MÃ HÓA & BẢO MẬT MẠNG
"Cryptography and Network Security"

Giáo viên

Nguyễn Minh Nhật

Mob : 0905125143

Lớp K12CDT - ĐHDT

ĐN, 08/2008

Nội dung

- **CHƯƠNG I** Tổng quan về an toàn mạng
- **CHƯƠNG II** Mã hóa và các dịch vụ xác nhận
- **CHƯƠNG III** Các công nghệ và dịch vụ bảo mật
- **CHƯƠNG IV** Firewall
- **CHƯƠNG V** Bảo mật hệ thống
- **CHƯƠNG VI** Cấu hình bảo mật Window
- **ÔN TẬP VÀ KIỂM TRA**

Chương II

Mã hóa và các dịch vụ xác nhận

2.1 Kỹ thuật mã hóa truyền thống (Classical EncryptionTechniques)

- Các thuật ngữ cơ bản (Basic Terminology)

+ plaintext : thông điệp gốc (original message)

+ Ciphertext : thông điệp mã hóa (coded message)

+ cipher : algorithm for transforming plaintext to ciphertext

+ key : info used in cipher known only to sender/receiver

+ encipher (encrypt) : converting plaintext to ciphertext

+ decipher (decrypt) : recovering ciphertext from plaintext

+ cryptography : study of encryption principles/methods

+ cryptanalysis (codebreaking) : the study of principles/ methods of deciphering ciphertext *without* knowing key

+ cryptology : lĩnh vực nghiên cứu của cả cryptography và cryptanalysis

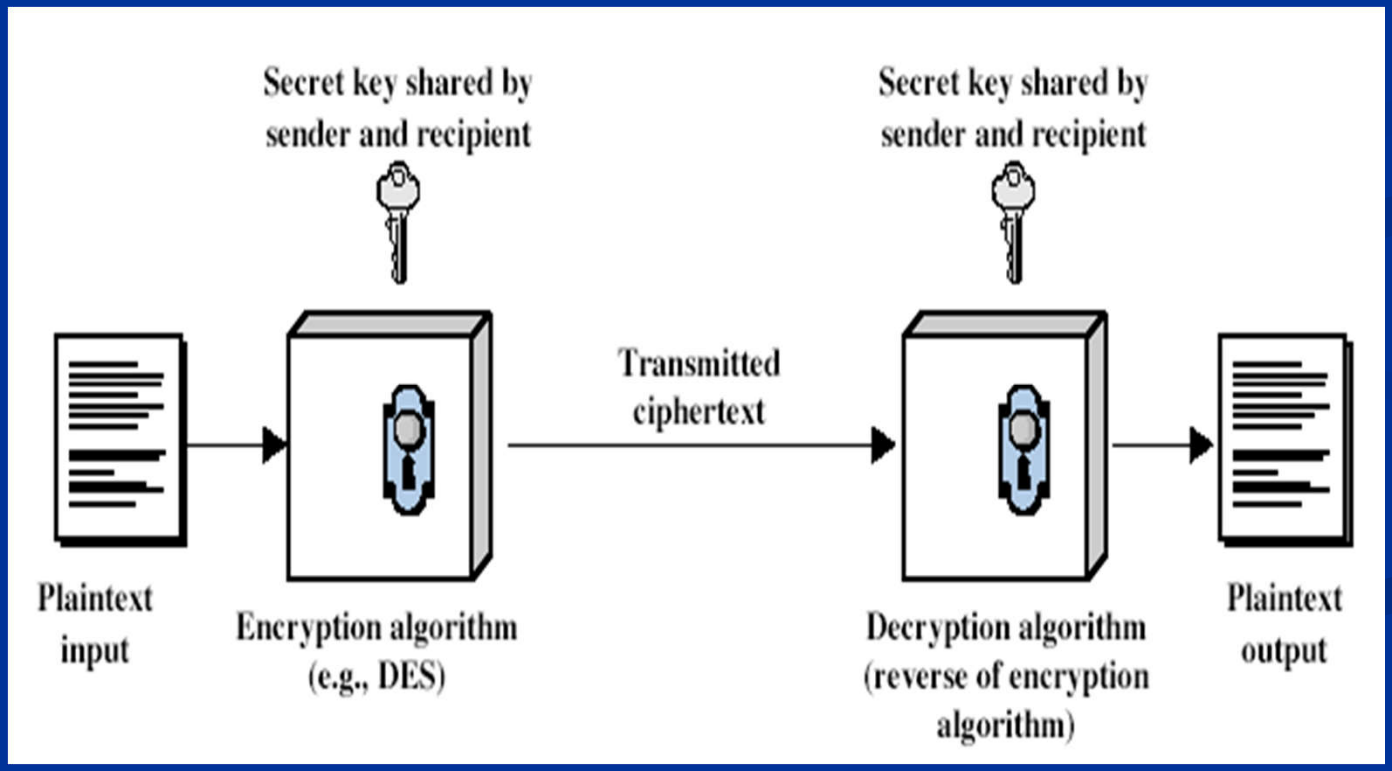
2.1 Kỹ thuật mã hóa truyền thống (Classical EncryptionTechniques)

- Mã hóa khóa đối xứng (Symmetric Encryption)
  +Quy ước tục(conventional) / khóa riêng / khóa đơn
  +Người gởi (sender) và người nhận dùng chung một khóa phổ biến (common key)
  +Tất cả các thuật tóan mã hóa truyền thống có khóa riêng
  +Chỉ là một kiểu người ta đưa ra trước khi có sự phát minh ra thuật tóan mã hóa khóa công khai vào những năm 1970
- Ví dụ :

2 người (Alice và Bob) trao đổi thông tin mật thông qua hệ thống bưu chính. Alice cần gửi một bức thư có nội dung cần giữ bí mật tới cho Bob và sau đó nhận lại thư trả lời (cũng cần giữ bí mật) từ Bob.

A sẽ cho bức thư vào hộp và khóa lại rồi gửi hộp theo đường bưu chính bình thường tới cho B. Khi B nhận được hộp, anh ta dùng một khóa giống hệt như khóa A đã dùng để mở hộp, đọc thông tin và gửi thư trả lời theo cách tương tự. Vấn đề đặt ra là A và B phải có 2 khóa giống hệt nhau bằng một cách an toàn nào đó từ trước (chẳng hạn như gặp mặt trực tiếp).

- Mô hình mã hóa đối xứng (Symmetric Cipher Model)



Yêu cầu (Requirements)

- Có 2 yêu cầu để đảm bảo sử dụng cho mã hóa khóa đối xứng này là :
  - Có một thuật tóan encryption tốt
  - Có một khóa bí mật chỉ được biết bởi người gởi / nhận

  →

  - Do đó, việc giữ bí mật khóa là đủ để đảm bảo để bảo mật cho thông điệp đã mã hóa
  - Có quan hệ phụ thuộc giữa plaintext X, ciphertext Y, key K, encryption algorithm Ek, decryption algorithm Dk.

$$Y = E_K(X)$$

$$X = D_K(Y)$$

  - Cung cấp một kênh bí mật để phân phát key

Mã hóa khóa bất đối xứng
(Non - Symmetric Encryption)

B và A có hai khóa khác nhau. Đầu tiên, A yêu cầu B gửi cho mình khóa (công khai) theo đường bưu chính bình thường và giữ lại khóa bí mật. Khi cần gửi thư, A sử dụng khóa nhận được từ B để khóa hộp. Khi nhận được hộp đã khóa bằng khóa công khai của mình, B có thể mở khóa và đọc thông tin. Để trả lời A, B cũng thực hiện theo quá trình tương tự với khóa của A.

Mã hóa khóa bất đối xứng
(Non - Symmetric Encryption)

-B và A không cần phải gửi đi khóa bí mật của mình → Điều này làm giảm nguy cơ một kẻ thứ 3 (chẳng hạn như một nhân viên bưu chính biến chất) làm giả khóa trong quá trình vận chuyển và đọc những thông tin trao đổi giữa 2 người trong tương lai. Thêm vào đó, trong trường hợp B do sơ suất làm lộ khóa của mình thì các thông tin do A gửi cho người khác vẫn giữ bí mật (vì sử dụng các cặp khóa khác).

Mã hóa khóa bất đối xứng
(Non - Symmetric Encryption)

-Không phải tất cả các thuật toán mật mã hóa khóa bất đối xứng đều hoạt động giống nhau nhưng phần lớn đều gồm 2 khóa có quan hệ toán học với nhau: một cho mã hóa và một để giải mã. Để thuật toán đảm bảo an toàn thì không thể tìm được khóa giải mã nếu chỉ biết khóa đã dùng mã hóa. → Điều này còn được gọi là mã hóa công khai vì khóa dùng để mã hóa có thể công bố công khai mà không ảnh hưởng đến bí mật của văn bản mã hóa.

Những điểm yếu

-Tồn tại khả năng một người nào đó có thể tìm ra được khóa bí mật. chưa có thuật toán mã hóa khóa bất đối xứng nào được chứng minh là an toàn trước các tấn công dựa trên bản chất toán học của thuật toán.

- Khả năng một mối quan hệ nào đó giữa 2 khóa hay điểm yếu của thuật toán dẫn tới cho phép giải mã không cần tới khóa hay chỉ cần khóa mã hóa vẫn chưa được loại trừ. An toàn của các thuật toán này đều dựa trên các ước lượng về khối lượng tính toán để giải các bài toán gắn với chúng. Các ước lượng này lại luôn thay đổi tùy thuộc khả năng của máy tính và các phát hiện toán học mới.

Những điểm yếu

-Mặc dù vậy, độ an toàn của các thuật toán mật mã hóa khóa công khai cũng tương đối đảm bảo. Nếu thời gian để phá một mã (bằng phương pháp duyệt toàn bộ) được ước lượng là 1000 năm thì thuật toán này hoàn toàn có thể dùng để mã hóa các thông tin về thẻ tín dụng

- Rõ ràng là thời gian phá mã lớn hơn nhiều lần thời gian tồn tại của thẻ (vài năm).

Những điểm yếu

-Nhiều điểm yếu của một số thuật toán mật mã hóa khóa bất đối xứng đã được tìm ra trong quá khứ. Thuật toán *đóng gói ba lô* là một ví dụ. Nó chỉ được xem là không an toàn khi một dạng tấn công không lường trước bị phát hiện. Gần đây, một số dạng tấn công đã đơn giản hóa việc tìm khóa giải mã dựa trên việc đo đạc chính xác thời gian mà một hệ thống phần cứng thực hiện mã hóa. Vì vậy, việc sử dụng mã hóa khóa bất đối xứng không thể đảm bảo an toàn tuyệt đối. Đây là một lĩnh vực đang được tích cực nghiên cứu để tìm ra những dạng tấn công mới.

- Một điểm yếu tiềm tàng trong việc sử dụng khóa bất đối xứng là khả năng bị tấn công dạng **kẻ tấn công đứng giữa** (man in the middle attack): kẻ tấn công lợi dụng việc phân phối khóa công khai để thay đổi khóa công khai. Sau khi đã giả mạo được khóa công khai, kẻ tấn công đứng ở giữa 2 bên để nhận các gói tin , giải mã rồi lại mã hóa với khóa đúng và gửi đến nơi nhận để tránh bị phát hiện. Dạng tấn công kiểu này có thể phòng ngừa bằng các phương pháp trao đổi khóa an toàn nhằm đảm bảo nhận thực người gửi và toàn vẹn thông tin. Một điều cần lưu ý là khi các chính phủ quan tâm đến dạng tấn công này: họ có thể thuyết phục (hay bắt buộc) nhà cung cấp chứng thực số xác nhận một khóa giả mạo và có thể đọc các thông tin mã hóa.

- **Mã hóa** (Cryptography)

Các điểm đặc trưng của mã hóa :

- Kiểu các hoạt động mã hóa được sử dụng
  - Thay thế (substitution) / Hóan vị(transposition) / Tích hợp
- Nhóm các khóa sử dụng :
  - single-key or private / two-key or public :
- Phương pháp mà thông điệp nguồn được xử lý
  - block / stream

Các hình thức tấn công mã hóa
(Types of Cryptanalytic Attacks)

- **Để có thể tấn công mã hóa cần :**

  + Hiểu biết về plaintext , ciphertext để tấn công

  →Sử dụng các kiến thức về thuật tóan để có thể sửa đổi thông điệp

- **Các hình thức tấn công**

  + Lựa chọn thông điệp gốc tấn công

  Lựa chọn plaintext và ciphertext thu được để tấn công quá trình chuyển đổi từ plaintext đến ciphertext

  + Lựa chọn thông điệp mã hóa tấn công

  Lựa chọn ciphertext và plaintext thu được để tấn công quá trình chuyển đổi từ plaintext đến ciphertext

  + Kết hợp cả 2 hình thức tấn công trên

  Lựa chọn plaintext hoặc ciphertext qua quá trình en/decrypt để tấn công

Tìm kiếm tra tấn (Brute Force Search)

- Người ta c/m : Với mỗi giá trị khóa khác nhau thì đều có thể thực hiện được một các dễ dàng
- Hầu hết các tấn công *mã hóa thông thường* thì thời gian xử lý tỷ lệ với (proportional) kích thước khóa
- Phụ thuộc vào sự hiểu biết và tổ chức thông điệp gốc

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

Nhận xét

Dù có nguồn tài nguyên phong phú (số lượng máy tính, tốc độ của CPU, v.v..) thì cũng khó lòng bẻ gãy thuật tóan chuyển đổi từ plaintext sang ciphertext, vì :

+ Thông tin cung cấp không đủ tương ứng với plaintext
+ Thời gian thực hiện thuật tóan rất lớn

2.3 Các phương pháp mã hóa kinh điển

Ý tưởng :

Nếu plaintext được biểu diễn như là :

- các ký tự của được thay thế bằng các ký tự khác hoặc bằng số hoặc bằng ký hiệu
- một chuỗi các bít, thì sau đó chúng được thay thế bằng các mẫu bit đã mã hóa

Mã hóa Caesar (Caesar Cipher)

- Được đưa ra sớm nhất bởi Julius Caesar
- Đầu tiên nó được sử dụng trong quân đội
- Thay thế mỗi kỹ tự trên plaintext, bằng ký tự thứ 3 kể từ nó trong bảng chữ cái alphabet
- Ví dụ:

```
meet me after the toga party
PHHW PH DIWHU WKH WRJD SDUWB
```

Mã hóa Caesar (Caesar Cipher)

- Có thể xác định sự chuyển đổi như sau :

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
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

- Thay thế cho mỗi ký tự 1 số :

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Công thức tổng quát cho mã hóa Caesar :

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

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

Mã hóa Caesar (Caesar Cipher)

- Sự giải mã/nhận dạng của mã hóa Caesar:
  - +Chỉ có 26 ciphers có thể thực hiện được
    - A ánh xạ đến A,B,C,D,...X,Y,Z
  - + Thể thực hiện thử đơn giản lần lượt mỗi ký tự
  - + Tìm kiếm tra tấn (brute force search)
  - + Cho thông điệp đã mã hóa cố gắng thử tất cả sự luân phiên của các ký tự
  - (shifts of letters)
  - + Việc thực hiện thừa nhận cho đến khi có một plaintext
- Ví dụ : Hãy phá ciphertext sau :

  " H KNUD XNT" → I LOVE YOU

  "GCUA VQ DTGCM"

Mã hóa Caesar (Caesar Cipher)

- Vấn đề bảo mật mã hóa ở bảng ký tự đơn (Monoalphabetic Cipher Security)
  + Số lượng khóa có thể : 26! = 4 x 1026 keys → Có thể được bảo mật an toàn
  + Nhưng có thể bị lỗi khi thực hiện giải mã. Vì sao ???
  ‡Do đặc điểm riêng của ngôn ngữ

Mã hóa Caesar (Caesar Cipher)

- Sự rườm rà của ngôn ngữ và giải mã mật mã (Language Redundancy and Cryptanalysis)

  + Ngôn ngữ tự nhiên (human languages) rất rườm rà

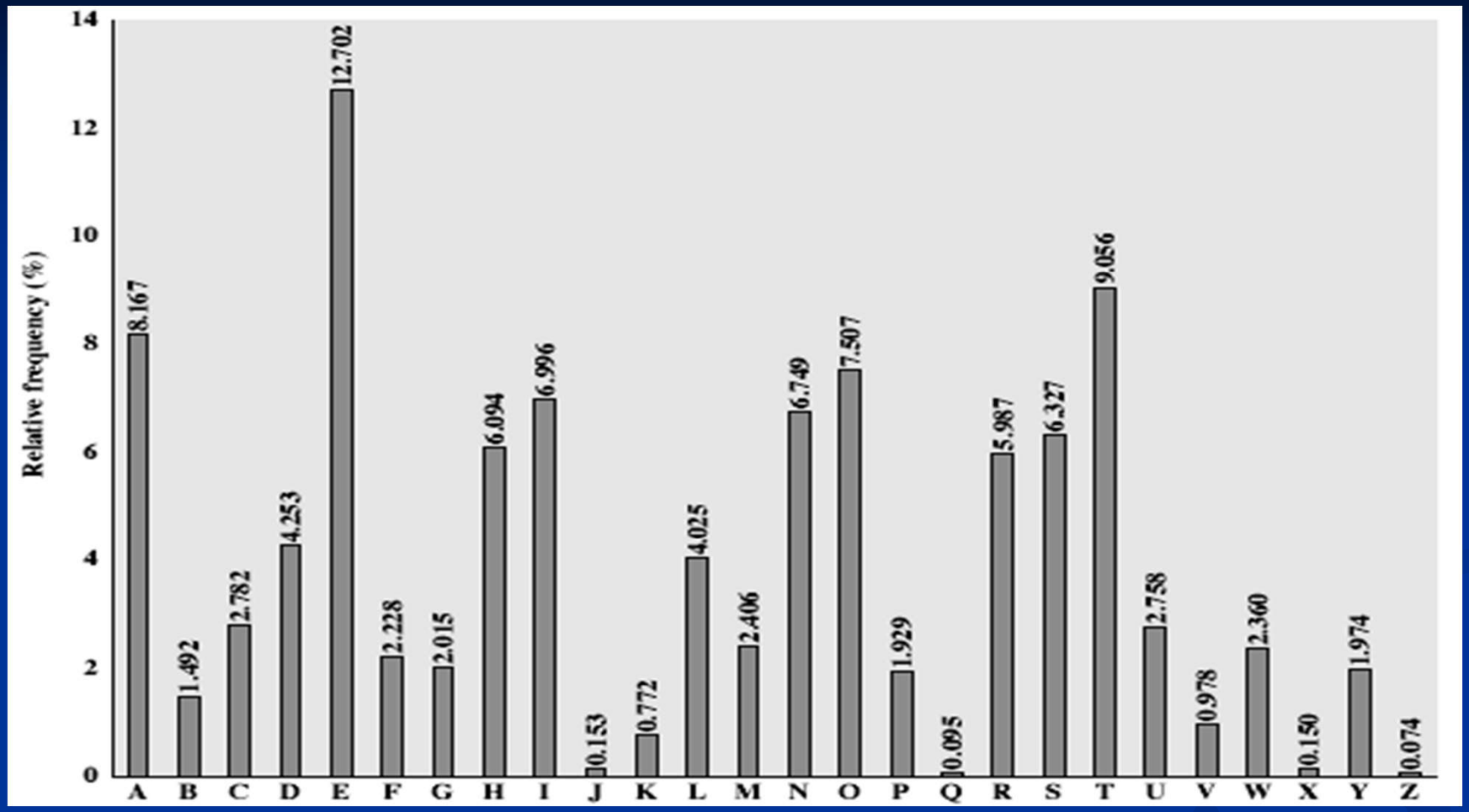
  Ví dụ : "th lrd s m shphrd shll nt wnt"

  +Những ký tự không tương tự ngôn ngữ thông thường sử dụng

  Chẳng hạn, ở ngôn ngữ English : **e** được sử dụng nhiều hơn các ký tự thông dụng khác, sau đó đến T,R,N,I,O,A,S. Những ký tự khác dùng ít hơn là : Z,J,K,Q,X

  +Có những bảng của đơn, đôi và bộ ba của những tần số ký tự (frequencies) cho thấy điều này.

English Letter Frequencies



Use in Cryptanalysis

- Việc chọn lựa khóa trong thuật tóan mã hóa thay thế bảng ký tự đơn không làm thay đổi quan hệ tần số chữ cái. Điều này được Arabian khám phá vào thế kỷ 9. Bằng so sánh sự xuất hiện của các chữ cái, ông vẽ lại những giá trị này, nhận thấy :

  + Ở thuật tóan Caesar tần số xuất hiện tăng nhanh ở các chữ cái : A-E-I, R-S-T; giàm mạnh ở J-K, X-Z
- Với mỗi bảng chữ cái đơn phải đồng nhất mỗi ký tự
  - Sự trợ giúp của các bảng đôi/ba ký tự chung (tables of common double/triple letters)

Ví dụ về giải mã mật mã

- Cho một thông điệp đã mã hóa như sau :

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ

  VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX

  EPYEPOPDZSZUFPOMBZWPFUPZDSTUDTMOHMQ

  +Đếm quan hệ tần số xuất hiện của các chữ cái

  +Dự đóan P & Z có thể là e và t

  +Đóan ZW là th → ZWP là : the

- Tiếp tục thử nghiệm với các chữ cái khác và nhận được kết quả như sau :

  it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the vietnam in moscow

Playfair Cipher

- Một phương pháp để cải tiến bảo mật là khóa mã hóa gồm nhiều chữ cái, thuật tóan **Playfair Cipher** là một ví dụ. Nó được đưa ra bởi Charles Wheatstone ở năm 1854

- Ma trận khóa Playfair (Key Matrix)

+Là một ma trận 5X5 của các chữ cái dựa trên một từ khóa

+Điền vào các ký tự của từ khóa, không trùng lại (sans duplicates)

+Điền phần còn lại của ma trận với các chữ cái khác

Ví dụ : Sử dụng từ khóa MONARCHY

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

An toàn của mã hóa Playfair Cipher

- Vấn đề bảo mật được cải tiến vượt ngoài bảng chữ cái đơn, lên đến 26 x 26 = 676 chữ ghép (digrams)
- Có thể cần đến một bảng tần số 676 mục từ để phân tích. Do đó, được sử dụng trong nhiều năm (quân đội ở Mỹ và Anh)
- Có thể bẻ gãy với vài trăm ký tự nếu có nhiều cấu trúc plaintext

Mã hóa Vigenère

- Mã hóa thay thế đa bảng ký tự đơn giản nhất là thuật tóan Vigenère Cipher, còn được goi thuật tóan **Ceasar bội/phức**
- Khóa gồm nhiều chữ cái $K = k_1\ k_2\ ...\ k_d$
- i^{th} chữ cái chỉ rõ i^{th} bảng chữ cái được dùng
- Dùng bảng chữ cái quay quay vòng, lập lại từ đầu sau d chữ cái ở thông điệp
- Ở quá trình decryption cung cấp cách làm việc ngược lại

Ví dụ :

Dùng từ khóa : *deceptive* để làm khóa

key: deceptivedeceptivedeceptive

Plaintext : w e a r e d l s c o v e r e d s a v e y o u r s e l f

Ciphertext:Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

3 4 2 4 15 …

key: d e c e p t I v e d e c e p t I v e d e c e p t I v e

P: w e a r e d I s c o v e r e d s a v e y o u r s e l f

C: Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

x,y,z

w → Z

f, g,h,i

e → I

……..

Security of Vigenère Ciphers

- Có nhiều chữ cái mã hóa ứng với mỗi chữ cái trên plaintext → **tần số xuất hiện chữ cái được che đậy** (obscured)
- Nhưng không phải không lần ra được
- Bắt đầu với những tần số của chữ cái
  - Nếu tìm thấy một bảng đơn chữ cái → trở về thuật tóan Ceasar
  - Nếu không thì thử lại để số lần lặp lại để sau đó quyết định số lượng bảng chữ cái và gắn lại với mỗi chữ cái tiếp theo của Ciphertext v.v…

Mã hóa hóan đổi (Transposition Ciphers)

- Còn được gọi là **classical transposition or permutation ciphers**
- Ở đây, ẩn đi các thông điệp bằng cách sắp xếp lại (rearranging) thứ tự chữ cái
- Thay đổi (altering) những chữ cái hiện tại (hiện tại) được dùng
- Có thể nhận ra chúng từ tần số như nhau phân bố trong tổ chức của thông điệp gốc

Mã hóa hàng rào đường ray (Rail Fence cipher)

- Viết một thông điệp chữ cái theo đường chéo trên từng hàng một
- Biểu diễn lại theo theo 1 hàng
- Ví dụ :

Cho 1 thông điệp như sau :

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

e t e f e t e o a a t

Thông điệp mã hóa

MEMATRHTGPRYETEFETEOAAT

Mã hóa dịch chuyển hàng(Row Transposition Ciphers)

- Có ý đồ phức tạp hơn
- Viết các chữ cái của thông điệp ra ngoài ở một hàng với số cột xác định
- Sau đó sắp xếp các cột theo khóa trước khi đọc vào các hàng

  + Key : 3 4 2 1 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

  + Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

3 4 2 1 5 6 7

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

TTNAAPTMTSUOAODWCOIXKNLYPETZ

Kết quả của mã hóa (Product Ciphers)

- Được sử dụng trong viêc thay thế hoặc hóan đổi và không an toàn do đặc tính của ngôn ngữ → do đó thường dùng nhiều thuật tóan mã hóa khác nhau liên tiếp nhau để thực hiện khó hơn, nhưng :
  - 2 sự thay thế tạo ra 1 thay thế phức tạp hơn
  - 2 sự hóan đổi tạo ra 1 hóan đổi phức tạp hơn
  - Nhưng 1 sự thay thế đi sau bằng 1 sự hóan đổi sẽ tạo nên mã hóa khó khăn hơn
- Đây là cầu nối từ mã hóa cổ điển để đi đến mã hóa hiện đại

Tóm tắt

- Chúng ta đã nghiên cứu:
  - classical cipher techniques and terminology
  - monoalphabetic substitution ciphers
  - cryptanalysis using letter frequencies
  - Playfair ciphers
  - polyalphabetic ciphers
  - transposition ciphers
  - product ciphers

Mã hóa khối (Block Ciphers)

- Mã hóa khối hiện đại(Modern Block Ciphers)

Trong mã hóa khối hiện đại, một trong những thuật tóan được sử dụng rộng rãi là các kiểu của thuật tóan mật mã+Nhằm cung cấp + các dịch vụ bí mật hoặc xác thực → chuẩn mã hóa dữ liệu (Data Encryption Standard -DES)

+Tiến trình mã hóa khối truyền thông điệp đến các khối, mỗi khối sẽ thực hiện en/decrypted sau khi nhận được thông điệp. Như mã hóa thay thế, nó sử dụng một block rất lớn : 64bits hoặc hơn

+Tiến trình mã hóa dòng truyền thông điệp thành dòng từng bit hoặc byte ở một thời điểm khi en/decrypting

+Hiện nay, có rất nhiều thuật tóan mã hóa khối được sử dụng

Block Ciphers

Quy tắc mã hóa khối (Block Cipher Principles)

- Hầu hết thuật tóan mã hóa khối đối xứng (symmetric block ciphers) đều dựa trên cấu trúc của thuật tóan **Feistel**
- Cần có một thời gian để giải mã ciphertext và bảo vệ thông điệp một cách có kết quả(efficiently)
- Thuật tóan khối trông giống như sự thay thế lớn vượt trội
- Cần bảng 264 muc cho một khối 64-bit
- Thay vì tạo từ việc xây dựng khối nhỏ, sử dụng ý tưởng của sản phẩm mã hóa
- Hầu hết các thuật tóan khối sử dụng rộng rãi trên thế giới thừa kế (adopted) bởi nhóm NBS vào năm1977 (NIST) như làFIPS PUB 46
- Mã hóa 64-bit dữ liệu sử dụng 56-bit key

Block Ciphers

- Hiện nay thế giới có vài cách phân tích tấn công đối với DES, bao gồm :
  - Giải mã tích phân (differential cryptanalysis)
  - Giải mã tuyến tính (linear cryptanalysis)

Trường hạn chế (Finite Fields)

- Các trường hạn chế ngày càng có vai trò quan trọng trong mật mã : AES, Elliptic Curve, IDEA, Public Key
- Tạo nên các khái niệm : nhóm, vành, trường ở trong tóan đại số (algebra)

Mã hóa đối xứng hiện đại
(Contemporary Symmetric Ciphers)

Một vài thuật tóan mã hóa khối đối xứng, như :

- Triple-DES
- Blowfish
- RC5
- briefly introduced stream ciphers
- RC4

Confidentiality using Symmetric Encryption

- Theo truyền thống sự mã hóa cân đối được dùng để cung cấp tính bí mật thông điệp confidentiality
- xem xét kịch bản tiêu biểu
  - workstations on LANs access other workstations & servers on LAN
  - LANs interconnected using switches/routers
  - with external lines or radio/satellite links
- xem xét những sự tấn công và sự xếp đặt trong kịch bản này
  - rình mò từ trạm làm việc khác
  - sử dụng dial-in đến LAN hoặc server để rình mò
  - sử dụng mối liên kết chương trình chuyển vận ngoài để vào & rình mò
  - theo dõi và/ hoặc sửa đổi giao thông một mối liên kết ngoài
- have two major placement alternatives link encryption

  end-to-end encryption

Confidentiality using Symmetric Encryption

- có hai giải pháp xếp đặt chính
  +sự mã hóa mối kết nối(link encryption)
  +sự mã hóa đầu cuối(end-to-end encryption)