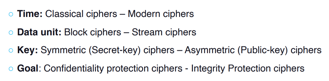
**Ôn tập cuối kì Mật mã học**

**NT219.L21.ANTN**

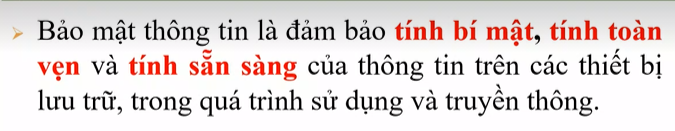
MMH=Mật mã+Phân tích mật mã

Cryptology=Cryptography + Cryptanalysis (Secret writing+Try to analysis the codes to reveal secrets)

C/C++: đa số thư viện crypto gốc, hỗ trợ build trên đa nền tảng (từ PC, server, Ios, Android)



Focus vào 3 key chính, authorization là lớp ẩn sau authentication, non-repudiation ko có trong trjang thái in-use.



* Tính mật của thông tin (Confidentiality)
* Tính toàn vẹn thông tin (Integrity)
* Tính sẵn sàng của hệ thống (Availability)

+ Confidentiality: tinh bao mat, nhưng ng so huu hoac uy quyen moi dc thao tac tren dl đó => mã hoa

Giữ bí mật, chỉ được phép truy cập bởi những đối tượng được cấp phép, đảm bảo rằng thông tin cá nhân hoặc bí mật không được cung cấp hoặc tiết lộ cho các cá nhân trái phép.

Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập:

Sau đây là một số cách thức như vậy:

+ Khóa kín và niêm phong thiết bị (tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó).

+ Yêu cầu đối tượng cung cấp credential, ví dụ, cặp username + password hay đặc điểm về tính xác thực.

+ Sử dụng firewall để ngăn chặn truy cập trái phép.

+ Mã hóa thông tin sử dụng thuật toán mạnh như AES.

Tính mật của thông tin được đại diện bởi quyền READ.

Ví dụ: một giao dịch tín dụng qua Internet, số thẻ tín dụng được gửi từ người mua hàng đến người bán, và từ người bán đến nhà cung cấp dịch vụ thẻ tín dụng. Hệ thống sẽ cố gắng thực hiện tính bí mật bằng cách mã hóa số thẻ trong suốt quá trình truyền tin, giới hạn nơi nó có thể xuất hiện (cơ sở dữ liệu, log file, sao lưu (backup), in hóa đơn…) và bằng việc giới hạn truy cập những nơi mà nó được lưu lại.

+ Integrity: Đảm bảo tính toàn vẹn thông tin, Đảm bảo rằng thông tin (cả được lưu trữ và trong các gói được truyền đi) và các chương trình chỉ được thay bởi người so huu or ng có thẩm quyền và có thể truy vết đc ai sửa sửa những j và neu dl bị thdoi 1 cách trái phép thì chúng ta phải fat hiện đc => hash

Những phương thức đó có thể là đột nhập vượt qua các quá trình xác thực, hoặc  
tấn công khai thác lỗ hổng bảo mật của hệ thống.

Tính toàn vẹn của thông tin được đại diện bởi quyền MODIFY.

+Availability: Đảm bảo dl luon o trang thai san sang khi ng so hưu or 1 ng nào đó muốn truy xuát vào để sd, Dam bao rằng hệ thống hoạt động kịp thời và dịch vụ không bị từ chối đối với người dùng có thẩm quyền. 🡺Load Balancing  Hệ thống có tính sẵn sàng cao hướng đến sự sẵn sàng ở mọi thời điểm, tránh được những rủi ro cả về phần cứng, phần mềm như: sự cố mất điện, hỏng phần cứng, cập nhật, nâng cấp hệ thống… đảm bảo tính sẵn sàng cũng có nghĩa là tránh được tấn công từ chối dịch vụ.

Khả năng đáp ứng của hệ thống cần được tính đến dựa trên số người truy cập, phần cứng và

mức độ quan trọng của dữ liệu.

Máy của hacker sẽ gửi hàng loạt các gói tin có các MAC nguồn giả tạo đến switch làm bộ nhớ lưu trữ MAC address table của switch nhanh chóng bị đầy khiến switch không thể hoạt động bình thường được nữa.

Authenticity(Tính xác thực): bảo rằng thông tin là thật, được xác thực nguồn gốc của thông tin (thuốc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy.

**Xác thực người dùng (Authentication user):**  
Xác thực dùng để định danh, nhận dạng (identify user) người dùng. Trong suốt quá trình xác thực, username và password của người dùng được kiểm tra và đối chiếu với cơ sở dữ liệu

**Phân quyền người dùng (Authorization user):**

**Sau bước xac thuc danh tinh he thong cho phep truy cap tai Nguyen nhat dinh, xd mưc do thao tac of ng đc uy quyen tren dl.**

-🡪 tạo file server dung công nghệ NFS, dung công nghệ permission.

Sau khi xác định được “danh tính” của tài khoản thì hệ thống mới chỉ trả lời được câu hỏi “Đó là ai?”, chúng ta sẽ tiến hành một bước quan trọng không kém đó là trả lời câu hỏi “Người đó có thể làm được gì?”, hay xác định quyền (phân quyền) của tài khoản hiện tại vừa mới được xác thực.

Authorization cho phép nhà quản trị điều khiển việc cấp quyền trong một khoảng thời gian, hay trên từng thiết bị, từng nhóm, từng người dùng cụ thể hay trên từng giao thức. AAA cho phép nhà quản trị tạo ra các thuộc tính mô tả các chức năng của người dùng được phép làm. Do đó, người dùng phải được xác thực trước khi cấp quyền cho người đó.

Accountability (non-repudiation) - Tính chống thoái thác trách nhiệm: doi tuong thao tac trên dl thì phải chịu trách nhiejm tren dl đó => Dùng chữ kí số.

Không thể chối cãi có nghĩa rằng một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác. , ko thể giã mạo đc

Ví dụ: trong khi giao dịch mua hàng qua mạng, khi khách hàng đã gửi số thẻ tín dụng cho bên bán, đã thanh toán thành công, thì bên bán không thể phủ nhận việc họ đã nhận được tiền, (trừ trường hợp hệ thống không đảm bảo tính an toàn thông tin trong giao dịch).

### Hệ mã Caesar

Hệ mã dịch chuyển, trong đó mỗi ký tự trong bản rõ được thay thế bằng một đứng sau nó k vị trí trong bảng chữ cái để tạo thành bản mã. Giải mã theo quy trình ngược lại để có được bản rõ.

Với mỗi chữ cái p thay bằng chữ mã hóa C, trong đó:

C = (p + k) mod 26

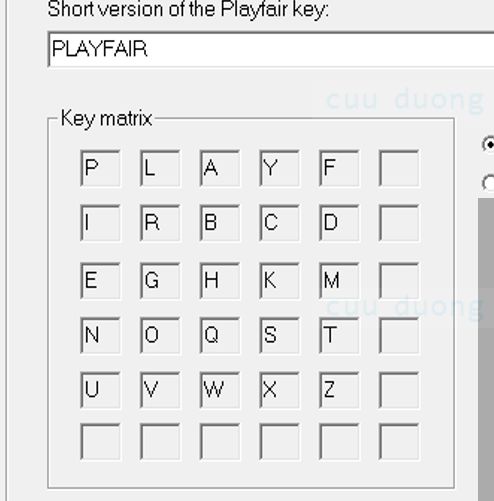
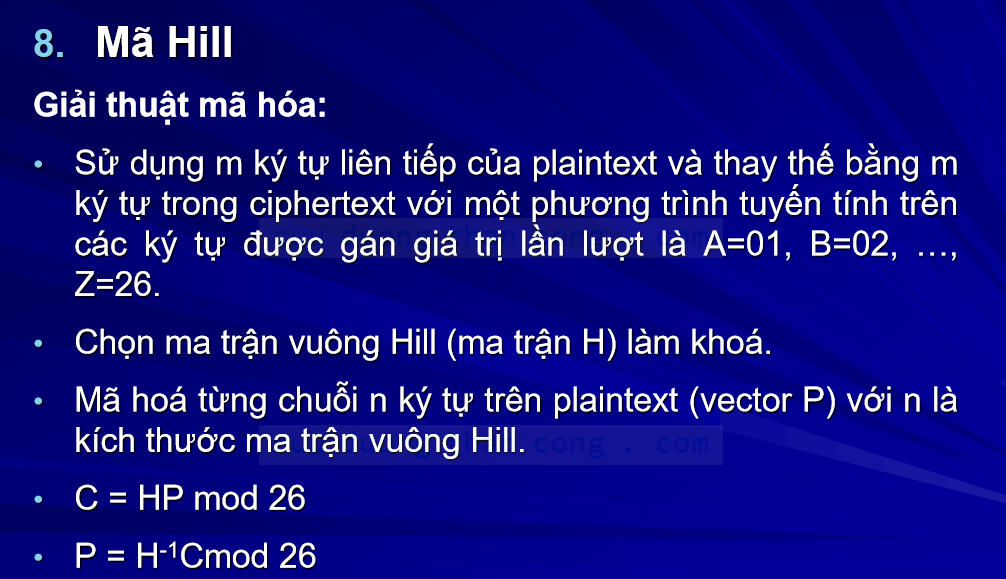
Và quá trình giải mã đơn giản là:

p = (C – k) mod 26

* biết được phương pháp mã hóa và giải mã là phép cộng trừ modulo 26
* Đối thủ có thể thử tất cả 25 trường hợp của k như sau
* thì bản giải mã tương ứng là có ý nghĩa

**Mã hóa thay thế đơn bảng (Monoalphabetic Substitution Cipher)**

* Vì 26! là một con số khá lớn nên việc tấn công phá mã vét cạn khóa là bất khả thi.
* Trong ngôn ngữ tiếng Anh, tần suất sử dụng của các chữ cái không đều nhau, chữ E được sử dụng nhiều nhất, còn các chữ ít được sử dụng thường là Z, Q, J. Tương tự như vậy 18 đối với cụm 2 chữ cái (digram), cụm chữ TH được sử dụng nhiều nhất.
* Phương pháp mã hóa đơn bảng ánh xạ một chữ cái trong bản rõ thành một chữ cái khác trong bản mã. Do đó các chữ cái trong bản mã cũng sẽ tuân theo luật phân bố tần suất trên.
* Phương pháp thứ nhất là mã hóa nhiều chữ cái cùng lúc(diagram-th; trigram-the). Phương pháp thứ hai là làm sao để một chữ cái trong bản rõ thì có tương ứng nhiều chữ cái khác nhau trong bản mã.
* **Đa kí tự** Known plaintext/ciphertext attacks.

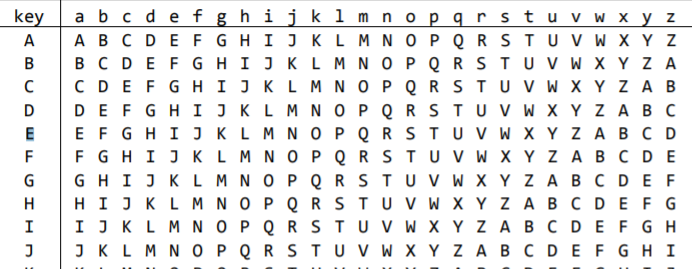
Như vậy nếu chỉ xét trên 26 chữ cái thì mã khóa Playfair có 26x26=676 cặp chữ cái, do đó các cặp chữ cái này ít bị chênh lệch về tần suất hơn so với sự chênh lệnh tần suất của từng chữ cái. Ngoài ra số lượng các cặp chữ cái nhiều hơn cũng làm cho việc phá mã tần suất khó khăn hơn.

Có thể thấy mã hóa Hill ẩn giấu các thông tin về tần suất nhiều hơn mã hóa Playfair do có thể mã hóa 3 hoặc nhiều hơn nữa các ký tự cùng lúc. Known plaintext/ciphertext attacks.

**Mã hóa thay thế đa bảng (Polyalphabetic Substitution Cipher)**

* Vigenere

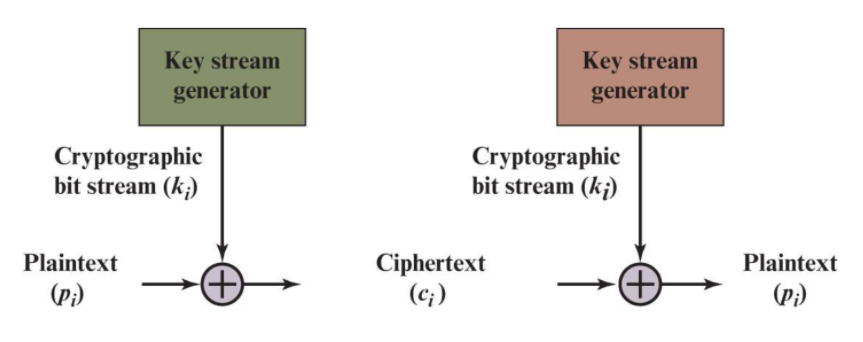
Dòng thứ k của bảng là một mã hóa Ceasar k-1 vị trí. Trong trường hợp tổng quát, mỗi dòng của bảng Vigenere là một mã hóa đơn bảng, do đó có tên gọi là mã hóa đa bảng.

****

các chữ e trong bản rõ được mã hóa tương ứng thành I, T, G, T, H, M trong bản mã. Do đó phương pháp phá mã dựa trên thống kê tần suất chữ cái là không 23 thực hiện được

Việc phá mã bằng cách thống kê sự lặp lại của các cụm từ để phỏng đoán chiều dài của khóa, trong ví dụ trên cụm từ VTW được lặp lại cách nhau 9 vị trí nên có thể đoán chiều dài của khóa là 9. Và từ đó có thể tách bản mã thành 9 phần, phần thứ nhất gồm các chữ 1, 10, 19, 28, … phần thứ hai gồm các chữ 2, 11, 20, 29….cho đến phần thứ chín. Mỗi phần coi như được mã hóa bằng phương pháp mã hóa đơn bảng. Từ đó áp dụng phương pháp phá mã dựa trên tần suất chữ cái cho từng phần một. Cuối cùng ráp lại sẽ tìm ra được bản rõ.

Vernam Known plaintext/ciphertext attacks.



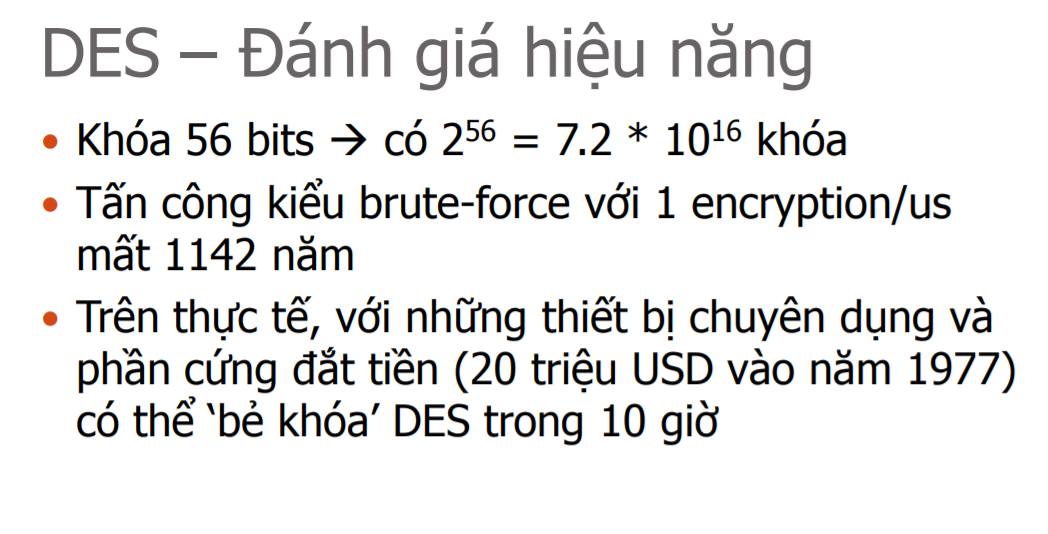
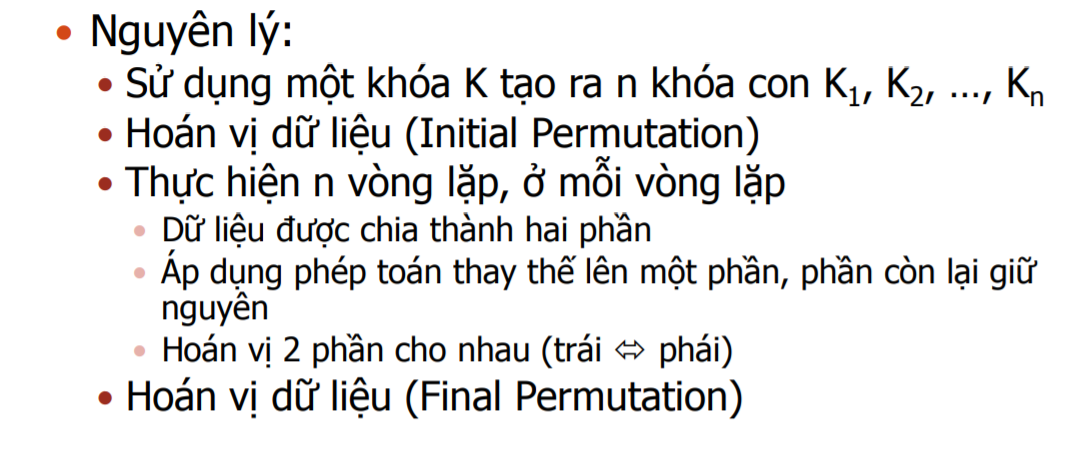
* One-Time Pad

Khóa ngẫu nhiên có chiều dài bằng chiều dài của bản rõ, mỗi khóa chỉ sử dụng một lần.

One-Time Pad phương pháp này có đặt tính là tồn tại rất nhiều khóa mà mỗi khóa khi đưa vào giải mã đều cho ra bản tin có ý nghĩa . Do đó việc vét cạn khóa không có ý nghĩa đối với mã hóa One-Time Pad.

Tuy nhiên, phương pháp One-Time Pad không có ý nghĩa sử dụng thực tế. Vì chiều dài khóa bằng chiều dài bản tin, mỗi khóa chỉ sử dụng một lần, nên thay vì truyền khóa trên kênh an toàn thì có thể truyền trực tiếp bản rõ mà không cần quan tâm đến vấn đề mã hóa.

**DES**

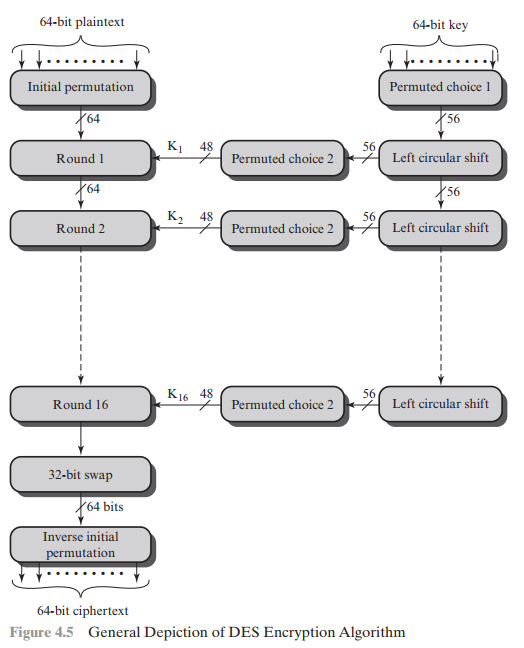
* Hiệu ứng tuyết lở
* Brute-force attack.
* **Mã hóa và giải mã** sử dụng cùng một thuật toán với quy trình khóa đảo ngược.
* **Block size: 64 bit**
* **Key size: 56 bit**
* **Rounds: 16**
* 3-DES an toàn hơn ,mở rộng không gian phím lên 56 \* 3 = 168 bit
* 

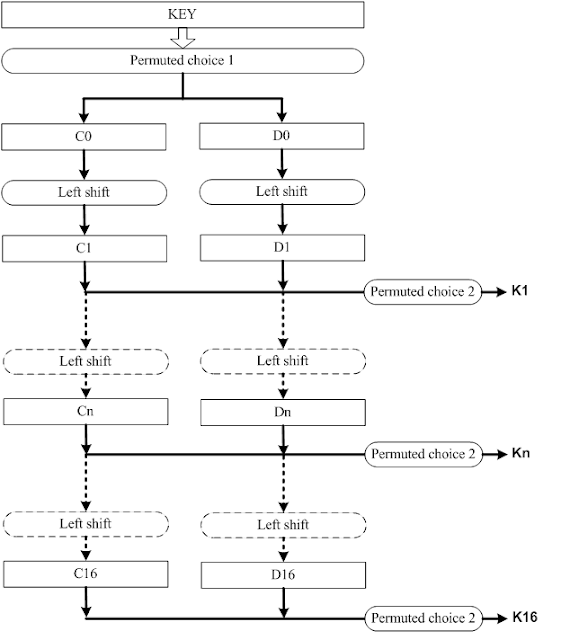
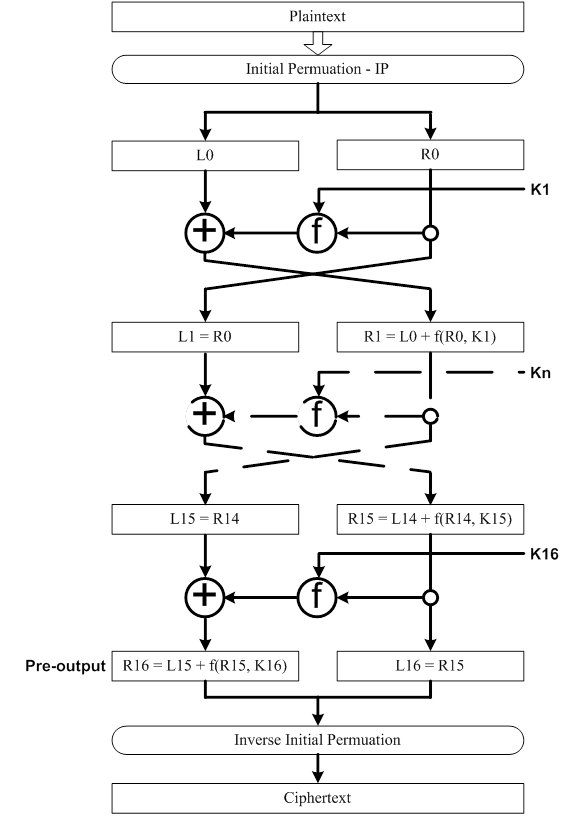
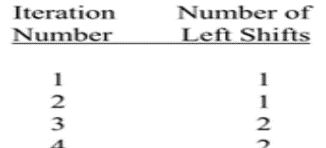
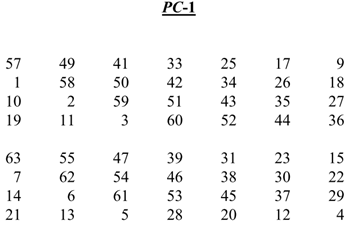
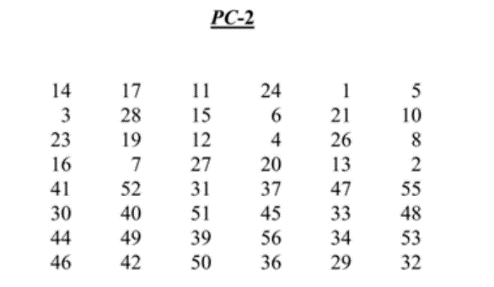
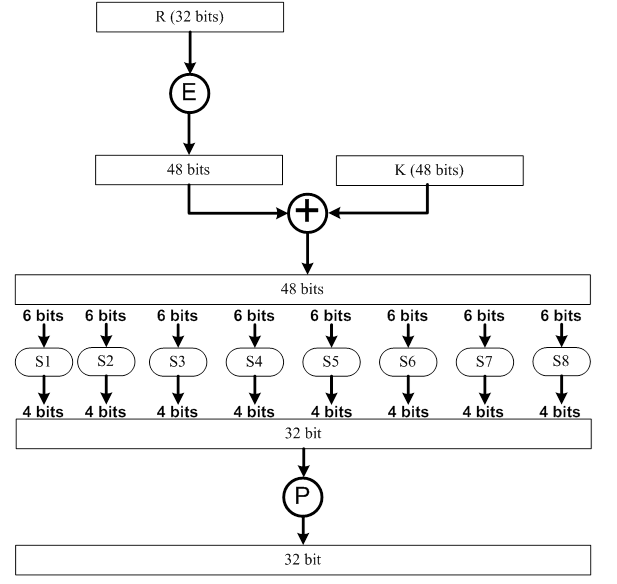
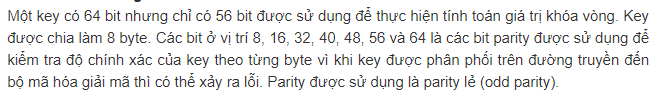
– Kích thước của khối là 64 bít: ví dụ bản tin “meetmeafterthetogaparty” biểu diễn theo mã ASCII thì mã DES sẽ mã hóa làm 3 lần, mỗi lần 8 chữ cái (64 bít): meetmeaf – tertheto – gaparty.

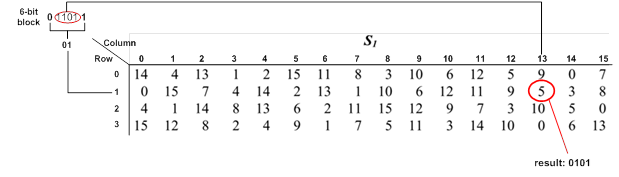
rong DES, hàm F của Feistel là:

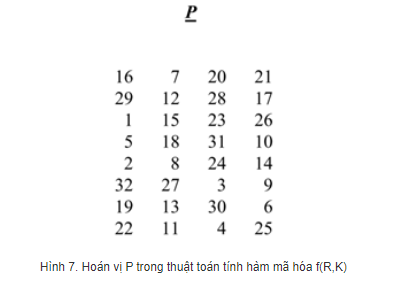
      F (Ri-1, Ki) = P-box(S-boxes (Expand (Ri-1) Ki))

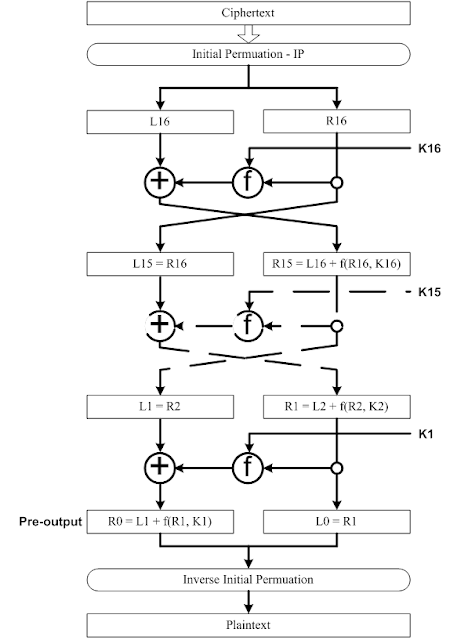
     Trong đó hàm Expand vừa mở rộng vừa hoán vị Ri-1 từ 32 bít lên 48 bít. Hàm               Sboxes nén 48 bít lại còn 32 bít. Hàm P-box là một hoán vị 32 bít.





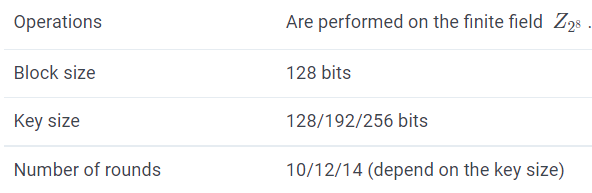


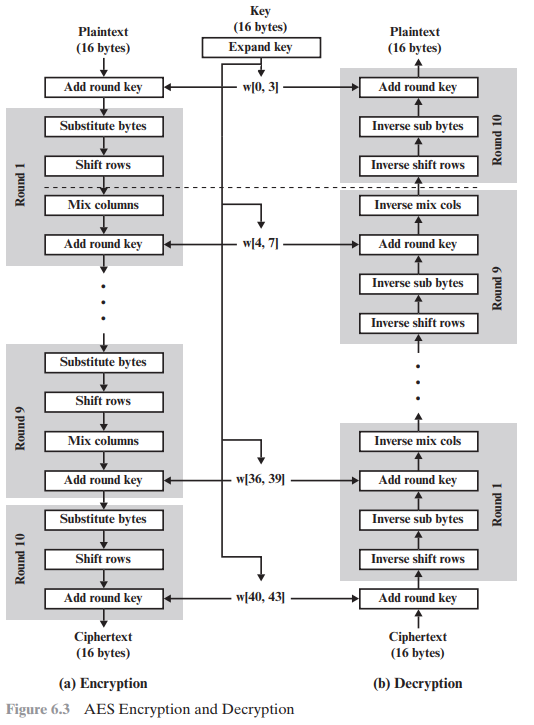


**AES**

* **Mã hóa và giải mã** sử dụng một thuật toán dường như tương tự với lịch khóa đảo ngược và các hoạt động được đảo ngược.
* input là 1 block 128bit (ma trận 4\*4 bytes), thực hiện trên trường hữu hạn GF (Z28), sử dụng số học trong trường hữu hạn GF (Z28) với đa thức x^8+x^4+x^3+x+1
* Mật mã bao gồm N vòng, trong đó số vòng phụ thuộc vào độ dài khóa: 10 làm tròn cho khóa 16 byte, 12 vòng cho khóa 24 byte và 14 vòng cho khóa 32 byte
* N - 1 vòng đầu tiên bao gồm bốn hàm biến đổi riêng biệt: SubBytes, ShiftRows, MixColumns và AddRoundKey, được mô tả sau đó.
* Vòng cuối cùng chỉ chứa ba phép biến đổi và có một phép biến đổi ban đầu (AddRoundKey) trước vòng đầu tiên, có thể được coi là Vòng 0

**128bit keys for SECRET, 192 OR 256 bit for TOP SECRET**

****



Block Cipher Modes :Four modes introduced with DES standard

• Electronic Codebook (ECB)

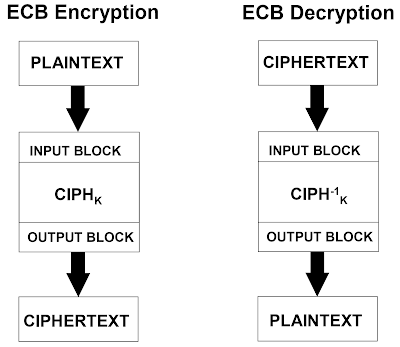
• Cipher Block Chaining (CBC)

• Cipher Feedback (CFB)

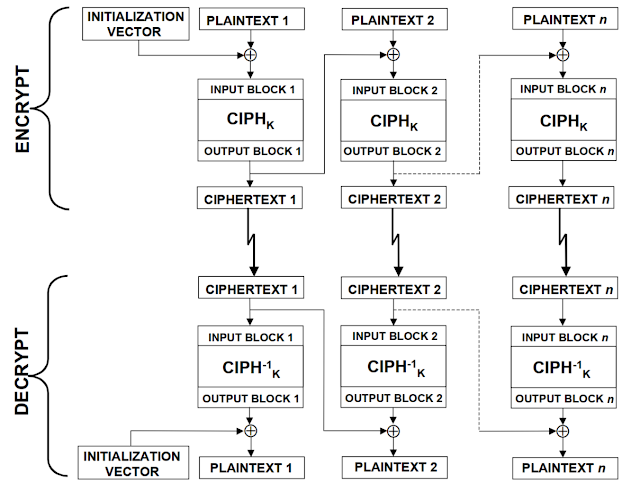
• Output Feedback (OFB)

An additional mode introduced later (standardized with AES) • Counter (CTR)

Mã hóa khối (block cipher) là mã hóa thực thi trên từng khối bit có kích thước cố định.

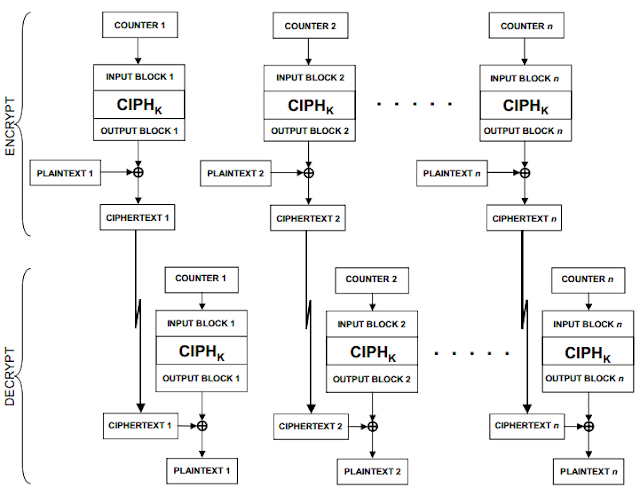
Mã hóa khối khác với mã hóa dòng (stream cihper), hay còn gọi là mã hóa luồng. Mã hóa dòng xử lý trên từng bit dữ liệu đầu vào.

* Ưu điểm:
* Thiết kế phần cứng đơn giản. Vấn đề cần quan tâm chính là thiết kế logic cho thuật toán mã hóa.
* Lỗi bit không bị lan truyền. Nếu lỗi bit xuất hiện trên một ciphertext của một khối dữ liệu thì nó chỉ ảnh hưởng đến việc giải mã khối dữ liệu đó chứ không ảnh hưởng đến việc giải mã khác khối dữ liệu khác.
* Có thể thực hiện mã hóa/giải mã song song (parallel) nhiều khối dữ liệu cùng lúc. Điều này giúp tăng tốc độ xử lý trong các hệ thống đòi hỏi mã hóa/giải mã tốc độ cao.
* Nhược điểm:
* Khả năng bảo mật kém. Do giá trị plaintext và ciphertext được ánh xạ độc lập một-một nên thông tin mã hóa dễ bị sửa đổi bằng cách như xóa bớt khối dữ liệu, chèn thêm khối dữ liệu, hoán đổi vị trí khối dữ liệu để làm sai lệch thông tin tại nơi nhận.



Đầu vào cho thuật toán mã hóa là XOR của khối plaintext và khối trước của bản mã.

* Ưu điểm:
* Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào ***IV***hoặc giá trị mã hóa (ciphertext) của khối dữ liệu liền trước.
* Quá trình giải mã (mã hóa nghịch) vẫn có thể thực hiện song song nhiều khối dữ liệu.
* Nhược điểm:
* Thiết kế phần cứng phức tạp hơn ECB ngoài logic thực thi thuật toán mã hóa, người thiết kế cần thiết kế thêm:
  + Logic quản lý độ dài chuỗi dữ liệu sẽ được mã hóa, cụ thể là số lượng khối dữ liệu trong chuỗi dữ liệu.
  + Bộ tạo giá trị ngẫu nhiên cho ***IV***.
* Lỗi bit bị lan truyền. Nếu một lỗi bit xuất hiện trên ciphertext của một khối dữ liệu thì nó sẽ làm sai kết quả giải mã của khối đữ liệu đó và khối dữ liệu tiếp theo.
* Không thể thực thi quá trình mã hóa song song vì xử lý của khối dữ liệu sau phụ thuộc vào ciphertext của khối dữ liệu trước, trừ lần mã hóa đầu tiên.



Thuật toán mã hóa không áp dụng trực tiếp trên plaintext mà dùng để biển đổi một khối dữ liệu sinh ra từ các bộ đếm (counter), sau đó mới đc XOR với plaintext ra ciphertext.

* Ưu điểm:
* Khả năng bảo mật cao hơn ECB. Tuy quá trình mã hóa/giải mã của mỗi khối dữ liệu là độc lập nhưng mỗi plaintext có thể ảnh xạ đến nhiều ciphertext tùy vào giá trị bộ đếm của các lần mã hóa.
* Có thể mã hóa/giải mã song song nhiều khối dữ liệu.
* Nhược điểm:
* Phần cứng cần thiết kế thêm các bộ đếm counter hoặc giải thuật tạo các giá trị counter không lặp lại.

Cryptanalysis-Phân tích mật mã

Tấn công dựa trên bản chất của thuật toán cộng với một số

kiến thức về các đặc điểm chung của bản rõ

Tấn công khai thác các đặc điểm của thuật toán để

cố gắng suy ra một bản rõ cụ thể hoặc suy ra

chìa khóa đang được sử dụng

Brute-force attack- Tấn công vũ lực

Kẻ tấn công thử mọi phím có thể có trên một phần của

ciphertext cho đến khi một bản dịch dễ hiểu thành bản rõ là

thu được

Trung bình, một nửa trong số tất cả các khóa có thể phải được thử

đạt được thành công

***Man-in-the-middle attack (MITM),*** là một cuộc tấn công mà kẻ tấn công bí mật chuyển tiếp và có thể làm thay đổi giao tiếp giữa hai bên mà họ tin rằng họ đang trực tiếp giao tiếp với nhau. Một ví dụ về các cuộc tấn công man-in-the-middle là nghe trộm (eavesdropping), trong đó kẻ tấn công kết nối độc lập với các nạn nhân và chuyển tiếp thông tin giữa họ để họ tin rằng họ đang nói chuyện trực tiếp với nhau qua kết nối riêng tư, trong khi thực ra toàn bộ cuộc trò chuyện được kiểm soát bởi kẻ tấn công.

Giả sử Alice muốn liên lạc với Bob. Trong khi đó, Mallory muốn chặn cuộc đối thoại để nghe trộm và có thể gửi tin sai cho Bob.

Đầu tiên, Alice hỏi Bob về chìa khóa công khai của mình. Nếu Bob gửi chìa khoá công cộng của mình đến Alice, nhưng Mallory có thể chặn nó, một cuộc tấn công xen giữa có thể bắt đầu. Mallory gửi một thông điệp giả mạo đến Alice mạo nhận rằng nó đến từ Bob, nhưng thiệt ra đó là khóa công khai của Mallory.

Alice, tin rằng khóa công khai này là của Bob, mã hóa tin nhắn của cô bằng chìa khoá của Mallory và gửi tin nhắn được mã hóa về Bob. Mallory một lần nữa chặn lại, giải mã tin nhắn sử dụng khóa riêng của mình, có thể thay đổi nó nếu cô ấy muốn và mã hóa lại nó bằng khóa công khai mà Bob gửi cho Alice. Khi Bob nhận được thông tin mới mã hóa, anh tin rằng nó đến từ Alice.

Hầu hết các giao thức mã hóa bao gồm một số dạng xác thực thiết bị đầu cuối đặc biệt để ngăn chặn các cuộc tấn công MITM. Ví dụ: TLS có thể xác thực một hoặc cả hai bên sử dụng một [nhà cung cấp chứng thực số](https://vi.wikipedia.org/wiki/Nh%C3%A0_cung_c%E1%BA%A5p_ch%E1%BB%A9ng_th%E1%BB%B1c_s%E1%BB%91" \o "Nhà cung cấp chứng thực số) được cả hai bên tin cậy.

TLS (Transport Layer Security-mới), cùng với SSL (Secure Sockets Layer-cũ) là các giao thức mật mã nhằm mục đích bảo vệ dữ liệu khi di chuyển trong môi trường Internet.  
Đây là tiêu chuẩn an ninh công nghệ toàn cầu, tạo ra liên kết được mã hóa giữa máy chủ và máy trạm. Phương pháp này cho phép bảo mật và xác thực tính toàn vẹn của các dữ liệu.

Nếu một hacker không thể cướp quyền truy cập vào một hệ thống, họ sẽ tìm cách tấn công từ chối dịch vụ (làm hệ thống không thể phục vụ người dùng được trong một khoảng thời gian, bằng cách truy cập đến hệ thống liên tục, số lượng lớn, có tổ chức). Có 2 kiểu tấn công từ chối dịch vụ:

* DoS (Denny of Service – tấn công từ chối dịch vụ): tấn công này có thể xảy ra với cả ứng dụng trực tuyến và ứng dụng offline. Với ứng dụng trực tuyến, hacker sử dụng các công cụ tấn công (tấn công Syn floods, Fin floods, Smurfs, Fraggles) trên một máy tính để tấn công vào hệ thống, khiến nó không thể xử lý được yêu cầu, hoặc làm nghẽn băng thông khiến người dùng khác khó mà truy cập được. Với ứng dụng offline, hacker tạo ra những dữ liệu cực lớn, hoặc các dữ liệu xấu (làm cho quá trình xử lý của ứng dụng bị ngưng trệ, treo)
* DDoS (Distributed Denny of Service – tấn công từ chối dịch vụ phân tán): một hình thức cao cấp của DoS, các nguồn tấn công được điều khiển bởi một (một vài) server của hacker (gọi là server điều khiển), cùng tấn công vào hệ thống. Loại tấn công này khó phát hiện ra hơn cho các hệ thống phát hiện tự động, giúp hacker ẩn mình tốt hơn.

### **Cách phòng chống tấn công DDoS**

* Theo dõi lưu lượng truy cập của bạn: Với cách này, bạn có thể phát hiện được các vụ tấn công DDoS nhỏ mà tin tặc vẫn thường dùng để Test năng lực của mạng lưới trước khi tấn công thật sự.
* Nếu bạn có thể xác định được địa chỉ của các máy tính thực hiện tấn công: có thể tạo một ACL (danh sách quản lý truy cập) trong tường lửa để thực hiện chặn các IP này.

