 1 chiều, tương ứng với các bài toán dùng để xây dựng mã:
 - + Bài toán Logarit rời rạc
 - + Bài toán phân tích thừa số
 - + Bài toán xếp ba lô
 - + Bài toán mã sửa sai
 - + Đường cong Elliptic

2.2. Bài toán logarit rời rạc và các hệ mật liên quan

2.2.1. Bài toán Logarit rời rạc

a) Bài toán logarit trên trường số thực R

+ Bài toán thuận: $y = a^x$ ($a, x \in R$)
+ Bài toán ngược: $y = \log_a x$

Hai bài toán thuận và ngược
đều là hàm **đồng biến**, có thể
tính tương đối được

- Tính chất: + $y = \log_a bc = \log_a b + \log_a c$

$$+ y = \log_a \frac{b}{c} = \log_a b - \log_a c$$

$$+ y = \log_a 1 = 0$$

$$+ y = \log_a x^{-1} = -\log_a x$$

2.2.1. Bài toán logarit rời rạc

b) Bài toán logarit trên trường hữu hạn

Xét vành số \mathbb{Z}_p , p – nguyên tố $\rightarrow \mathbb{Z}_p = GF(p)$

Tất cả các phần tử $\neq 0$ của trường tạo thành nhóm nhân (cyclic): $\mathbb{Z}_p^* = \mathbb{Z}_p / \{0\}$

+ **Bài toán thuận:** $y = a^x$

Ví dụ: $p=19$; $a=2$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$\log_2 x$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(do $2^{18}=1$ nên $\log_2 1=18$)

Chú ý: các phần tử lấy modulo theo $p=19$

2.2.1. Bài toán logarit rời rạc

Chú ý: + Nếu α là phần tử nguyên thủy thì α^i sẽ đi qua hết các phần tử của nhóm.

+ Nếu α là phần tử nguyên thủy thì α^i cũng là nguyên thủy nếu $(i, |\mathbb{Z}_{19}^*|) = 1$

$$\Rightarrow i = \{1, 5, 7, 11, 13, 17\}; \text{ và } N(i) = \varphi(18)$$

$$\text{Do } 18 = 2 \cdot 3^2 \rightarrow N(i) = \varphi(18) = 18 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 6$$

Các phần tử nguyên thủy tạo thành các cặp nghịch đảo

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$\log_2 x$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

Các cặp nghịch đảo

Ta có: $2^{-1} = 10$ là hai phần tử nghịch đảo vì: $2 \cdot 10 \equiv 1 \pmod{19}$

Tương tự hai cặp nghịch đảo là: $(3, 13)$ và $(14, 15)$

2.2.1. Bài toán logarit rời rạc

+ **Bài toán ngược:** $y = \log_a x, a, x \in \mathbb{Z}_p^*$

Dựa trên tính chất của hàm loga:

$$y = \log_a bc = (\log_a b + \log_a c) \pmod{p}$$

$$y = \log_a \frac{b}{c} = (\log_a b - \log_a c) \pmod{p}$$

$$y = \log_{a^{-1}} x = -\log_a x = p-1 - \log_a x$$

$$y = \log_a 1 = p-1 = 0$$

Bài toán Logarit rời rạc: Cho \mathbb{Z}_p , p - số nguyên tố; α là phần tử nguyên thủy $\in \mathbb{Z}_p^*$

Hãy tìm: $y = \log_\alpha x, \alpha, x \in \mathbb{Z}_p^*$

Nhận xét: $\forall x \in \mathbb{Z}_p^*$ + Bài toán có nghiệm khi α là phần tử nguyên thủy.

+ Bài toán có thể không có nghiệm khi α bất kỳ

2.2.1. Bài toán logarit ròi rạc

Giải: Với bài toán khi $p = 19$, ta có 6 điểm nguyên thủy (3 cặp nghịch đảo)

$$2 \leftrightarrow 2^{-1} = 10 \quad 3 \leftrightarrow 3^{-1} = 13 \quad 14 \leftrightarrow 14^{-1} = 15$$

Áp dụng $\log_{a^{-1}} x = -\log_a x = p-1 - \log_a x \Rightarrow \log_{a^{-1}} x + \log_a x = p-1$

Xét với cặp nguyên thủy (2,10): ta có $\log_{10} x = p-1 - \log_2 x$ (chú ý: 0=18)

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2^x	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
$\log_2 x$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9
$\log_{10} x$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

Với cặp (13,3) ta có: (Chú ý: $13 = 2^5 \leftrightarrow 13^i = 2^{5i}$)

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
13^x	13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
$\log_{13} x$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9
$\log_3 x$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

Nhận xét: Khi biết bài toán thuận thì khó tính bài toán ngược vì **hàm không đồng biến**.

2.2.2. Các hệ mật liên quan

a) Trao đổi và thỏa thuận khóa Diffie - Hellman

Bài toán: A và B cần thống nhất 1 khóa K dùng cho hệ khóa bí mật.

Cho p - nguyên tố; α - là phần tử nguyên thủy của \mathbb{Z}_p^* $\rightarrow (\mathbf{p}, \alpha)$ **Khóa công khai**.

- | | |
|---|---|
| A
+ A chọn x ngẫu nhiên ($1 < x < p-1$)
và tính $\alpha^x \text{ mod } p \rightarrow$ gửi cho B.
+ A nhận α^y và tính $(\alpha^y)^x \text{ mod } p = K$ | B
+ B chọn y ngẫu nhiên ($1 < y < p-1$)
và tính $\alpha^y \text{ mod } p \rightarrow$ gửi cho A.
+ B nhận α^x và tính $(\alpha^x)^y \text{ mod } p = K$ |
|---|---|

Ví dụ: $p = 19$; $\alpha = 2$;

- | | |
|---|--|
| A
+ A chọn $x = 3$ ngẫu nhiên và tính
$2^3 \text{ mod } 19 = 8 \rightarrow$ gửi cho B.
+ A nhận 13; tính $K = (13)^3 \text{ mod } 19 = 12$ | B
+ B chọn $y = 5$ ngẫu nhiên và tính
$2^5 \text{ mod } 19 = 13 \rightarrow$ gửi cho A.
+ B nhận 8 và tính $K = (8)^5 \text{ mod } 19 = 12$ |
|---|--|

Nhận xét: Để tìm K thám mã phải giải bài toán logarit ròi rạc ngược. Tức là phải xác định $x = \log_a \alpha^y$ và $y = \log_a \alpha^x$

a. Trao đổi và thỏa thuận khóa Diffie - Hellman

Nhược điểm:

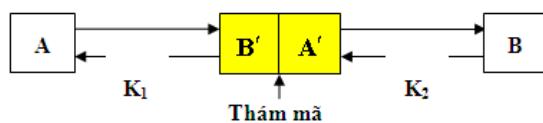
Thám mã có thể sử dụng **phép tấn công Kẻ đứng giữa** (Man in the middle)

-Thám mã là kẻ đứng giữa sẽ giả danh cả hai bên A và B.

Thám mã liên lạc với A bằng mã K_1 , giải mã để lấy cắp thông tin.

Sau đó lại mã hóa thông tin của A bằng khóa K_2 để liên lạc với B.

→ A và B vẫn nhận đúng thông tin tưởng là liên lạc đúng với nhau nhưng thực ra là liên lạc với thám mã.



Đây là điểm yếu, để khắc phục sử dụng xác thực.

b. Hệ mật Omura - Massey

b) Hệ mật Omura – Massey



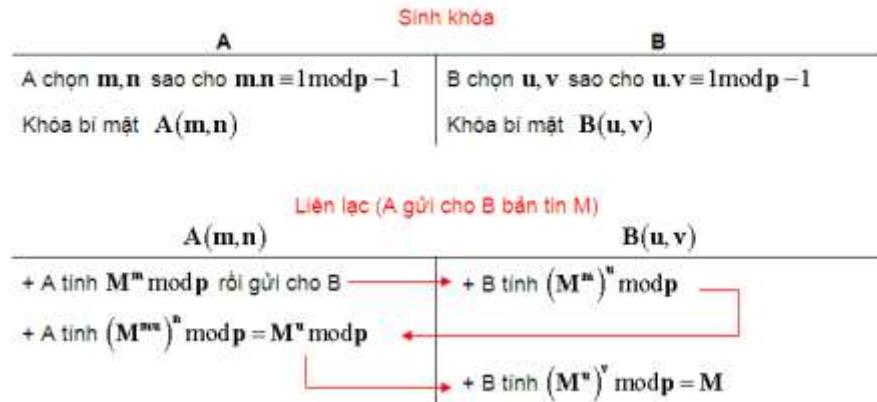
Nhược điểm: Phải thực hiện truyền 3 lần.

B mở khóa B để lấy bản tin M

b. Hệ mật Omura – Massey (O-M)

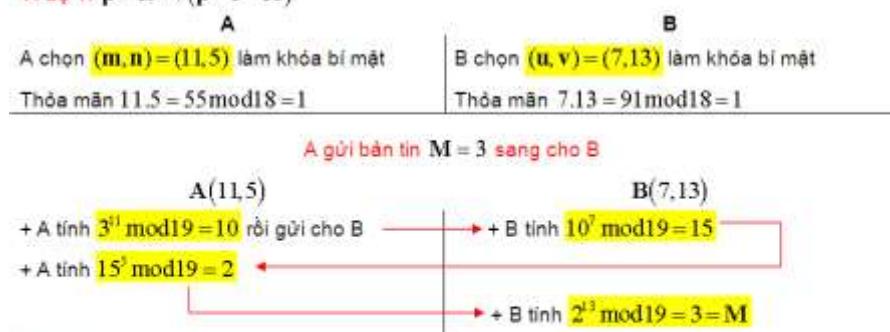
Dùng bài toán logarit rời rạc:

Cho Z_p ; p - nguyên tố (khóa công khai)



b. Hệ mật Omura – Massey (O-M)

Ví dụ 1: $p = 19 \rightarrow (p-1=18)$



Nhận xét: - Để tìm bản tin M thàm mã phải giải bài toán logarit rời rạc.

- Về mặt hiệu quả: Tốc độ truyền $R = \frac{1}{3}$ (thấp) \rightarrow thích hợp truyền tin ngắn hoặc truyền khóa (phân phối khóa cho một hệ mật khóa bí mật)

b. Hệ mật Omura - Massey

Ví dụ 2: Tìm các khóa cho hệ mật O-M

Chọn \mathbb{Z}_p ; p – nguyên tố \rightarrow khóa công khai:

$$\left. \begin{array}{l} A \text{ chọn } (m,n): mn \equiv 1 \pmod{p-1} \\ B \text{ chọn } (u,v): uv \equiv 1 \pmod{p-1} \end{array} \right\} \quad \boxed{\text{Tập khóa là: } |\mathbb{Z}_{p-1}^*| = \varphi(p-1)}$$

Với $p = 19$ thì $p-1 = 18 = 2 \cdot 3^2 \rightarrow$ Ta có: $|\mathbb{Z}_{18}^*| = \varphi(18) = 18 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 6$

Vậy $\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\} \rightarrow$ tạo thành các **cặp nghịch đảo**.

Ta có: $+ 1 \cdot 1 \equiv 1 \pmod{18} \rightarrow$ loại vì khóa đồng nhất.

$+ 5 \cdot 11 \equiv 1 \pmod{18}$

$+ 7 \cdot 13 \equiv 1 \pmod{18}$

$+ 17 \cdot 17 \equiv 1 \pmod{18} \rightarrow$ tự nghịch đảo

c. Hệ mật ElGamal

c. Hệ mật ElGamal

+ **Tạo khóa:** Mỗi bên liên lạc (A,B) tự tạo cho mình một cặp khóa công khai và bí mật, theo các bước sau:

Bước 1: Chọn p - nguyên tố lớn, α là phần tử nguyên thủy $\in \mathbb{Z}_p^*$

Bước 2: chọn a ngẫu nhiên ($1 < a < p-1$) và tính $\alpha^a \pmod{p}$

Bước 3: **Khóa công khai:** (p, α, α^a)

Khóa bí mật: a

c. Hệ mật Elgamal

+ **Mã hóa:** B cần gửi bản tin m cho A (coi độ dài $m < p$)

Bước 1: B nhận khóa công khai của A: (p, α, α^a)

Bước 2: B chọn k ngẫu nhiên ($1 < k < p - 1$) và tính:

$$\gamma = \alpha^k \bmod p$$

$$\delta = m(\alpha^a)^k \bmod p$$

Bước 3: B gửi bản mã $C = (\gamma, \delta)$ cho A

(nhược điểm: độ dài bit bằng 2 lần chiều dài m)

+ **Giải mã:** A nhận bản mã C và giải mã.

Bước 1: A tính $\gamma^{p-1-a} \bmod p = (\alpha^k)^{p-1-a} \bmod p = \alpha^{-ak} \bmod p$

Bước 2: A tính $\delta \cdot \gamma^{p-1-a} = m \alpha^{ak} \alpha^{-ak} \bmod p = m$

c. Hệ mật ElGamal

Ví dụ:

+ **Tạo khóa:** A chọn $p = 17; \alpha = 3; a = 6;$

A tính: $3^6 \bmod 17 \equiv 15$

- Khóa công khai của A: $(17, 3, 15)$

- Khóa bí mật của A: $a = 6$

+ **Mã hóa:** B cần gửi bản rõ $m = 7$ cho A

- Bước 1: B nhận khóa công khai của A: $(17, 3, 15)$

- Bước 2: B chọn $k = 4$ và tính:

$$\gamma = 3^4 \bmod 17 \equiv 13; \quad \delta = 7 \cdot 15^4 \bmod 17 \equiv 10$$

- Bước 3: B gửi bản mã $C = (13, 10)$ cho A

+ **Giải mã:** A nhận bản mã C và giải mã

- Bước 1: A tính $\gamma^{16-6} = 13^{10} \bmod 17 \equiv 16$

- Bước 2: A tính $m = \delta \cdot \gamma^{p-1-a} = 10 \cdot 16 \bmod 17 \equiv 7$

c. Hệ mật ElGamal

Nhận xét

- Để giải mã thì thám mã phải biết a (khóa bí mật), và do đó phải giải bài toán logarit rời rạc (Tính $a = \log_{\alpha} \alpha^a$) với p lớn không thể giải được → an toàn.
- Hiệu quả truyền tin thấp: Hệ số mở rộng bản tin là 2 (Do bản mã $C = (\gamma, \delta)$ có độ dài bằng 2 lần độ dài m).

2.3. Bài toán phân tích thừa số và hệ mật RSA

3. Bài toán phân tích thừa số và hệ mật RSA

a) Bài toán phân tích thừa số:

+ Định lý cơ bản của số học:

Cho n là một số nguyên dương thì tồn tại phân tích duy nhất:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

với: p_i - số nguyên tố;

e_i - số nguyên dương.

Nếu n là tích của hai số nguyên tố: $n = pq$

(p, q là các số nguyên tố lớn thỏa mãn $|p| \approx |q|$).

Thì khi đó việc phân tích $n = pq$ là bài toán khó.

(tức là biết p, q thì tìm n đơn giản; nhưng cho n thì rất khó tìm p, q)

b) Hệ mật RSA (Rivest – Shamir – Adleman)

b) Hệ mật RSA (Rivest – Shamir – Adleman)

Tạo khóa: Mỗi bên liên lạc (A,B) tự tạo cho mình một cặp khóa công khai – bí mật theo các bước sau:

- + Bước 1: Chọn 2 số nguyên tố lớn p và q có độ lớn tương đương
- + Bước 2: Tính $n = pq \rightarrow \varphi(n) = (p - 1)(q - 1)$
- + Bước 3: Chọn e ngẫu nhiên thỏa mãn: $(e, \varphi(n)) = 1$
- + Bước 4: Tính d với $ed \equiv 1 \pmod{\varphi(n)}$
- + Bước 5: Khóa công khai: (n, e)

Khóa bí mật: d

Trong đó: e là số mũ mã hóa; d là số mũ giải mã.

Vai trò của e và d là như nhau (2 số nghịch đảo), tức là nếu mã hóa dùng e thì giải mã dùng d và ngược lại.

b) Hệ mật RSA (Rivest – Shamir – Adleman)

+ **Mã hóa:** B cần gửi bản tin m cho A.

Bước 1: B nhận khóa công khai của A: (n, e)

Bước 2: B tính $C \equiv m^e \pmod{n}$

Bước 3: B gửi bản mã C cho A.

+ **Giải mã:** A nhận C và giải mã ra m:

A tính $C^d \pmod{n} = (m^e)^d \pmod{n} = m$

+ **Nhận xét:** - Tham mã phải thực hiện bài toán phân tích thừa số $n = pq$

thì mới tính được $\varphi(n)$ (nếu biết d muốn tìm $e \rightarrow ed \equiv 1 \pmod{\varphi(n)}$)

- Hiệu quả truyền tin cao $R \approx 1 \rightarrow$ Hệ mật RSA được sử dụng rộng rãi
hơn 30 năm qua.

b) Hệ mật RSA (Rivest – Shamir – Adleman)

Ví dụ 1: Xây dựng các tham số cho hệ mật RSA (Tạo khóa)

Bước 1: A chọn $p = 7$ và $q = 17$

Bước 2: A tính $n = pq = 119$

$$\Rightarrow \phi(n) = (p-1)(q-1) = 96$$

Bước 3: Chọn $e = 5$ thỏa mãn: $(5, 16) = 1$; $(5, 6) = 1$

Bước 4: Tính d : $ed \equiv 1 \pmod{\phi(n)} \Rightarrow 5d \equiv 1 \pmod{96}$

giải phương trình đồng dư để tính d : $5d = 1 + k \cdot 96$

$$- \text{tim đc } k = 4 \Rightarrow d = \frac{385}{5} = 77$$

Bước 5: + Khóa công khai: $(119, 5)$; Khóa bí mật: $d = 77$

+ Hoặc: Khóa công khai: $(119, 77)$; Khóa bí mật: $d = 5$

b) Hệ mật RSA (Rivest – Shamir – Adleman)

Ví dụ 2: Mã hóa cho hệ mật RSA

+ Chọn $p = 43$; $q = 59 \Rightarrow n = pq = 2537$

$$\Rightarrow \phi(n) = (p-1)(q-1) = 42 \cdot 58 = 2436$$

+ Chọn $d = 517 \Rightarrow e = d^{-1} = 517^{-1} = 1357$

+ B mã hóa bản tin: $m = \text{CRYPTOGRAPH}$

Biểu diễn dạng hexa của m :

$m_{\text{hex}} = 43.52.59.50.54.4F.47.52.41.50.48$

$m_{\text{bin}} = 01000011.01010010.01011001.01010000.01010100.01001111.$

$01000111.01010010.01000001.01010000.01001000 \text{ (88 bit)}$

Chú ý: $n = 2537 > 2048 = 2^{11} \Rightarrow |m| = 11 \text{ số bit tối đa cho 1 khối. Chia thành 8 khối}$

$m_{\text{bin}} = 01000011010.10010010110.01010100000.10101000100.1111$

$0100011.10101001001.00000101010.00001001000 \text{ (8 khối)}$

$\rightarrow m_{\text{dec}} = 538.1174.672.1348.1955.1353.42.72$

b) Hệ mật RSA (Rivest – Shamir – Adleman)

+ Mã hóa: $C_i = m_i^e \text{ mod } n = m_i^{1337} \text{ mod } 2537$

$$m_{\text{dec}} = 538.1174.672.1348.1955.1353.42.72 = m_1.m_2...m_8$$

$$\left. \begin{array}{l} C_1 = 538^{1337} \text{ mod } 2537 = 905 \\ C_2 = 1174^{1337} \text{ mod } 2537 = 1307 \\ C_3 = 672^{1337} \text{ mod } 2537 = 1040 \\ C_4 = 1348^{1337} \text{ mod } 2537 = 1987 \\ C_5 = 1955^{1337} \text{ mod } 2537 = 750 \\ C_6 = 1353^{1337} \text{ mod } 2537 = 1567 \\ C_7 = 42^{1337} \text{ mod } 2537 = 1590 \\ C_8 = 72^{1337} \text{ mod } 2537 = 1093 \end{array} \right\}$$

Khi truyền đi chuyển
thành chuỗi bit.

+ Giải mã: $m_1 = C_1^d \text{ mod } 2537 = 905^{517} \text{ mod } 2537 = 538$

Nhận xét:

Phai tính các phép lũy thừa modulo lớn → sử dụng thuật toán nhân và bình phương.

c) Thuật toán nhân và bình phương

+ Tính lũy thừa modulo và thuật toán nhân và bình phương.

$$e^t \text{ mod } n = (e.e....e) \text{ mod } n \Rightarrow e^t \text{ mod } n = \underbrace{[(e \text{ mod } n).(e \text{ mod } n)....(e \text{ mod } n)]}_{t \text{ lần}} \text{ mod } n$$

Hay: $e^t \text{ mod } n = \left[\prod^t (e \text{ mod } n) \right] \text{ mod } n \rightarrow$ tính theo thuật toán nhân và bình phương biểu

diễn t theo dạng tổng của các lũy thừa bậc 2 khác nhau.

Ví dụ: Tính $11^{207} \text{ mod } 13$; ta có: $207 = 1+2+4+8+64+128$ hay $(11110011)_{\text{bin}}$

$$11^{207} \text{ mod } 13 = 11^{(128+64+8+4+2+1)} \text{ mod } 13 = 11^{128}.11^{64}.11^8.11^4.11^2.11 \text{ mod } 13$$

$$11^{207} \text{ mod } 13 = \left[\underbrace{(11^{128} \text{ mod } 13)}_{= 9}, \underbrace{(11^{64} \text{ mod } 13)}_{= 3}, \underbrace{(11^8 \text{ mod } 13)}_{= 9}, \underbrace{(11^4 \text{ mod } 13)}_{= 3}, \underbrace{(11^2 \text{ mod } 13)}_{= 4}, \underbrace{(11 \text{ mod } 13)}_{= 11} \right] \text{ mod } 13$$

$$= 32076 \text{ mod } 13 = 5$$

c) Thuật toán nhân và bình phương

- VÀO: $a \in Z_n$ và số nguyên k , ($0 \leq k \leq n$) có biểu diễn nhị phân: $k = \sum_{i=0}^t k_i 2^i$
- RA: Kết quả $b \equiv a^k \pmod{n}$
 - (1) Đặt $b \leftarrow 1$. Nếu $k = 0$ thì return (b)
 - (2) Đặt $A \leftarrow a$
 - (3) Nếu $k_0 = 1$ thì đặt $b \leftarrow a$
 - (4) For i from 1 to t do
 - (4.1) Đặt $A \leftarrow A^2 \pmod{n}$
 - (4.2) nếu $k_i = 1$ thì đặt $b \leftarrow A \cdot b \pmod{n}$
 - (5) Return (b)

BTVN: Sử dụng một ngôn ngữ lập trình nào đó để thực hiện thuật toán nhân và bình phương để tính hàm mũ theo modulo

c) Thuật toán nhân và bình phương

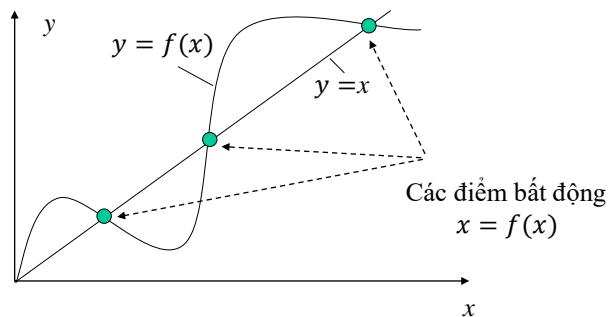
Ví dụ: Tính $a^k = 5^{35} \pmod{37}$.

$$k = 35 = 2^5 + 2^1 + 2^0 = 32 + 2 + 1 \rightarrow (100011)$$
$$(k_0 = 1; k_{1,5} = 1; k_{2,3,4} = 0)$$

- (1) Đặt $b \leftarrow 1$. ($k \neq 0$)
 - (2) Đặt $A \leftarrow a = 5$
 - (3) Do $k_0 = 1$ đặt $b \leftarrow a = 5$
 - (4) For i from 1 to $t = 5$ do
 - $+ i = 1$: Đặt $A \leftarrow A^2 \pmod{37} = 25$
 - $k_1 = 1$ đặt $b \leftarrow A \cdot b \pmod{n} = 5 \cdot 25 \pmod{37} = 14$
 - $+ i = 2$: ...
 - (5) Return ($b = 15$)
- $\rightarrow 5^{35} \pmod{37} = 15$

d) Vấn đề điểm bất động trong RSA

- Mã hóa là ánh xạ 1:1: $y = f(x)$ (hoặc $c = f(m)$)
- Tồn tại các giá trị: x sao cho: $x = f(x) \rightarrow$ các x này gọi là các điểm bất động (không che giấu được thông tin)
- Ví dụ: xét RSA: $p = 5, q = 7 \rightarrow n = 35$, chọn $e = 17$
khi đó: $m = 8 \rightarrow C = m^e \bmod n = 8^{17} \bmod 35 = 8 = m$.



d) Vấn đề điểm bất động trong RSA

- Định lý:** Với hệ mật RSA có tham số khóa (n, e) ; $n = p \cdot q$ thì số bản tin không thể che giấu (số điểm bất động) tính như sau:
$$N = [1 + \text{UCLN}(e - 1, p - 1)] * [1 + \text{UCLN}(e - 1, q - 1)]$$

- Ví dụ: $(n, e) = (35, 17)$; $(p = 5, q = 7)$

$$N = [1 + UCLN(16, 4)] * [1 + UCLN(16, 6)] = 15 \rightarrow XS \sim 1/2$$
$$m = (0, 1, 6, 7, 8, 13, 14, 15, 20, 21, 22, 27, 28, 29, 34)$$

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

2.4.1. Bài toán xếp ba lô

a) Định nghĩa dãy siêu tăng:

Xét một dãy (a_1, a_2, \dots, a_n) ; với a_i nguyên dương.

Nếu: $a_i \geq \sum_{j=1}^{i-1} a_j$ thì dãy này là dãy siêu tăng.

Ví dụ dãy: (1,2,4,8,16,32,64,128)

b) Bài toán xếp ba lô:

- Cho một tập hợp các gói có trọng lượng M_i , yêu cầu xếp các gói vào 1 ba lô chứa được trọng lượng S .

$$S = \sum_{i=1}^n b_i M_i$$

Với: $b_i = 0$ nếu gói M_i **không được** xếp vào ba lô.

$b_i = 1$ nếu gói M_i **được** xếp vào ba lô.

- Bài toán có: 2^n phương án (2^n vecto nhị phân) nếu n lớn (và trăm) \rightarrow không thể giải ở thời gian thực.

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

c) Giải bài toán xếp ba lô trong trường hợp dãy siêu tăng

- Độ phức tạp của BT ~ n (không phải 2^n)

VÀO: - Dãy siêu tăng (M_1, M_2, \dots, M_n)

- Trọng lượng ba lô chứa được: S

RA: Phương án sắp xếp, hay vecto $b = (b_1, b_2, \dots, b_n)$

- Bước 1: $i \leftarrow n$

- Bước 2: while $i \geq 1$ do

if $S \geq M_i$ then: $\begin{cases} b_i = 1 \\ S \leftarrow S - M_i \end{cases}$

else $b_i = 0$

end

$i \leftarrow i - 1$; End.

- Bước 3: $b = (b_1, b_2, \dots, b_n)$

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

Ví dụ: Vào: - Dãy siêu tăng $(1,2,4,8,16,32,64)$; $n = 7$

- Trọng lượng ba lô chưa được: $S = 57$

Ra: - Tìm phương án sắp xếp $b = (b_1, b_2, \dots, b_7)$

• Bước 1: $i = 7$

• Bước 2: while $i \geq 1$

$$+ 57 < 64 \rightarrow b_7 = 0; i = 6$$

$$+ 57 > 32 \rightarrow b_6 = 1; S = 57 - 32 = 25; i = 5$$

$$+ 25 > 16 \rightarrow b_5 = 1; S = 25 - 16 = 9; i = 4$$

$$+ 9 > 8 \rightarrow b_4 = 1; S = 9 - 8 = 1; i = 3$$

$$+ 1 < 4 \rightarrow b_3 = 0; i = 2$$

$$+ 1 < 2 \rightarrow b_2 = 0; i = 1$$

$$+ 1 = 1 \rightarrow b_1 = 1; S = 1 - 1 = 0; i = 0$$

• Bước 3: $b = (1,0,0,1,1,1,0)$

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

2.4.2. Hệ mật Merkle – Hellman

a) Tạo khóa:

Mỗi bên liên lạc tạo cho mình một cặp khóa BM-CK theo các bước sau:

- B1: Chọn 1 dãy siêu tăng (M_1, M_2, \dots, M_n) và một giá trị modulo M thỏa mãn

$$M \geq \sum_{i=1}^n M_i$$

(M là số thứ tự thứ $n+1$ của dãy siêu tăng).

- B2: Chọn một số ngẫu nhiên W ($1 < W < M$) với $(W, M) = 1$. Dễ nhất chọn M là số nguyên tố.
- B3: Tính các $a_i \equiv W \cdot M_i \pmod{M}; i = 1..n$
- B4: **Khóa CK:** $A_{CK} = (a_1, a_2, \dots, a_n)$ dãy ngẫu nhiên

Khóa BM: $(M, W, (M_1, M_2, \dots, M_n))$

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

b) Mã hóa:

Giả sử B cần gửi bản tin $\mathbf{m} = (m_1, m_2, \dots, m_n)$ cho bên A,

với $m_i \in \{0,1\}$

- B1: B nhận khóa CK của A: (a_1, a_2, \dots, a_n)
- B2: B tính

$$C = \sum_{i=1}^n m_i a_i$$

- B3: B gửi bản mã C cho A.

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

c) Giải mã:

A nhận bản mã C và giải mã theo các bước:

- B1: A tính $S = W^{-1}C \text{ mod } M$.
(Tính W^{-1} bằng thuật toán O'clid mở rộng, hoặc lũy thừa liên tiếp, hoặc giải phương trình đồng dư).
- B2: Sử dụng thuật giải bài toán xếp ba lô trong trường hợp dãy siêu tăng để tính:

$$S = \sum_{i=1}^n m_i M_i$$

- Bản tin cần tìm là $\mathbf{m} = (m_1, m_2, \dots, m_n)$

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

Ví dụ:

Tạo khóa:

- B1: + A chọn ngẫu nhiên: $M_1 \in [1,16]$; $M_2 \in [17,32]$;
 $M_3 \in [33,64]$; $M_4 \in [113,128]$
+ Chọn dãy siêu tăng: $M_i = (5, 23, 57, 119)$; $\sum_{i=1}^4 M_i = 204$;
→ Chọn $M = 257$
- B2: Chọn một số ngẫu nhiên $W = 113$, $\rightarrow W^{-1} = W^{\varphi(M)-1} \bmod M$.
 $\rightarrow W^{-1} = 113^{255} \bmod 257 = 116$
- B3: Tính các $a_i \equiv W \cdot M_i \bmod M; i = 1..n$
 $a_1 = 113 \cdot 5 \bmod 257 = 51; \quad a_2 = 113 \cdot 23 \bmod 257 = 29$
 $a_3 = 113 \cdot 57 \bmod 257 = 16; \quad a_4 = 113 \cdot 119 \bmod 257 = 83$
- B4: + Khóa CK: $A = (a_1, a_2, a_3, a_4) = (51, 29, 16, 83)$
+ Khóa BM:
 $(M, W, \{M_1, M_2, M_3, M_4\}) = (257, 113, \{5, 23, 57, 119\})$

2.4. Bài toán xếp ba lô và hệ mật Merkle - Hellman

2.4.2. Hệ mật Merkle – Hellman

b) Mã hóa:

Giả sử B cần gửi bản tin $m = (1, 1, 0, 1)$ cho bên A

B1: B nhận khóa CK của A: $(51, 29, 16, 83)$

B2: B tính $C = \sum_{i=1}^4 m_i a_i = 1 \times 51 + 1 \times 29 + 0 \times 16 + 1 \times 83 = 163$

B3: B gửi bản mã $C = 163$ cho A.

c) Giải mã: A nhận bản mã C = 163 và giải mã:

B1: A tính $S = W^{-1}C \bmod M = 116 \cdot 163 \bmod 257 = 147$

B2: Sử dụng thuật giải bài toán xếp ba lô trong trường hợp dãy siêu tăng:

$$M_i = (5, 23, 57, 119)$$

+ $i = 4$

+ while $i \geq 1$ do

$$* 147 > 119 \rightarrow m_4 = 1; S = S - 119 = 147 - 119 = 28; i = 3$$

$$* 28 < 57 \rightarrow m_3 = 0; i = 2$$

$$* 28 > 23 \rightarrow m_2 = 1; S = 28 - 23 = 5; i = 1$$

$$* 5 = 5 \rightarrow m_1 = 1; S = 5 - 5 = 0; i = 0$$

+ Bản tin cần tìm: $m = (1, 1, 0, 1)$

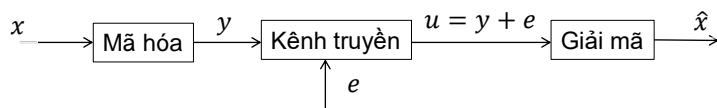
2.5. Bài toán mã sửa sai và hệ m^{át} McEliece

2.5.1. Mã tuyến tính C(n,k,d);

- + Ma trận sinh: $[G]_{k \times n}$
- + Ma trận kiểm tra: $[H]_{r \times n}$, với: $r = n - k$; và: $[G] * [H]^T = [0]$
- + Khoảng cách m^{át} là khoảng cách Hamming tối thiểu: d
với: $d = 2t + 1$; t số sai sửa được

• Một số phương pháp giải m^{át}:

1) Phương pháp “Người láng giềng gần nhất”

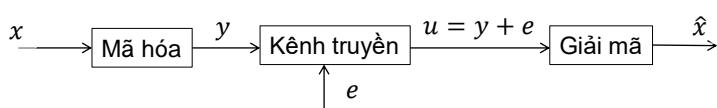


$$y = x \cdot G; \quad x \in (Z_2)^k; \quad y \in (Z_2)^n$$

- Tính 2^k vector đúng và so sánh với vector thu được u
→ Độ phức tạp theo hàm mũ, khi k lớn thì rất khó giải.

2.5. Bài toán m^{át} sửa sai và hệ m^{át} McEliece

2) Giải m^{át} theo syndrom:



Ta có: $s(y) = y \cdot H^T = 0 \rightarrow s(u) = s(e)$ (chú ý: $u = y + e$)

+ Khi giải m^{át}: nếu $s(u) = 0 \rightarrow$ không có lỗi và $u = y$

+ nếu $s(u) \neq 0 \rightarrow$ có sai:

Tạo lần lượt các vector sai e (1 bit) có trọng số bằng 1 và tính $s(e)$.

- Nếu $s(e) = s(u)$ thì $y = u + e$.

- Nếu không có vector e nào thỏa mãn thì tạo các vector e có trọng số lần lượt là 2,3,...,t. cho đến khi $s(e) = s(u)$.

2.5. Bài toán mã sửa sai và hệ mật Mc.Eliece

2.5.2. Hệ mật Mc. Eliece

Tạo khóa: Mỗi bên liên lạc tạo cho mình 1 cặp khóa CK-BM :

+ B1: Chọn một mã tuyến tính sửa sai (n, k, d) khuyến nghị $k = \frac{n}{2}$, có thuật toán giải mã hiệu quả, với ma trận sinh G . (Số lượng G nhiều).

+ B2: - Chọn ma trận hoán vị: P Tồn tại P^{-1} sao cho: $P.P^{-1} = I$.

(mỗi hàng và mỗi cột của P chỉ có một số “1”).

- Chọn ma trận khả nghịch: $S_{k \times k}$ Tồn tại S^{-1} với $S.S^{-1} = I$

+ B3: Tính $G' = S.G.P$

+ B4: Khóa CK: (G', t) (t là số sai khả sửa)

Khóa BM: (S, P, G)

2.5. Bài toán mã sửa sai và hệ mật Mc.Eliece

2.5.2. Hệ mật Mc. Eliece

• **Mã hóa:** B cần gửi bản tin $m \in (Z_2)^k$ cho A.

+ B1: Nhận khóa CK của A: (G', t)

+ B2: B tính: $y = m.G' = x.G'$ ($x = m$)

+ B3: B chọn $e \in (Z_2)^n$ thỏa mãn $W(e) \leq t$

+ B4: B tính $C = y + e$

+ B5: B gửi bản mã C cho bên A.

2.5. Bài toán mã sửa sai và hệ mật Mc.Eliece

2.5.2. Hệ mật Mc. Eliece

- Giải mã: A nhận bản mã C và giải mã

+ B1: A tính:

$$\begin{aligned}C.P^{-1} &= (y + e).P^{-1} = y.P^{-1} + e.P^{-1} \\&= x.G'.P^{-1} + eP^{-1} \\&= x.S.G.P.P^{-1} + e.P^{-1} = x.S.G + e.P^{-1} \\&= x'G + e.P^{-1}\end{aligned}$$

+ B2: Giải mã sửa sai để tìm x' .

+ B3: Tính $x = x'.S^{-1} = x.S.S^{-1} = x = m$

2.6. Đường cong Elliptic và các hệ mật có liên quan

a) Các thặng dư bậc 2

Định nghĩa: Xét \mathbb{Z}_p^* , nhóm nhán \mathbb{Z}_p^* có số phần tử $|\mathbb{Z}_p^*| = \varphi(p)$:

phần tử $a \in \mathbb{Z}_p^*$ được gọi là thặng dư bậc 2 (theo modulo) nếu $a \equiv x^2 \pmod{p}$, $x \in \mathbb{Z}_p^*$.

Có các phần tử không lấy căn bậc 2 được \rightarrow gọi là các thặng dư không bậc 2.

Q_p - tập các thặng dư bậc 2.
 \bar{Q}_p - tập các thặng dư không bậc 2. } Hiển nhiên: $Q_p \cup \bar{Q}_p = \mathbb{Z}_p^*$; $Q_p \cap \bar{Q}_p = \emptyset$

Định lý 1:

Với p - nguyên tố; α - phần tử nguyên thủy của \mathbb{Z}_p^* . Khi đó α^i là thặng dư bậc hai khi và chỉ khi i chẵn.

$$|Q_p| = \frac{p-1}{2}; \quad |\bar{Q}_p| = \frac{p-1}{2}$$

a. Các thặng dư bậc 2

Ví dụ: $p=11$; $\alpha=2$

i	1	2	3	4	5	6	7	8	9	10
i^2	1	4	9	5	10	9	7	3	6	1

$$Q_{11} = \{4, 5, 9, 3, 1\}; \quad \bar{Q}_{11} = \{2, 8, 10, 7, 6\}; \quad |Q_{11}| = |\bar{Q}_{11}| = 5$$

Chú ý: $a = x^2 \bmod p$ và $a = (p-x)^2 \bmod p$ vì: $(p-x)^2 = p^2 - 2px + x^2 = x^2$

$$(p^2 \bmod p = 0; 2px \bmod p = 0)$$

Do đó: $\sqrt{a} = \{x, p-x\}$

i	1	2	3	4	5	6	7	8	9	10
i^2	1	4	9	5	3	3	5	9	4	1

$$\text{Ta có: } \sqrt{1} = \{1, 10\}; \quad \sqrt{3} = \{5, 6\}; \quad \sqrt{4} = \{2, 9\}; \quad \sqrt{5} = \{4, 7\}; \quad \sqrt{9} = \{3, 8\}$$

a. Các thặng dư bậc 2

Bài tập: Cho Z_{13} , biết $\alpha = 2$ là phần tử nguyên thuỷ của Z_{13}^* .

Hãy tìm các thặng dư bậc 2 và các căn bậc hai của Q_{13}

Giải:

- Số các thặng dư bậc 2: $|Q_{13}| = \frac{13-1}{2} = 6$
- Các thặng dư bậc 2: $\{\alpha^i \bmod p, i = 2, 4, 6, 8, 10, 12\}$

$$Q_{13} = \{4, 3, 12, 9, 10, 1\}$$

- Các căn bậc 2:

i	1	2	3	4	5	6	7	8	9	10	11	12
i^2	1	4	9	3	12	10	10	12	3	9	4	1

$$\sqrt{1} = (1, 12); \quad \sqrt{4} = (2, 11); \quad \sqrt{9} = (3, 10)$$

$$\sqrt{3} = (4, 9); \quad \sqrt{12} = (5, 8); \quad \sqrt{10} = (6, 7)$$

a. Các thặng dư bậc 2

Định lý 2: Với $n = pq$ thì $a \in Q_n$ khi và chỉ khi $a \in Q_p$ và $a \in Q_q$

$$|Q_n| = \frac{(p-1)}{2} \times \frac{(q-1)}{2} = \frac{1}{4}(p-1)(q-1)$$

$$|\bar{Q}_n| = \frac{3}{4}(p-1)(q-1)$$

Định lý 3: Cho $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ với p_i - nguyên tố; e_i - nguyên dương.

Nếu $a \in Q_n$ thì a có đúng 2^k các căn bậc 2.

Ví dụ: $n = 315 = 5 \cdot 7 \cdot 3^2 \rightarrow k = 3$ có $2^3 = 8$ căn bậc 2.

xét $121 \in Q_{315}$ ta có: $\sqrt{121} = \{11, 74, 101, 151, 164, 214, 241, 304\}$

Các cặp tương ứng: $11+304=315$; $74+241=315\dots$

a. Các thặng dư bậc 2

Bài tập về nhà:

Tìm các thặng dư bậc 2 và các căn bậc hai của Z_p^* với:

+ $p = 17$; biết $\alpha = 3$ là phần tử nguyên thuỷ của Z_{17}^* .

+ $p = 19$; $\alpha = 2$ là phần tử nguyên thuỷ của Z_{19}^* .

b. Đường cong Elliptic

b) Đường cong Elliptic

- Định nghĩa: Đường cong Elliptic trên trường số thực có dạng:
 $y^2 + axy + by = x^3 + cx^2 + dx + e$ (a, b, c, d, e là các số thực)
- Định nghĩa: Đường cong Elliptic (dạng Weierstrass) trên trường hữu hạn Z_p ; p -nguyên tố

$$y^2 \equiv (x^3 + ax + b) \pmod{p} \quad a, b \in Z_p^*$$

Điều kiện tồn tại: $\Delta = (4a^3 + 27b^2) \pmod{p} \neq 0$

b. Đường cong Elliptic

Ví dụ: Cho đường cong Elliptic trên Z_{17} : $y^2 = x^3 + x + 1 \pmod{17}$

$$\Delta = 4 + 27 = 31 \pmod{17} \neq 0$$

-Phải xác định các thang dư bậc 2:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
i^2	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

$$\rightarrow Q_{17} = \{1, 4, 9, 16, 8, 2, 15, 13\}$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
y^2	1	3	11	14	1	12	2	11	11	8	8	0	7	1	5	8	16
$y^2 \in Q_{17}?$	Y	N	N	N	Y	N	Y	N	N	Y	Y	N	Y	N	Y	Y	
y_1	1				1		6			5	5	0		1		5	4
y_2	16				16		11			12	12	0		16		12	13

Ta có 18 điểm $P(x, y)$ tạo thành nhóm cộng cấp 18 như sau:

$$\{(0,1), (0,16), (4,1), (4,16), (6,6), (6,11), (9,5), (9,12), (10,5), (10,12), (11,0), (13,1), (13,16), (15,5), (15,12), (16,4), (16,13), 0\}$$

b. Đường cong Elliptic

* Nhóm cộng các điểm trên đường cong Elliptic

Các phần tử của nhóm: $P(x,y)$;

- Phần tử Zero: $0(\infty, \infty)$ (nằm ngoài tập hợp).

- Thỏa mãn các tính chất:

$$+ P + 0 = 0 + P = P$$

$$+ P + P = 2P$$

$$+ P + (-P) = 0$$

$$+ P(x,y) = -P(x,-y)$$

$$P(x_1, y_1) + Q(x_2, y_2) = K(x_3, y_3) \text{ trong đó:}$$

$$\begin{aligned} x_3 &= [\lambda^2 - x_1 - x_2] \bmod p \\ y_3 &= [\lambda(x_1 - x_3) - y_1] \bmod p \end{aligned} \quad \text{Với } \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p; & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \bmod p; & P = Q \end{cases}$$

b. Đường cong Elliptic

Ví dụ: xét đường cong Elliptic $y^2 = x^3 + ax + b \bmod p$

Xây dựng nhóm $E_p(a, b) = E_{17}(1, 1)$

Cấu trúc nhóm $E_p(a, b)$:

$$E_p(a, b) = \{P, 2P, 3P, \dots\}$$

Trong đó: $P(x, y)$ là phần tử nguyên thủy

* Xây dựng nhóm với phần tử nguyên thủy $P(0, 1)$; Chú ý:

$$\begin{aligned} x_3 &= [\lambda^2 - x_1 - x_2] \bmod p \\ y_3 &= [\lambda(x_1 - x_3) - y_1] \bmod p \end{aligned} \quad \text{Với } \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p; & P \neq Q \\ \frac{3x_1^2 + a}{2y_1} \bmod p; & P = Q \end{cases}$$

$$+ 2P = P + P \rightarrow \lambda = \frac{3 \cdot 0 + 1}{2 \cdot 1} = \frac{1}{2} = 2^{-1} = 9 \Rightarrow x_3 = 9^2 \bmod 17 = 13; y_3 = 1$$

$$\text{Vậy } 2P(13, 1)$$

b. Đường cong Elliptic

$$+ 3P = P + 2P \rightarrow \begin{cases} \lambda = 0 \\ x_3 = -13 = 4 \\ y_3 = -1 = 16 \end{cases} \rightarrow 3P(4,16)$$

+ Tính tương tự: $4P(9,12); 5P(16,4); 6P(10,12); 7P(6,6); 8P(15,12); 9P(11,0)$

Chú ý: điểm $10P(x,y) = -10P(x,-y) = 8P(x,-y)$

$$\Rightarrow 10P = 8P(15, -12) \Rightarrow 10P(15, 5) \quad (5=17-12)$$

$$\text{Do đó: } + 11P = 7P(x, -y) \Rightarrow 11P(6, -6) = 11P(6, 11)$$

$$+ 12P = 6P(x, -y) \Rightarrow 12P(10, -12) = 12P(10, 5)$$

- Tính tương tự có: $13P(16,13); 14P(9,5); 15P(4,1); 16P(13,16); 17P(0,16)$

$$+ 18P = 0 \text{ (thêm phần tử zero)}$$

Các điểm nguyên thủy: K thỏa mãn $(K, 18) = 1 \Rightarrow K = \{1, 5, 7, 11, 13, 17\}$

$$\Rightarrow P, 5P, 7P, 11P, 13P, 17P$$

c. Hệ mật Omura-Massey trên đường cong Elliptic

c. Hệ mật Omura-Massey trên đường cong Elliptic

Khóa công khai: $E_p(a, b)$

Khóa bí mật: + A chọn (m, n) với $m + n = \#E_p(a, b)$

+ B chọn (u, v) với $u + v = \#E_p(a, b)$

A cần truyền bản tin M cho B

+ A tính $mQ + M$ và gửi cho B \rightarrow B tính $(mQ + M) + uQ$ và gửi cho A

+ A tính:

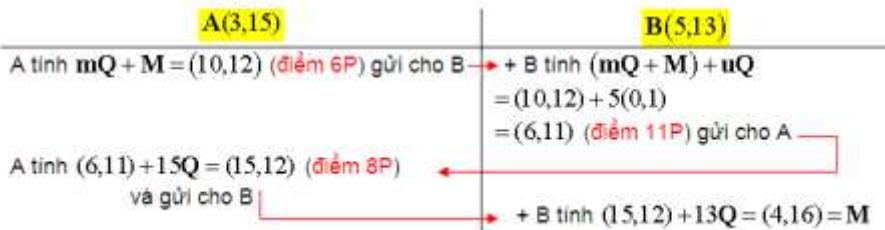
$$[(mQ + M) + uQ] + nQ = M + uQ \text{ gửi cho B} \rightarrow B \text{ tính } [M + uQ] + vQ = M$$

c. Hệ mật Omura-Massey trên đường cong Elliptic

Ví dụ: Khóa công khai: $E_{17}(1,1)$; Chọn: $Q(0,1)$ (điểm P)

Bản tin: $M(4,16)$ (Điểm $3P$)

Khóa bí mật: + A chọn $(m,n) = (3,15)$; B chọn $(u,v) = (5,13)$



d. Hệ mật Elgamal trên đường cong Elliptic

d. Hệ mật Elgamal trên đường cong Elliptic

* **Tạo khóa:** Mỗi bên liên lạc tạo cho mình một cặp khóa công khai - bí mật.

Chọn $E_p(a,b)$ và điểm nguyên thủy P .

Chọn a ($1 < a < \#E_p(a,b) - 1$) ngẫu nhiên; và tính $aP = Q$.

+ Khóa công khai: $(E_p(a,b); P; Q)$; Khóa bí mật: a

* **Mã hóa:** Giả sử B cần gửi bản tin M cho A.

+ B1: B nhận khóa công khai của A là $(E_p(a,b); P; Q)$

+ B2: B chọn k ngẫu nhiên và tính: $\gamma = kP$; $\delta = M + kQ$

+ B3: B gửi bản mã $C = (\gamma, \delta)$ cho A.

* **Giải mã:** + B1: A nhận $C = (\gamma, \delta)$.

+ B2: A tính $a\gamma = akP = kQ$

A tính: $M = \delta - kQ = M + kQ - kQ = M$

d. Hệ mật Elgamal trên đường cong Elliptic

Ví dụ: $E_{17}(1,1)$; $P(0,1)$; $M = (4,16)$ (điểm $3P$).

* Tạo khóa của A:

A chọn $a = 3$ và tính $aP = Q = (4,16)$ (điểm $3P$).

+ Khóa công khai: $(E_{17}(1,1); (0,1); (4,16))$; Khóa bí mật: $a = 3$

* Mã hóa: B cần gửi bản tin $M = (4,16)$ cho A.

+ B chọn $k = 5$ và tính: $\gamma = kP = (16,4)$; (Điểm $5P$)

$$\delta = M + kQ = (0,0) \text{ (Điểm } 18P\text{)}$$

+ B gửi bản mã $C = ((16,4), (0,0))$ cho A.

* Giải mã: + A nhận $C = ((16,4), (0,0))$.

+ A tính $a\gamma = 5(16,4) = (4,1)$ (điểm $15P$)

A tính: $M = \delta - a\gamma = (4,16)$ (18P-15P = 3P = M)

2.5. Ưu và nhược điểm của hệ mật khóa công khai

2.5. Ưu và nhược điểm của hệ mật khóa công khai

- Ưu điểm:**
- + Không sử dụng kênh an toàn (đây là nhược điểm của hệ mật khóa bí mật)
 - + Dễ bảo vệ, lưu trữ và sinh khóa.
 - + Dễ tạo các dịch vụ an toàn khác.

Ví dụ: Với n người dùng:

	Số khóa cần tạo	Số khóa cần lưu giữ bí mật
Hệ mật khóa bí mật	$\frac{n(n-1)}{2}$	$(n-1)$
Hệ mật khóa công khai	$2n$	1

Nhược điểm: + Phức tạp (với trường số lớn thi phần cứng phức tạp)

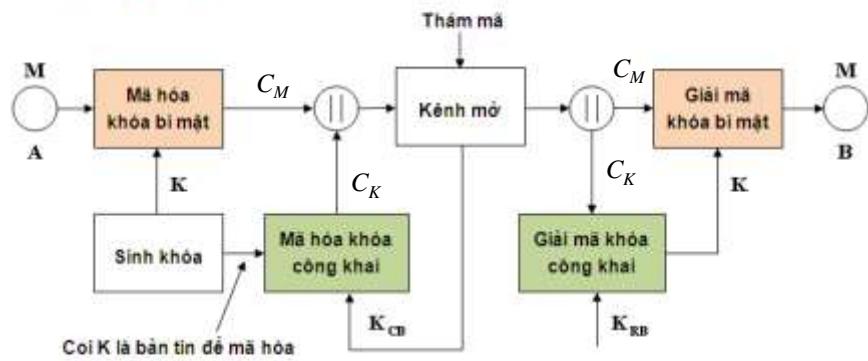
+ Hiệu quả không cao

→ Khó thực hiện các dịch vụ nhạy cảm đối với độ trễ và dịch vụ di động.

2.6. Xây dựng các chương trình ứng dụng kiến trúc PGP

2.6. Xây dựng các chương trình ứng dụng kiến trúc PGP

(Pretty Good Privacy- Riêng tư tốt đẹp)



- Sử dụng mã hóa công khai để truyền khóa bí mật.
- Bản tin sử dụng hệ mật mã khóa bí mật để truyền



BÀI GIẢNG

CƠ SỞ MẬT MÃ HỌC

Giảng viên: TS. Ngô Đức Thiện

Điện thoại: 0912.928.928

E-mail: thienptit@gmail.com

Bộ môn: Xử lý tín hiệu và Truyền thông - Khoa KTDT1

Bài giảng: Cơ sở mật mã học

CHƯƠNG III

HÀM BĂM, XÁC THỰC VÀ CHỮ KÝ SỐ

3. 1. Hàm băm

3.1.1. Định nghĩa hàm băm

Hàm băm là một ánh xạ $h(x)$ thỏa mãn hai tính chất:

- Tính chất nén.
- Tính chất dễ tính toán.

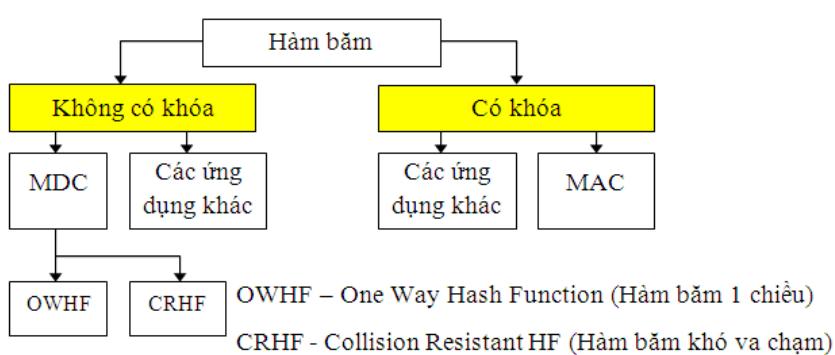
3.1.2. Định nghĩa hàm băm mật mã

Hàm băm mật mã là một hàm băm thỏa mãn các tính chất sau:

- Tính chất nén
- Tính chất dễ tính toán
- Khó tìm nghịch ảnh. Tức là biết x thì dễ dàng tính $y = h(x)$, nhưng nếu biết y rất khó tìm được $x = h^{-1}(y)$.
- Khó tìm nghịch ảnh thứ hai: Biết x khó xác định $x' \neq x$ sao cho: $h(x) = h(x')$.
- Khó va chạm: Khó xác định cặp x và x' để $h(x) = h(x')$.

3. 1. Hàm băm

3.1.3. Phân loại hàm băm



MDC: Manipulation Detection Code: Mã phát hiện sửa đổi.

MAC: Message Authentication Code: Mã xác thực thông báo.

3. 1. Hàm băm

- Một số hàm băm họ MD4

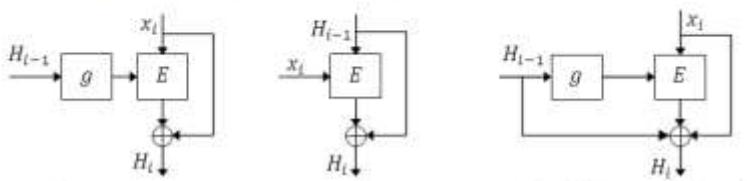
	Độ dài từ w (theo bit)	Các thanh ghi	Độ dài đầu ra n(m) (theo bit)	Các bước s
MD4	32	4	$4 \cdot 32 = 128$	$3 \cdot 16 = 48$
Ext.MD4	32	2×4	$8 \cdot 32 = 256$	2×48
MD5	32	4	$4 \cdot 32 = 128$	$4 \cdot 16 = 64$
RIPEMD-0 (*)	32	2×4	$4 \cdot 32 = 128$	2×48
RIPEMD-128	32	2×4	$4 \cdot 32 = 128$	2×64
RIPEMD-160	32	2×5	$5 \cdot 32 = 160$	2×80
RIPEMD-256	32	2×4	$8 \cdot 32 = 256$	2×64
RIPEMD-320	32	2×5	$10 \cdot 32 = 320$	2×80
SHA-0 (*)	32	5	$5 \cdot 32 = 160$	80
SHA-1	32	5	$5 \cdot 32 = 160$	80
SHA-224	32	8	$7 \cdot 32 = 224$ ($8 \cdot 32 = 256$)	64
SHA-256	32	8	$8 \cdot 32 = 256$	64
SHA-384	64	8	$6 \cdot 64 = 384$ ($8 \cdot 64 = 512$)	64
SHA-512	64	8	$8 \cdot 64 = 512$	80

3. 2. Các phương pháp xây dựng hàm băm

3.2.1. MDC

a) MDC độ dài đơn

(Dựa trên việc sử dụng lập các thuật toán mật mã)



a) Sơ đồ Matyas-Mayer-Oseas

b) Sơ đồ Davies-Mayer

c) Sơ đồ Miyaguchi - Preneel

Đầu vào: gồm m khối $x = (x_1, x_2, \dots, x_m)$ có độ dài cố định.

Đầu ra: $h(x) = H_M$ (lấy giá trị băm ở bước cuối cùng)

$H_0 = IV$ (Init Vector) giá trị khởi đầu.

g : Ánh xạ lựa chọn bit.

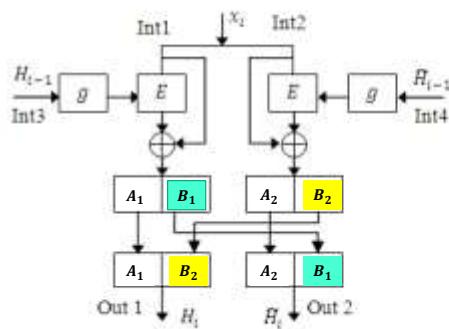
E : là các mật mã khối: nếu dùng DES thì đầu ra 64 bit và khóa là 56 bit

3.2. Các phương pháp xây dựng hàm băm

b) MDC độ dài kép (MDC-2)

Trước đây khi dùng DES với độ dài đầu ra 64 bit là đảm bảo an toàn.

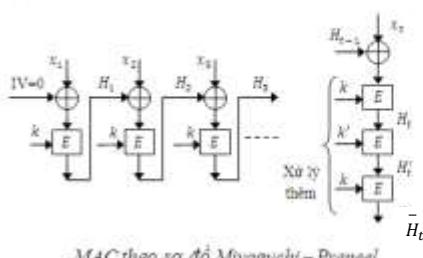
Tuy nhiên với khả năng tấn công của thám mã hiện tại thì không đảm bảo nữa, do đó phải tăng độ dài hàm băm.



Sơ đồ MDC-2 (độ dài tăng gấp đôi)

3.2. Các phương pháp xây dựng hàm băm

c) MAC



MAC theo sơ đồ Miyaguchi-Preneel.

Vào: Dữ liệu x , mật mã khối E , khóa MAC bí mật k của E .

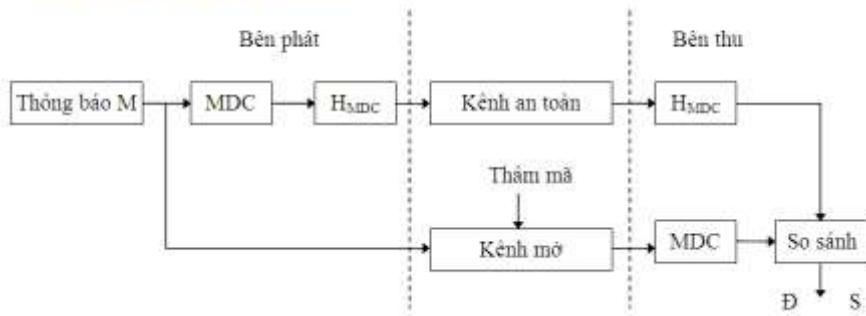
Ra: n bit MAC trên x (n là độ dài khối của E)

- (1) Độn và chia khối: Độn thêm các bit vào x nếu cần. Chia dữ liệu đã độn thành t khối, mỗi khối n bit: x_1, x_2, \dots, x_t .
- (2) Xử lý theo chế độ CBC.
- (3) Xử lý thêm để tăng sức mạnh của MAC: Dùng thêm khóa $k' \neq k$
- (4) Kết thúc: MAC là khối n bit \bar{H}_t .

3.3. Một số sơ đồ xác thực nội dung thông báo

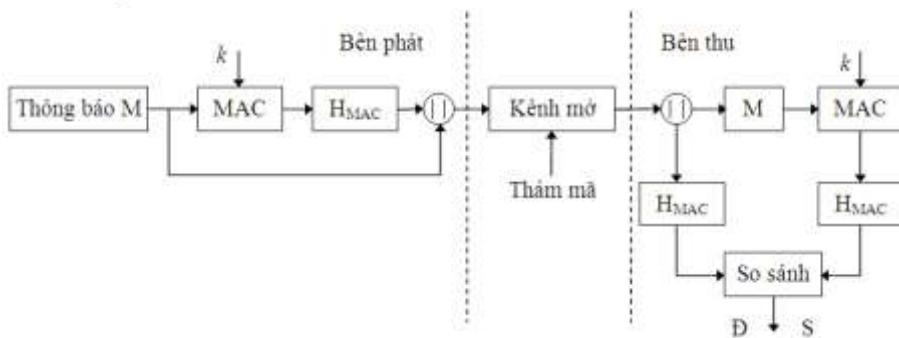
Trong thực tế có các thông báo cần công khai nhưng phải đảm bảo nội dung chính xác.

3.3.1. Dùng MDC và kênh an toàn



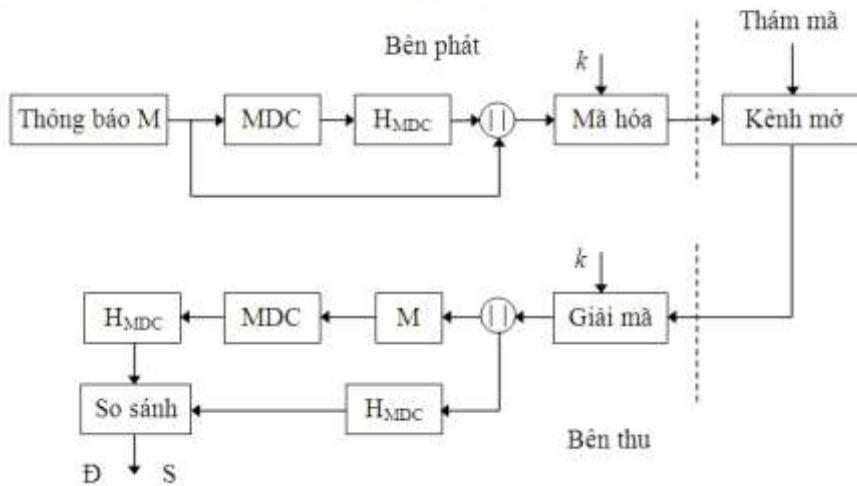
3.3. Một số sơ đồ xác thực nội dung thông báo

3.3.2. Dùng MAC



3.3. Một số sơ đồ xác thực nội dung thông báo

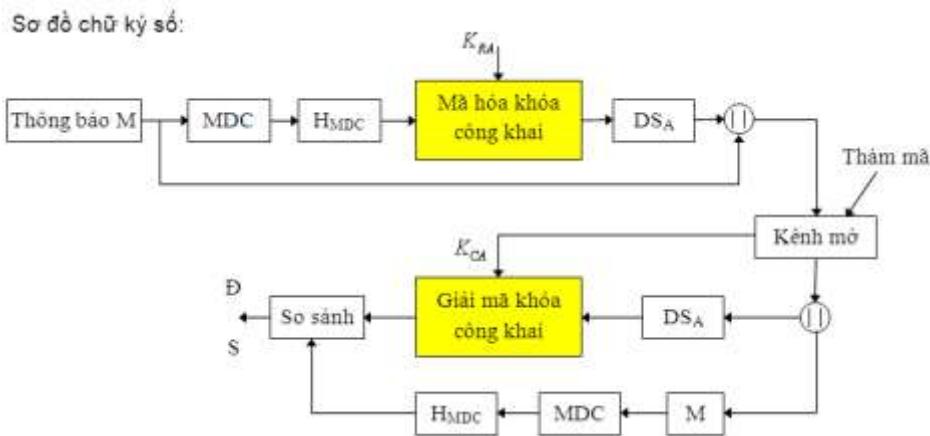
3.3.3. Dùng MDC và thuật toán mật mã



3.4. Chữ ký số (Digital Signature – DS)

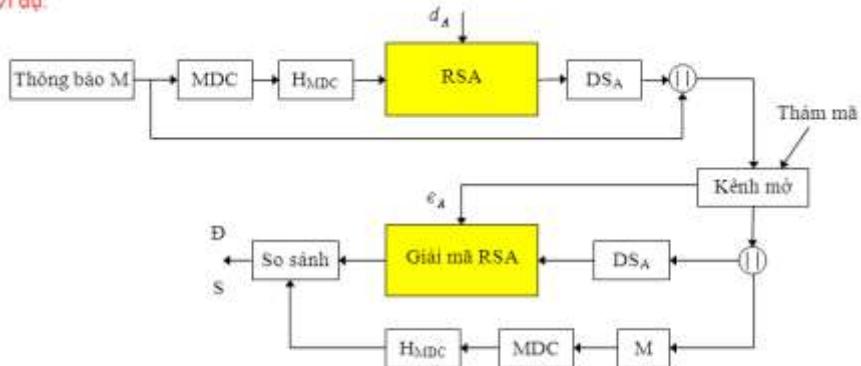
- Chữ ký tay phải đảm bảo yêu cầu:
 - + Ngắn gọn (ngắn hơn văn bản)
 - + Đại diện duy nhất.
 - + Khó bắt chước.
- Khi làm việc qua mạng, do không gặp trực tiếp nên phải dùng chữ ký điện tử và nó cũng thỏa mãn các yêu cầu như chữ ký tay.
- Tuy nhiên: Chữ ký số gắn với từng văn bản.
- Nếu dùng hàm băm:
 - + Không khóa \rightarrow ai cũng làm được
 - + Có khóa: phải trao đổi khóa \rightarrow giả mạo được.

3.4. Chữ ký số (Digital Signature – DS)



3.4. Chữ ký số (Digital Signature – DS)

Ví dụ:



Mã hóa:

$$\begin{aligned}
 &+ h_{MDC} = h(m) \\
 &+ DS_A = h(m)^{d_A} \bmod n_A \\
 &+ ghép với thông báo: m || DS_A
 \end{aligned}$$

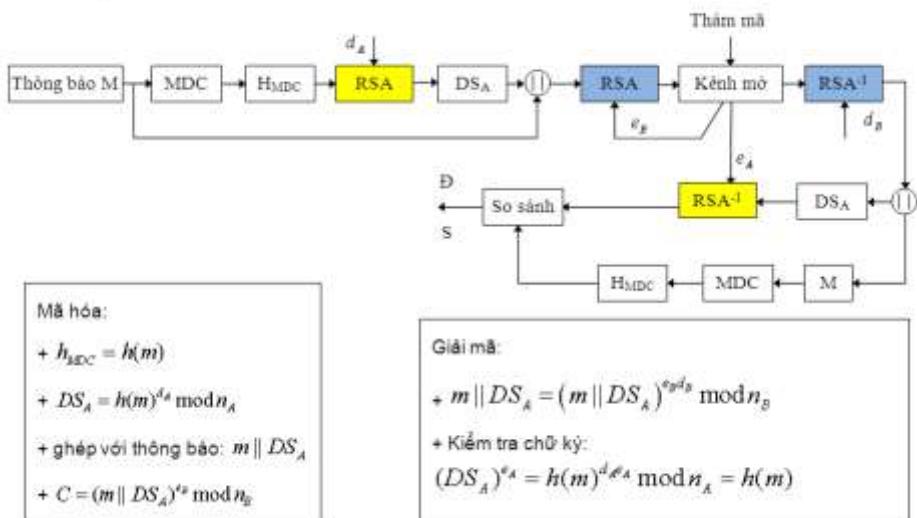
Giải mã: $h(m) = (h^{d_A}(m))^{e_A} \bmod n_A$

(Dùng d_A mã hóa; e_A giải mã)

Sơ đồ này không bảo mật

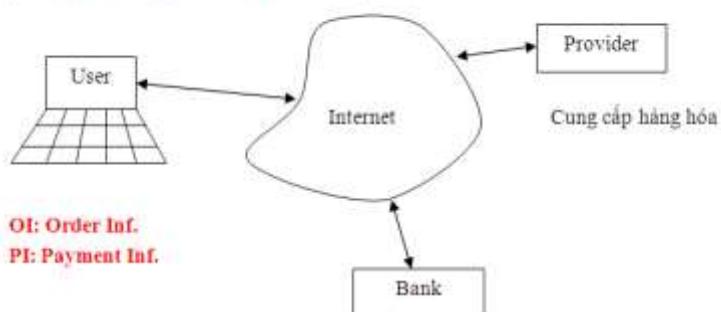
3. 4. Chữ ký số (Digital Signature – DS)

Ví dụ: Chữ ký RSA có bảo mật



3. 5. Chữ ký số kép (Double DS) trong giao dịch điện tử an toàn

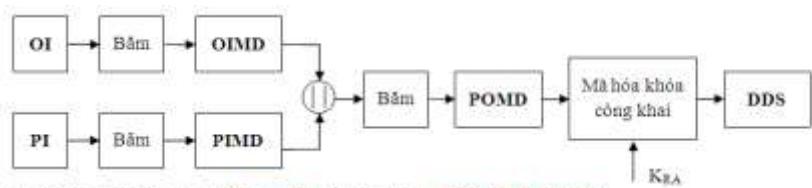
(SET – Secure Electronic Transaction)



User: chỉ muốn trao cho ngân hàng PI và cho nhà cung cấp OI.

→ Giao dịch không thể thành công. Để giao dịch được phải cung cấp thông tin để kiểm tra
(Tối thiểu và đảm bảo tin cậy)

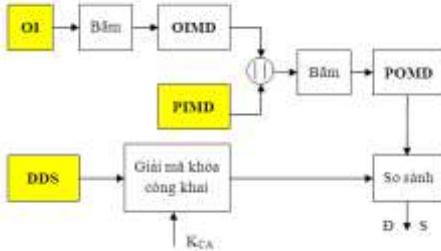
3.5. Chữ ký số kép (Double DS) trong giao dịch điện tử an toàn



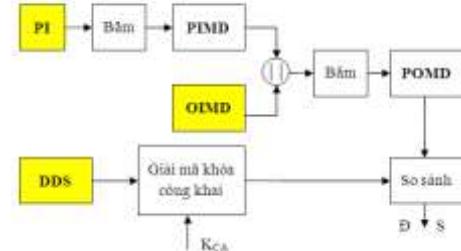
+ USER gửi tới Provider: OI; PIMD (Hashed băm PI); DDS (Chữ ký kép)

+ USER gửi tới Ngân hàng: PI; OIMD (Hashed băm OI); DDS

Nhà cung cấp kiểm tra:



Ngân hàng kiểm tra:



3.5. Chữ ký số kép (Double DS) trong giao dịch điện tử an toàn

- Khi mua hàng nếu không xem hàng có thể bị lừa đảo, nhưng có thể kiện được vì các thông tin về đơn hàng và chi trả các bên đều có ràng buộc.
- Giao dịch trên mạng vẫn có rủi ro, nhưng so với tiện ích sử dụng thì vẫn thấp hơn.

3. 6. Bài toán “Tấn công ngày sinh nhật”

- Khi sd hàm băm → có va chạm → y/c phải sd các hàm băm có xác suất va chạm nhỏ.
- Bài toán: Tấn công ngày sinh nhật: Lớp A có k sinh viên → hãy tìm xác suất để có ít nhất 2 SV cùng ngày sinh (giả sử số ngày trong 1 năm là $n = 365$ ngày).

$$P(n, k) \geq 1 - \exp\left\{-\frac{k(k-1)}{2n}\right\}$$

- Tìm k để $P = \frac{1}{2}$

$$k \leq \sqrt{2n \cdot \ln 2}$$

$$P(365, 23) \approx 0,5000175218271$$

Để giảm XS va chạm, → tăng n. Áp dụng vào các hàm băm.

Ví dụ: sử dụng AES trong hàm băm, $n = 2^{128}$, số các vector để có khả năng $h(x) = h(x')$ (xác suất va chạm $p = \frac{1}{2^{128}}$)

$$k \leq \sqrt{2 \cdot 2^{128} \ln 2} = 2,1791 \cdot 10^{19} \sim 2^{60}$$

Chương 4: Mật mã ngụy trang

Chương 4: Mật mã ngụy trang

(**Steganography**, Hidden Crypto)

1. Khái niệm về steganography

- Có từ lâu đời.
- Các phương pháp:
 - Hóa học: Mực vô hình: Xử lý nhiệt để hiện nội dung, vật mang có thể quyển sách, báo.
 - Vật lý: + Đánh dấu ký tự hoặc châm lỗ lên trên bài báo.
 - Phương pháp số: giấu tt vào các nội dung số có định dạng phổ biến: (file âm thanh, hình ảnh...gọi là các file nền).
- Mục tiêu của ngụy trang: tránh sự chú ý tò mò của đối phương.

Chương 4: Mật mã ngụy trang

2. Kỹ thuật Thủy vân, bóng mờ

- Sử dụng trong bản quyền số.
- Chèn thông tin bản quyền vào nội dung số.