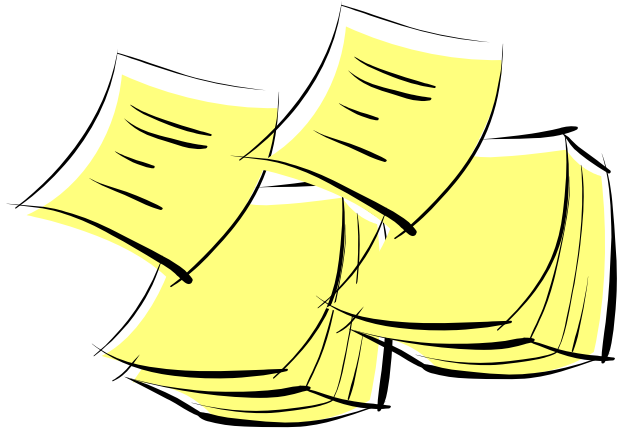


CHƯƠNG II

Mã đối xứng (cổ điển)

II.1 Mở đầu

- Mã hoá cổ điển là phương pháp mã hoá đơn giản nhất xuất hiện đầu tiên trong lịch sử ngành mã hoá.
- Thuật toán đơn giản và dễ hiểu.
- Những phương pháp mã hoá này là cở sở cho việc nghiên cứu và phát triển thuật toán mã hoá đối xứng được sử dụng ngày nay.
- Trong mã hoá cổ điển có hai phương pháp nổi bật đó là:
  - **Mã hoá thay thế**
  - **Mã hoá hoán vị**
- Mọi mã cổ điển đều là mã đối xứng

II.1 Mã đối xứng

II.1.1 Các khái niệm cơ bản

- Mật mã đối xứng sử dụng cùng một khóa cho việc mã hóa và giải mã. Có thể nói mã đối xứng là mã một khoá hay mã khóa bí mật hay mã khoá thỏa thuận
- Giả sử X là văn bản cần mã hóa và Y là dạng văn bản đã được thay đổi qua việc mã hóa

$$Y = E_K(X) \qquad X = D_K(Y)$$

  - **Khoá chung K**
  - **E là hàm biến đổi bản rõ thành bản mã**
  - **D là hàm biến đổi bản mã trở về bản rõ.**

Các khái niệm cơ bản

- Thông tin về khóa được chia sẻ giữa người gửi và người nhận.
- Mã đối xứng là kiểu duy nhất trước khi phát minh ra khoá mã công khai (còn được gọi là mã không đối xứng) vào những năm 1970.
- Hiện nay các mã đối xứng và công khai tiếp tục phát triển và hoàn thiện. Mã công khai ra đời hỗ trợ mã đối xứng chứ không thay thế nó, mã đối xứng đến nay vẫn được sử dụng rộng rãi.

Thuật ngữ về mã hóa

1. **Bản rõ** X được gọi là là bản tin gốc. Bản rõ có thể được chia nhỏ có kích thước phù hợp.
2. **Bản mã** Y là bản tin gốc đã được mã hoá. Ở đây ta thường xét phương pháp mã hóa mà không làm thay đổi kích thước của bản rõ, tức là chúng có cùng độ dài.
3. **Mã** là thuật toán E chuyển bản rõ thành bản mã. Thông thường chúng ta cần thuật toán mã hóa mạnh, cho dù kẻ thù biết được thuật toán, nhưng không biết thông tin về khóa cũng không tìm được bản rõ.

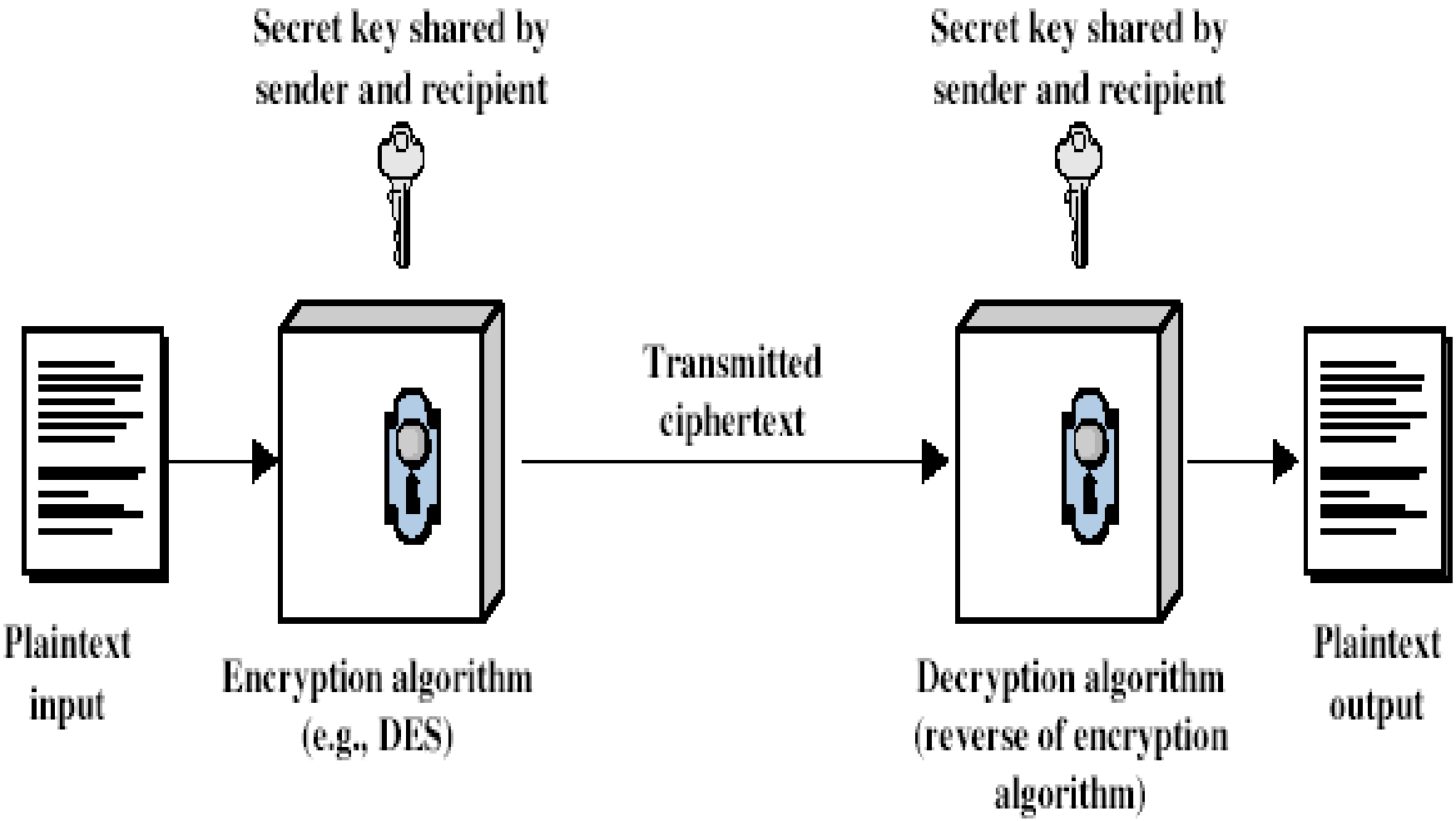
Thuật ngữ về mã hóa

4. **Khoá** K là thông tin tham số dùng để mã hoá, chỉ có người gửi và người nhận biết. Khóa là độc lập với bản rõ và có độ dài phù hợp với yêu cầu bảo mật.
5. **Mã hoá** là quá trình chuyển bản rõ thành bản mã, thông thường bao gồm việc áp dụng thuật toán mã hóa và một số quá trình xử lý thông tin kèm theo.
6. **Giải mã** chuyển bản mã thành bản rõ, đây là quá trình ngược lại của mã hóa.

Thuật ngữ về mã hóa

7. **Mật mã học** là chuyên ngành khoa học của Khoa học máy tính nghiên cứu về các nguyên lý và phương pháp mã hoá. Hiện nay người ta đưa ra nhiều chuẩn an toàn cho các lĩnh vực khác nhau của công nghệ thông tin.
8. **Thám mã** nghiên cứu các nguyên lý và phương pháp giải mã thường là không biết khóa. Thông thường khi đưa các mã mạnh ra làm chuẩn phổ biến công khai các mã đó được các kẻ thám mã cũng như những người phát triển mã tìm hiểu nghiên cứu.
9. **Lý thuyết mã** bao gồm cả mật mã và thám mã để đánh giá một mã mạnh hay không.

Mô hình mã đối xứng



II.1.2 Các yêu cầu

- Một mã đối xứng có các đặc trưng là cách xử lý thông tin của thuật toán mã hóa, giải mã, tác động của khóa vào bản mã, độ dài của khóa.
- Mối liên hệ giữa bản rõ, khóa và bản mã thông qua thuật toán càng phức tạp càng tốt.

Các yêu cầu

- Cụ thể hai yêu cầu để sử dụng an toàn mã khoá đối xứng là
  - **Thuật toán mã hoá mạnh: Có cơ sở toán học vững chắc đảm bảo rằng dù công khai thuật toán, nhưng việc thám mã là rất khó khăn và phức tạp nếu không biết khóa.**
  - **Khoá được giữ bí mật:**
    - **Chỉ có người gửi và người nhận biết.**
    - **Có kênh an toàn để phân phối khoá giữa các người sử dụng chia sẻ khóa.**
    - **Mối liên hệ giữa khóa và bản mã là không nhận biết được.**

II.1.3 Mật mã

Hệ mật mã được đặc trưng bởi các yếu tố sau

- Kiểu của thao tác mã hoá được sử dụng trên bản rõ:
  - **Phép thế: thay thế các ký tự trên bản rõ bằng các ký tự khác**
  - **Hoán vị: thay đổi vị trí các ký tự trong bản rõ, tức là thực hiện hoán vị các ký tự của bản rõ.**
  - **Tích: của chúng, tức là kết hợp cả hai kiểu thay thế và hoán vị các ký tự của bản rõ.**

Mật mã (tt)

- Số khoá được sử dụng khi mã hóa:
  - **Một khoá duy nhất: khoá riêng**
  - **Hai khoá: khoá công khai.**
- Cách mà bản rõ được xử lý, theo:
  - **Khối: dữ liệu được chia thành từng khối có kích thước xác định và áp dụng thuật toán mã hóa với tham số khóa cho từng khối.**
  - **Dòng: từng phần tử ở đầu vào được xử lý liên tục tạo phần tử đầu ra tương ứng.**

II.1.4 Thám mã

- Có hai cách tiếp cận tấn công mã đối xứng.
  - **Tấn công dùng thuật toán: dựa trên thuật toán và một số đặc trưng chung về bản rõ hoặc một số mẫu bản rõ/bản mã. Kiểu tấn công này nhằm khai phá các đặc trưng của thuật toán để tìm bản rõ cụ thể hoặc tìm khóa.**
  - **Tấn công duyệt toàn bộ: kẻ tấn công tìm cách thử mọi khóa có thể trên bản mã cho đến khi nhận được bản rõ. Trung bình cần phải thử một nửa số khóa.**

Các kiểu tấn công thám mã

- Biết thuật toán và bản mã, dùng phương pháp thống kê, xác định bản rõ.
- Biết thuật toán, biết được bản mã/bản rõ tấn công tìm khóa.
- Chọn bản rõ và nhận được bản mã, biết thuật toán tấn công tìm khóa.
- Chọn bản mã và có được bản rõ tương ứng, biết thuật toán tấn công tìm khóa…

II.1.5 Tìm duyệt tổng thể (Brute-Force)

- Về mặt lý thuyết phương pháp duyệt tổng thể là luôn thực hiện được, do có thể tiến hành thử từng khoá, mà số khoá là hữu hạn.
- Phần lớn công sức của các tấn công đều tỷ lệ thuận với kích thước khoá. Khóa càng dài thời gian tìm kiếm càng lâu và thường tăng theo hàm mũ.
- Ta có thể giả thiết là kẻ thám mã có thể dựa vào đặc trưng về ngữ cảnh để nhận biết được bản rõ.

Thời gian đòi hỏi

Key Size (bits)	Number of Alternative Keys	Time required at 1 encryption/μs	Time required at 10^6 encryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^{6} years

II.1.6 Độ an toàn

- **An toàn không điều kiện:** ở đây không quan trọng máy tính mạnh như thế nào, có thể thực hiện được bao nhiêu phép toán trong một giây, bản mã không thể bị bẻ, vì bản mã không cung cấp đủ thông tin để xác định duy nhất bản rõ. Việc dùng bộ đệm ngẫu nhiên một lần để mã dòng cho dữ liệu mà ta sẽ xét cuối bài này được coi là an toàn không điều kiện. Ngoài ra chưa có thuật toán mã hóa nào được coi là an toàn không điều kiện.

Độ an toàn (tt)

- **An toàn tính toán:** với nguồn lực máy tính giới hạn và thời gian có hạn (chẳng hạn thời gian tính toán không quá tuổi của vũ trụ) mã hoá coi như không thể bị bẻ. Trong trường hợp này coi như mã hóa an toàn về mặt tính toán. Nói chung từ nay về sau, một thuật toán mã hóa an toàn tính toán được coi là an toàn.

II.2 Các mã thế cổ điển thay thế

- **Mã thay thế** là phương pháp mà từng kí tự (nhóm kí tự) trong bản rõ được thay thế bằng một kí tự (một nhóm kí tự) khác để tạo ra bản mã. Bên nhận chỉ cần thay thế ngược lại trên bản mã để có được bản rõ ban đầu.
- Xét các mã cổ điển sử dụng phép thay thế các chữ của bản rõ bằng các chữ khác của bảng chữ để tạo thành bản mã.
  - **Ở đây các chữ của bản rõ được thay bằng các chữ hoặc các số hoặc các ký tự khác.**
  - **Hoặc nếu xem bản rõ như một dãy bít, thì phép thế thay các mẫu bít bản rõ bằng các mẫu bít bản mã.**

II.2.1 Mã Ceasar

- Đây là mã thế được biết sớm nhất, được sáng tạo bởi Julius Ceasar. Lần đầu tiên được sử dụng trong quân sự. Việc mã hoá được thực hiện đơn giản là **thay mỗi chữ trong bản rõ bằng chữ thứ ba tiếp theo** trong bảng chữ cái.
- Ví dụ:
  - **Meet me after the toga party**
  - **PHHW PH DIWHU WKH WRJD SDUWB**

$$c = E(p) = (p + k) \bmod (26)$$

$$p = D(c) = (c - k) \bmod (26)$$

- **Thám mã Ceasar: Chỉ có 26 khoá**
- GCUA VQ DTGCM ?

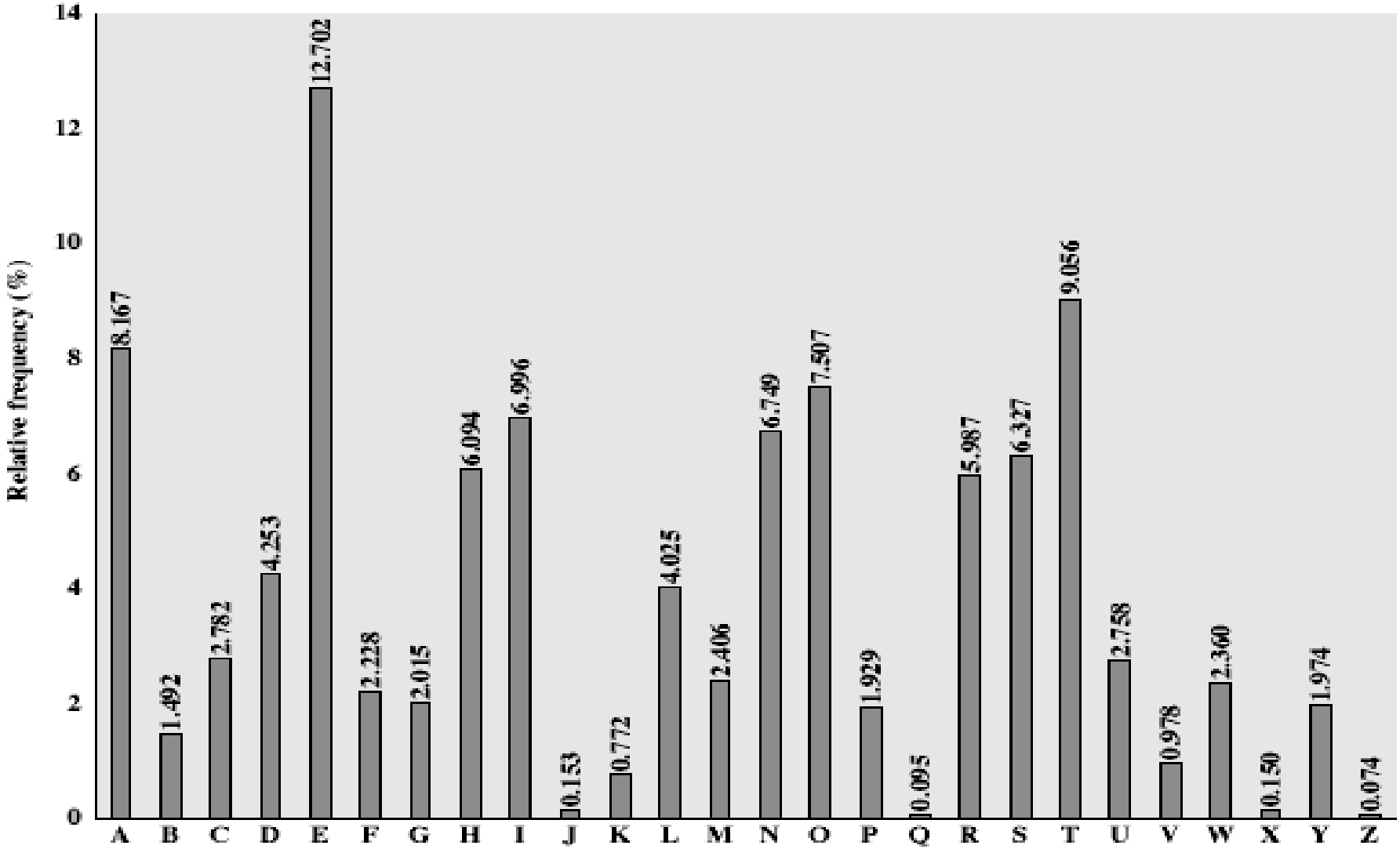
II.2.2 Các mã bảng chữ đơn

- Trong một mã **mỗi chữ của bản rõ được ánh xạ đến một chữ khác nhau** của bản mã
- Như vậy độ dài khoá ở đây là 26 và số khoá có thể có là 26!.
  - **Plain: abcdefghijklmnopqrstuvwxyz**
  - **Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN**
  - **Plaintext: ifwewishtoreplaceletters**
  - **Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA**

Thám mã bảng chữ đơn

- Dựa vào các đặc trưng về tần suất xuất hiện của các chữ
- Trong tiếng Anh chữ E được sử dụng nhiều nhất; sau đó đến các chữ T, R, N, I, O, A, S. Một số chữ rất ít dùng như: Z, J, K, Q, X; các bộ chữ thường dùng "th lrd s m shphrd shll nt wnt".
- Điều quan trọng là mã thế trên bảng chữ đơn không làm thay đổi tần suất tương đối của các chữ, có nghĩa là ta vẫn có bảng tần suất trên nhưng đối với bảng chữ mã tương ứng. Điều đó được phát hiện bởi các nhà khoa học Ai cập từ thế kỷ thứ 9.

Bảng tần suất chữ cái tiếng Anh



Thám mã bảng chữ đơn

- Thám mã trên bảng chữ đơn:
  - **Tính toán tần suất của các chữ trong bản mã**
  - **So sánh với các giá trị đã biết**
  - **Tìm kiếm các chữ đơn hay dùng (A,I,E…), bộ đôi (NO) và bộ ba (RST); và các bộ ít dùng J,K, X,Z.**
  - **Trên bảng chữ đơn cần xác định các chữ dùng các bảng bộ đôi và bộ ba trợ giúp**

Ví dụ

- **UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPE SXUDBMETSXAIZVUEPHZHMDZSHZOWSFPAP PDTSVPQUZWYMXUZUHSXEPYEP OPDZSZUFPOUDTMOHMQ**
- Tính tần suất các chữ
- Đoán P và Z là e và t.
- Khi đó ZW là th và ZWP là the.
- Suy luận tiếp tục ta có bản rõ: **it was disclosed yesterday that several informal but direct contacts have been made with political representatives in moscow**

II.2.3 Mã Playfair

- Sáng tạo bởi Charles Wheastone vào năm 1854 và mang tên người bạn là Baron Playfair
- **Ma trận khoá Playfair:** Cho trước một từ làm khoá, với điều kiện trong từ khoá đó không có chữ cái nào bị lặp. Ta lập ma trận Playfair là ma trận cỡ 5 x 5 dựa trên từ khoá đã cho và gồm các chữ trên bảng chữ cái, được sắp xếp theo thứ tự như sau:
  - **Trước hết viết các chữ của từ khoá vào các hàng của ma trận bắt từ hàng thứ nhất.**
  - **Nếu ma trận còn trống, viết các chữ khác trên bảng chữ cái chưa được sử dụng vào các ô còn lại. Có thể viết theo một trình tự qui ước trước, chẳng hạn từ đầu bảng chữ cái cho đến cuối.**

Mã Playfair (tt)

- Vì có 26 chữ cái tiếng Anh, nên thiếu một ô. Thông thường ta dồn hai chữ nào đó vào một ô chung, chẳng hạn I và J.
- Giả sử sử dụng từ khoá MORNACHY. Lập ma trận khoá Playfair tương ứng như sau:

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

Mã hoá và giải mã

- Chia bản rõ thành từng cặp chữ. Nếu một cặp nào đó có hai chữ như nhau, thì ta chèn thêm một chữ lọc chẳng hạn **X**. Ví dụ, trước khi mã **"balloon"** biến đổi thành **"ba lxloxon".**
- Nếu cả hai chữ trong cặp đều rơi vào cùng một hàng, thì mã mỗi chữ bằng chữ ở phía bên phải nó trong cùng hàng của ma trận khóa, chẳng hạn "**ar**" biến đổi thành **"rm"**

Ma trận Mã Playfair

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

Mã hoá và giải mã

- Nếu cả hai chữ trong cặp đều rơi vào cùng một cột, thì mã mỗi chữ bằng chữ ở phía bên dưới nó trong cùng cột của ma trận khóa, chẳng hạn "**mu**" biến đổi thành "**cm**"
- Trong các trường hợp khác, mỗi chữ trong cặp được mã bởi chữ cùng hàng với nó và cùng cột với chữ cùng cặp với nó trong ma trận khóa. Chẳng hạn, **"hs"** mã thành **"bp"**, và **"ea"** mã thành **"im"** hoặc **"jm"** (tùy ý)

An toàn của mã Playfair

- An toàn được nâng cao so hơn với bảng đơn, vì ta có tổng cộng 26 x 26 = 676 cặp. Mỗi chữ có thể được mã bằng 7 chữ khác nhau, nên tần suất các chữ trên bản mã khác tần suất của các chữ cái trên văn bản tiếng Anh nói chung.
- Muốn sử dụng thống kê tần suất, cần phải có bảng tần suất của 676 cặp để thám mã (so với 26 của mã bảng đơn). Như vậy phải xem xét nhiều trường hợp hơn và tương ứng sẽ có thể có nhiều bản mã hơn cần lựa chọn. Do đó khó thám mã hơn mã trên bảng chữ đơn.
- Mã Playfair được sử dụng rộng rãi nhiều năm trong giới quân sự Mỹ và Anh trong chiến tranh thế giới thứ 1. Nó có thể bị bẻ khoá nếu cho trước vài trăm chữ, vì bản mã vẫn còn chứa nhiều cấu trúc của bản rõ.

II.2.4 Các mã thế đa bảng

- Một hướng khác làm tăng độ an toàn cho mã trên bảng chữ là sử dụng nhiều bảng chữ để mã.
- Ta sẽ gọi chúng là các mã thế đa bảng.
- Mỗi chữ có thể được mã bằng bất kỳ chữ nào trong bản mã tùy thuộc vào ngữ cảnh khi mã hoá. Làm như vậy để trải bằng tần suất các chữ xuất hiện trong bản mã. Do đó làm mất bớt cấu trúc của bản rõ được thể hiện trên bản mã và làm cho thám mã đa bảng khó hơn.

Các mã đa bảng

- Ta sử dụng từ khoá để chỉ rõ chọn bảng nào được dùng cho từng chữ trong bản tin. Sử dụng lần lượt các bảng theo từ khóa đó và lặp lại từ đầu sau khi kết thúc từ khoá.
- Độ dài khoá là chu kỳ lặp của các bảng chữ. Độ dài càng lớn và nhiều chữ khác nhau được sử dụng trong từ khoá thì càng khó thám mã.

Mã Vigenere

- Mã thế đa bảng đơn giản nhất là mã Vigenere.
- Thực chất quá trình mã hoá Vigenere là việc tiến hành đồng thời dùng nhiều mã Ceasar cùng một lúc trên bản rõ với nhiều khoá khác nhau.
- Giả sử khoá là một chữ có độ dài d được viết dạng K = K1K2…Kd, trong đó Ki nhận giá trị nguyên từ 0 đến 25
- Tần suất các chữ trong bản mã dãn tương đối đều.

Các bước mã hóa

- Viết bản rõ ra
- Viết từ khoá lặp nhiều lần phía trên tương ứng của nó
- Sử dụng mỗi chữ của từ khoá như khoá của mã Ceasar
- Mã chữ tương ứng của bản rõ với bước nhảy tương ứng.
- Chẳng hạn sử dụng từ khoá deceptive

  key: deceptivedeceptivedeceptive
  plaintext: wearediscoveredsaveyourself

Ví dụ

- Chẳng hạn sử dụng từ khoá deceptive

  key: deceptivedeceptivedeceptive

  plaintext: wearediscoveredsaveyourself
- Để mã chữ w đầu tiên ta tìm chữ đầu của khóa là d, như vậy w sẽ được mã trên bảng chữ tịnh tiến 3 (tức là a tịnh tiến thành d). Do đó chữ đầu w được mã bởi chữ Z.
- Chữ thứ hai trong từ khóa là e, có nghĩa là chữ thứ hai trong bản rõ sẽ được tịnh tiến 4 (từ a tịnh tiến đến e). Như vậy thứ hai trong bản rõ e sẽ được mã bởi chữ i.
- Tương tự như vậy cho đến hết bản rõ.

Trang Saint – Cyr

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
EFGHIJKLMNOPQRSTUVWXYZABCD
FGHIJKLMNOPQRSTUVWXYZABCDE
GHIJKLMNOPQRSTUVWXYZABCDEF
HIJKLMNOPQRSTUVWXYZABCDEFG
IJKLMNOPQRSTUVWXYZABCDEFGH
JKLMNOPQRSTUVWXYZABCDEFGHI
KLMNOPQRSTUVWXYZABCDEFGHIJ
LMNOPQRSTUVWXYZABCDEFGHIJK
MNOPQRSTUVWXYZABCDEFGHIJKL
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZABCDEFGHIJKLMN
PQRSTUVWXYZABCDEFGHIJKLMNO
QRSTUVWXYZABCDEFGHIJKLMNOP
RSTUVWXYZABCDEFGHIJKLMNOPQ
STUVWXYZABCDEFGHIJKLMNOPQR
TUVWXYZABCDEFGHIJKLMNOPQRS
UVWXYZABCDEFGHIJKLMNOPQRST
VWXYZABCDEFGHIJKLMNOPQRSTU
WXYZABCDEFGHIJKLMNOPQRSTUV
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX

An toàn của mã Vigenere

- Như vậy có chữ mã khác nhau cho cùng một chữ của bản rõ. Suy ra tần suất của các chữ bị là phẳng, nghĩa là tần suất xuất hiện các chữ trên bản mã tương đối đều nhau.
- Tuy nhiên chưa mất hoàn toàn, do độ dài của khoá có hạn, nên có thể tạo nên chu kỳ vòng lặp. Kẻ thám mã bắt đầu từ tần suất của chữ để xem có phải đây là mã đơn bảng chữ hay không. Giả sử đây là mã đa bảng, sau đó xác định số bảng chữ trong từ khoá và lần tìm từng chữ. Như vậy cần tăng độ dài từ khoá để tăng số bảng chữ dùng khi mã để "là" tần suất của các chữ.

Phương pháp thám mã Kasiski

- Phương pháp phát triển bởi Babbage và Kasiski.
- Ta thấy các chữ như nhau trên bản rõ và cách nhau một khoảng đúng bằng độ dài từ khoá (chu kỳ), thì sẽ được mã bằng cùng một chữ. Như vậy từ độ lặp của các chữ trong bản mã có thể cho phép xác định chu kỳ. Tất nhiên không phải khi nào cũng tìm được độ dài từ khoá.
- Sau đó tìm các chữ trong từ khoá bằng cách tấn công từng bảng chữ đơn với cùng kỹ thuật dựa trên các bảng tần suất của các bộ chữ như trước.

Mã khoá tự động

- Lý tưởng nhất là ta có khoá dài như bản tin. Do đó Vigenere đề xuất khoá tự động sinh cho bằng độ dài bản tin như sau: từ khoá được nối tiếp bằng chính bản rõ để tạo thành khoá.
- Sau đó dùng mã Vigenere để mã bản rõ đã cho.
- Khi đó biết từ khoá có thể khôi phục được một số chữ ban đầu của bản rõ. Sau đó tiếp tục sử dụng chúng để giải mã cho văn bản còn lại.
- Sự cải tiến này làm mất khái niệm chu kỳ, gây khó khăn cho việc thám mã, nhưng vẫn còn đặc trưng tần suất để tấn công.

Ví dụ

- key: deceptivewearediscoveredsav
- plaintext: wearediscoveredsaveyourself
- ciphertext: ZICVTWQNGKZEIIGASXSTSLVVWLA

II.2.5 Bộ đệm một lần

- Nếu khoá thực sự ngẫu nhiên được dùng và có độ dài bằng bản rõ thì ta nói đó là bộ đệm một lần. Vì nó chỉ được dùng một lần và ngẫu nhiên, nên mã hoá sẽ an toàn. Mã sẽ không bẻ được vì bản mã không có liên quan thống kê gì với bản rõ, do bộ đệm được sinh ngẫu nhiên.
- Có thể nói mã bộ đệm một lần là an toàn tuyệt đối, vì với bản rõ bất kỳ và bản mã bất kỳ, luôn tồn tại một khoá để ánh xạ bản rõ đó sang bản mã đã cho.

Bộ đệm một lần (tt)

- Về mặt lý thuyết, xác suất để mọi mẩu tin (có cùng độ dài với bản rõ) trên bảng chữ là mã của một bản rõ cho trước là như nhau. Khoá chỉ sử dụng một lần, nên các lần mã là độc lập với nhau.
- Vấn đề khó khăn của mã bộ đệm một lần là việc sinh ngẫu nhiên khóa và phân phối khoá an toàn. Do đó bộ đệm một lần ít được sử dụng và chỉ dùng trong trường hợp đòi hỏi bảo mật rất cao.

II.3 Các mã thế cổ điển hoán vị

- Mã hoán vị: các chữ trong bản rõ không được thay thế bằng các chữ khác mà chỉ thay đổi vị trí, tức là việc mã hoá chỉ dịch chuyển vị trí tương đối giữa các chữ trong bản rõ.
- Bản mã có cùng phân bố tần suất xuất hiện các chữ như bản gốc nên dễ thám mã

II.3.1 Mã Rail Fence

- Đây là mã hoán vị đơn giản. Viết các chữ của bản rõ theo đường chéo trên một số dòng. Sau đó đọc các chữ theo theo từng dòng sẽ nhận được bản mã. Số dòng chính là khoá của mã. Vì khi biết số dòng ta sẽ tính được số chữ trên mỗi dòng và lại viết bản mã theo các dòng sau đó lấy bản rõ bằng cách viết lại theo các cột.
- **Ví dụ.** "meet me after the toga party"

  m e m a t r h t g p r y

  e t e f e t e o a a t

  mematrhtgpryetefeteoaat

II.3.2 Mã dịch chuyển dòng

- Mã có sơ đồ phức tạp hơn. Viết các chữ của bản tin theo các dòng với số cột xác định. Sau đó thay đổi thứ tự các cột theo một dãy số khoá cho trước, rồi đọc lại chúng theo các cột để nhận được bản mã. Quá trình giải mã được thực hiện ngược lại.
- Key: 4 3 1 2 5 6 7

Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

II.4 Mã tích

- Ta có thể kết hợp cả hai phương pháp này trong cùng một mã và có thể sử dụng đan xen hoặc lặp nhiều vòng.
- Đôi khi ta tưởng lặp nhiều lần cùng một loại mã sẽ tạo nên mã phức tạp hơn, nhưng trên thực tế không phải như vậy
  - **Tích của hai phép thế sẽ là một phép thế;**
  - **Tích của hai phép hoán vị sẽ là một phép hoán vị.**
- Trong trường hợp đặc trưng có thể tạo mã mới phức tạp hơn. Đây chính là chiếc cầu nối từ mã cổ điển sang mã hiện đại.

Mã tích (tt)

- Mã cổ điển chỉ sử dụng một trong hai phương pháp thay thế hoặc hoán vị.
- Mã dùng hoán vị hoặc dịch chuyển không an toàn vì các đặc trưng tần xuất của ngôn ngữ không thay đổi.
- Để làm cho mã khó thám mã hơn ta có thể áp dụng một số mã liên tiếp nhau

Điểm yếu của mã cổ điển

- Phương pháp mã hoá cổ điển có thể dễ dàng bị giải mã bằng cách đoán chữ dựa trên phương pháp thống kê tần xuất xuất hiện các chữ cái trên mã và so sánh với bảng thống kê quan sát của bản rõ.
- Để dùng được mã hoá cổ điển thì bên mã hoá và bên giải mã phải thống nhất với nhau về cơ chế mã hoá cũng như giải mã.

II.5 Một số vấn đề khác

- **Máy quay**
  - **Trước khi có mã hiện đại, máy quay là mã tích thông dụng nhất. Chúng được sử dụng rộng rãi trong chiến tranh thế giới thứ hai. Máy quay tạo nên mã thay thế rất đa dạng và phức tạp. Trong máy có sử dụng một số lõi hình trụ, mỗi lõi ứng với một phép thế, khi quay sẽ thay thế mỗi chữ bằng một chữ khác tương ứng. Với 3 hình trụ khác nhau, ta có 26 x 26 x 26 = 17576 bảng chữ.**

Máy quay

Dấu tin

- Dấu tin là dấu sự tồn tại của bản tin cần bảo mật trong một thông tin khác như:
  - **Trong bản tin dài chỉ dùng một tập con các chữ/từ được đánh dấu bằng cách nào đó**
  - **Sử dụng mực không nhìn thấy**
  - **Dấu tin trong các file âm thanh hoặc hình ảnh.**
- Chỉ dấu được lượng thông tin nhỏ
- Có thể kết hợp với mã.