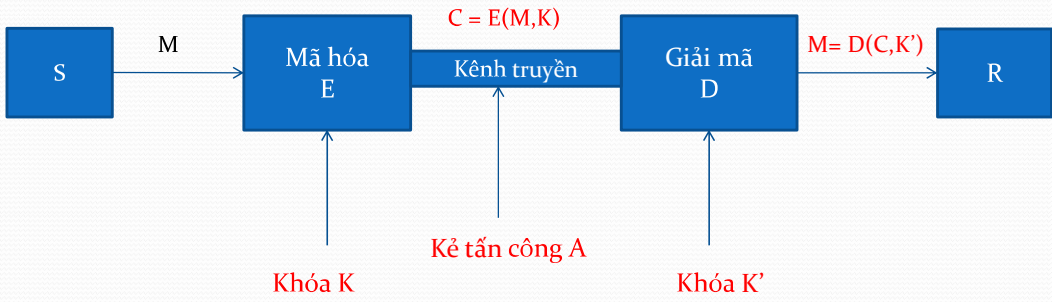
Chương 2- Cơ sở mật mã

2.1 Các khái niệm cơ bản

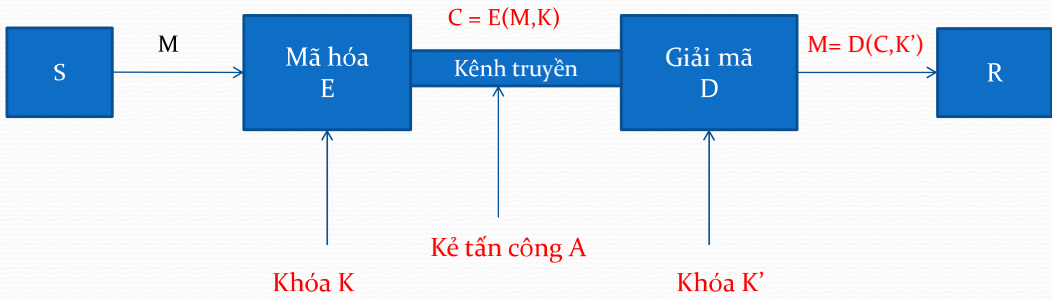
- Mật mã (Cryptology) là lĩnh vực
- Thuật ngữ Cryptology xuất phát từ krypto, trong tiếng Hy Lạp nghĩa là "che giấu"
- Mật mã bao gồm 2 lĩnh vực con
  - Lập mã (Cryptography): sáng tạo ra
  - Thám mã (Cryptanalysis): nghiên cứu các kỹ thuật phân tích để phá vỡ cơ chế lập mã, tiết lộ bí mật của thông tin đã được mã hóa

A) Mô hình truyền tin mật mã cơ bản (GTATTT 1.1.2)



Bài toán bảo mật truyền tin

- S cần truyền bản tin M cho R trong điều kiện kênh truyền tin giữa S và R có thể bị tấn công bởi A.
- Mục tiêu:
- Giải pháp:
  - 1. Sử dụng phép mã hóa E biến M thành C.
  - 2. Chuyển C qua kênh truyền
  - 3. Sử dụng phép giải mã D biến C thành M



- Trong sơ đồ, khóa K là tham số quan trọng
- Kẻ tấn công A được xem như biết phép mã hóa E và giải mã D nhưng **không biết khóa K**
- Do đó, khóa K giữ một vai trò

Một số thuật ngữ và ký hiệu viết tắt

- M: bản rõ (plaintext)
- C: bản mã (ciphertext)
- E: phép mã hóa (encryption)
- D: phép giải mã (decryption)
- K: khóa (key)
- **Hệ mật mã (cryptosystem)**: là một hệ thống bao gồm

- Căn cứ vào đặc tính và cách tổ chức quản lý khóa K, có hai loại hệ mật mã khác nhau
  - Hệ mật mã khóa đối xứng (Symmetric Key Cryptosystem)
  - Hệ mật mã khóa công khai (Public Key Cryptosystem)

B. Độ bảo mật của hệ mật mã

- Độ bảo mật (hay độ an toàn) của hệ mật mã là khả năng
- Mục tiêu thám mã:
- Mức độ bảo mật được đánh giá thông qua
  - Chứng minh bằng toán học
  - Thử nghiệm tấn công thám mã vào hệ mật mã

- Độ an toàn được xác nhận nếu
  - Chứng minh được độ khó của mật mã thỏa mãn điều kiện đặt ra.
  - Thử nghiệm tấn công mà không phá vỡ được mật mã trong điều kiện cho phép

Các mô hình đánh giá mức độ bảo mật hiện nay

- **1. Bảo mật vô điều kiện** (tuyệt đối): kẻ tấn công dù thu thập được tất cả bản mã và bản rõ trước đây, đồng thời có năng lực tính toán vô tận cũng
- **2. Bảo mật chứng minh được** : chứng minh được cụ thể mức độ phức tạp của việc thám mã tương đương

- **3. Bảo mật thực tế:** Không chứng minh bằng toán học nhưng

Ví dụ: sau khi thử nghiệm cho thấy siêu máy tính mạnh nhất với các dạng thám mã từ thấp đến cao cần khoảng 10000 năm mới phá vỡ được mật mã.

Do đó, có thể xem như đạt độ an toàn thực tế

- Mô hình số 1 chỉ mang tính tham chiếu vì không thực tế
- Mô hình số 2 phù hợp với các hệ mật mã dựa trên lý thuyết số (toán học)
- Mô hình số 3 mang tính thực nghiệm và phù hợp với mọi hệ mật mã

Các tiêu chí lựa chọn hệ mật mã

- 1) Mức độ an toàn
- 2) Có hiệu quả
  - Có thể cài đặt phép mã hóa và giải mã trên hardware / software
  - Tốc độ xử lý của thuật toán mã hóa đạt yêu cầu thực tế.

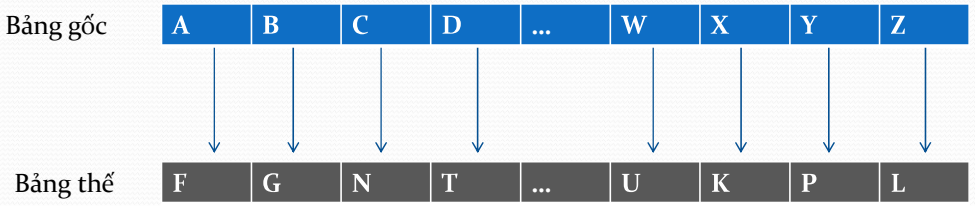
2.2 Một số hệ mật mã cổ điển

- Lịch sử mật mã được chia thành 2 thời kỳ
  - Mật mã cổ điển: xuất hiện từ trước Công nguyên cho đến cuối thế kỷ 19
  - Mật mã hiện đại: trở thành 1 ngành khoa học chính thức từ giữa thế kỷ 20
- Kỹ thuật mã hóa điển hình của mật mã cổ điển

A. Mã hóa bảng thế tổng quát

- Cách mã hóa:

- Ví dụ: Cho bản rõ M= "A DAY", sử dụng bảng thế dưới đây thu được bản mã



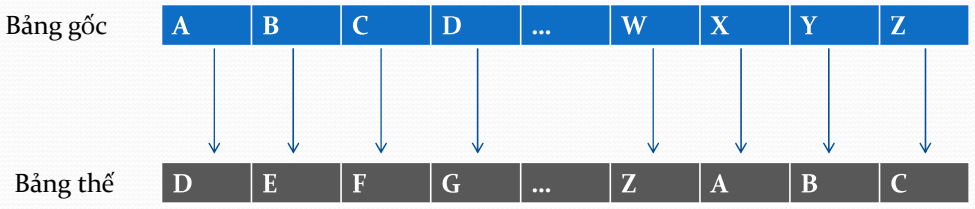
- Mỗi một bảng thế chính là

- Với bảng chữ cái gồm 26 kí tự, tổng số khóa K có thể có là bao nhiêu ?

B. Mã Ceasar

- Do hoàng đế La Mã Julius Ceasar tạo ra.

- Bảng thế là bảng chữ cái



Đặc điểm mã Ceasar

- Mã Ceasar được gọi là mã cộng (additive cipher) theo cách như sau
- Gán cho mỗi chữ cái 1 giá trị số tương ứng. Ví dụ: A là 0, B là 1,...

A	0
B	1
C	2
D	3
E	4
...	...
Z	25

Công thức mã hóa

m: kí tự của bản rõ M
c: kí tự của bản mã C

Công thức giải mã

A	0
B	1
C	2
D	3
E	4
…	…
Z	25

- Ví dụ mã hóa kí tự B
  - m= 1
- Ví dụ giải mã kí tự E
  - c = 4
  -

A	0
B	1
C	2
D	3
E	4
…	…
Z	25

- Biến thể của mật mã Ceasar là
- Do chỉ sử dụng 1 bảng thế nên
  sẽ giữ nguyên trong bản mã

Mã hóa và giải mã Ceasar

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
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

- Mã hóa bản tin “HELLO IT WORLD” bằng mã Ceasar (K = 3)
- Mã hóa bản tin “SECURITY” với mã Ceasar khi K = 15

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
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

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
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

- Giải mã bản tin “CKKZFKX” biết K = 22

Thám mã

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

- Hãy thám mã khi chỉ biết bản mã C= “DZRX SN AQDZJ”. Tìm M và K.

C. Mã Vigenere

- Do một nhà ngoại giao người Pháp tên là Blaise de Vigenère sống ở thế kỷ 14 tạo ra
- Là một dạng mật mã bảng thế phát triển từ mã Ceasar
- Cải tiến:

Mã Vigenere

- Sử dụng 26 bảng thế, mỗi bảng thế là

	A	B	C	D	...	W	X	Y	Z
0	A	B	C	D	...	W	X	Y	Z
1	B	C	D	E	...	X	Y	Z	A
2	C	D	E	F	...	Y	Z	A	B
3	D	E	F	G	...	Z	A	B	C
...									
22	W	X	Y	Z	...	S	T	U	V
23	X	Y	Z	A	...	T	U	V	W
24	Y	Z	A	B		U	V	W	X
25	Z	A	B	C	...	V	W	X	Y

bảng thế ứng với kí tự B và dịch 1 vị trí

Cách mã hóa

- Chọn khóa K là một chuỗi kí tự bất kỳ. VD: K= “BBC”
- Cho bản rõ M= “A NICE DAY”
- Cách chọn bảng thế theo khóa K

Khóa K	B	B	C	B	B	C	B	B
Bản rõ M	A	N	I	C	E	D	A	Y
Bảng thế	1	1	2	1	1	2	1	1
Bản mã C								

Đặc điểm của Vigenere

- Mở rộng không gian khóa K so với mã Ceasar
- Nếu độ dài khóa K là n thì số lượng khóa K là bao nhiêu ?
- Do sử dụng nhiều bảng thế nên tần suất xuất hiện của kí tự

Mã hóa Vigenere

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

- Cho M = “INFORMATION” , K = “KEY”, mã hóa M để thu được C

Khóa K											
Bản rõ M	I	N	F	O	R	M	A	T	I	O	N
Bảng thế											
Bản mã C											

Giải mã Vigenere

- Cho C = “UEMHY GZYL UG” , K = “HARD”, giải mã C để thu được M

Khóa K											
Bản mã C	U	E	M	H	Y	G	Z	Y	L	U	G
Bảng thế											
Bản rõ M											

D. Mã Vernam

- Do kỹ sư và nhà mật mã người Mỹ, Gilbert Vernam tạo ra vào đầu thế kỉ 20
- Đóng góp lớn cho

Mã Vernam sử dụng bảng thế

- **Trường hợp mã hóa bản tin kí tự,** mã Vernam
- Sử dụng khóa K

Khóa K: R A H T W N S Z (ngẫu nhiên)
Bản tin M: S E C U R I T Y
Bản mã C:

Mã Vernam sử dụng phép XOR bit

- **Trong trường hợp mã hóa,** thao tác mã hóa
- Khóa K

khóa K: 1 1 0 0 1 0 0 0
bản tin M: 1 1 1 1 0 1 0 1
bản mã C:

Tiếp

- **Trong trường hợp giải mã,**

khóa K: 1 1 0 0 1 0 0 0
bản mã C: 0 0 1 1 1 1 0 1
bản tin M:

Đặc điểm chính

- Khóa K sinh ngẫu nhiên và chỉ sử dụng 1 lần (không lặp lại) với mọi bản tin M
- Mã Vernam đạt đến
- Mã Vernam còn có tên gọi