**ĐỀ CƯƠNG ÔN TẬP MẬT MÃ HỌC CƠ SỞ - D17**

**CHƯƠNG I**

**Câu 1: Độ an toàn của thuật toán là gì? Hãy trình bày một số tiêu chí cơ bản để đánh giá độ an toàn của một thuật toán.**

Độ an toàn thuật toán: Trong các nghiên cứu của Lars Knudsen đã trình bày chi tiết và cụ thể về độ an toàn của thuật toán mã hóa cũng như các tiêu chí đánh giá mức độ an toàn của một thuật toán. Dưới đây là một số tiêu chí cơ bản để đánh giá độ an toàn của một thuật toán mã hóa:

* Chi phí yêu cầu cho việc phá mã lớn hơn so với việc mã hóa thì thuật toán đó tương đối an toàn;
* Thời gian yêu cầu để phá mã dài hơn so với thời gian mà dữ liệu mã hóa cần giữ bí mật thì thuật toán đó là an toàn;
* Tổng lượng dữ liệu mã hóa bằng 1 khóa ít hơn lượng dữ liệu đưa vào để phá mã thì nó được coi là an toàn.

**Câu 2:** **Hãy trình bày về các phương pháp phân loại mã hóa?**

Cách 1: Phân loại mã hóa theo đặc trưng của khoá:

* Mã hóa khóa đối xứng (Hay còn gọi là mã hóa khóa bí mật): là phương pháp mã hóa mà quá trình mã hóa và giải mã dùng chung một khóa. Khóa được dùng trong mã hóa đối xứng gọi là khóa bí mật. Các thuật toán mã hóa đối xứng thường gặp: DES, AES…
* Mã hóa khóa bất đối xứng (Hay còn gọi là mã hóa khóa công khai): là phương pháp mã hóa mà khóa sử dụng để mã hóa sẽ khác với khóa dùng để giải mã. Khóa dùng để mã hóa gọi là khóa công khai và khóa dùng để giải mã gọi là khóa bí mật. Tất cả mọi người đều có thể biết được khóa công khai (kể cả hacker), và có thể dùng khóa công khai để mã hóa thông tin. Nhưng chỉ có người nhận mới nắm giữ khóa bí mật, nên chỉ có người nhận mới có thể giải mã được thông tin.

Cách 2: Phân loại mã hóa theo đặc trưng xử lý thông điệp

* Mã hóa dòng: là kiểu mã hóa mà từng bit (hoặc từng ký tự) của thông điệp được kết hợp với từng bit (hoặc từng ký tự) tương ứng của khóa để tạo thành bản mã.
* Mã hóa khối: là kiểu mã hóa mà dữ liệu được chia ra thành từng khối có kích thước cố định để mã hóa.

**Câu 3:** **Hãy nêu vai trò của mật mã học?**

Mật mã học có vai trò rất lớn trong việc đảm bảo an toàn cho hệ thống thông tin cũng như các ứng dụng hiện nay. Việc ứng dụng mật mã học nhằm đảm bảo các tính chất:

- Tính bí mật (confidentiality): thông tin chỉ được phép truy cập bởi những đối tượng hợp lệ, những đối tượng được cấp phép.

- Tính toàn vẹn thông tin (integrity): đảm bảo thông tin không bị thay đổi trong quá trình truyền tin; hoặc nếu có thay đổi thì sẽ bị phát hiện.

- Tính sẵn sàng (availability): đảm bảo thông tin phải luôn luôn sẵn sàng khi cần thiết. Điều đó có nghĩa rằng mật mã học cung cấp một cơ chế bảo mật tốt, có thể tránh được những rủi ro cả về phần cứng, phần mềm và tránh được các cuộc tấn công của tin tặc.

- Tính xác thực (authentication): đảm bảo các bên liên quan nhận biết và tin tưởng nhau trong một hệ truyền tin, đồng thời đảm bảo thông tin trao đổi là thông tin thật. - Tính chống chối bỏ (non-repudiation): đảm bảo rằng các bên liên quan không thể chối bỏ các hành động đã thực hiện trước đó.

**Câu 4: Trình bày ưu nhược điểm của giao thức Kerberos?**

* Ưu điểm: Kerberos được đánh giá là giao thức xác thực an toàn nhờ các đặc điểm sau:

- Khi sử dụng Kerberos, mật khẩu không bao giờ truyền dưới dạng rõ mà luôn được mã hóa.

- Kerberos không yêu cầu người dùng lặp đi lặp lại thao tác nhập mật khẩu trước khi truy cập vào các dịch vụ điều đó hạn chế được nguy cơ tấn công ăn cắp dữ liệu. - Giao thức được mã hóa theo các chuẩn mã hóa cao cấp như Triple DES, RC4, AES nên rất an toàn.

- Tất cả các trao đổi giữa các máy đều chứa timestamp nên vé bị đánh cắp không thể tái sử dụng, chống được tấn công dùng lại (replay attack).

* Hạn chế của Kerberos: Bên cạnh các ưu điểm kể trên, hệ thống Kerberos cũng tồn tại một số hạn chế nhất định:

- Độ bảo mật của hệ thống phụ thuộc vào sự an toàn của hệ thống KDC (Key Distribution Center). Nếu KDC bị tấn công thì toàn bộ các thành phần trong hệ thống cũng bị tê liệt.

- Do tất cả các trao đổi đều gắn timestamp nên đòi hỏi các máy tính trong hệ thống phải đồng bộ về thời gian (không chênh lệch nhau quá 5 phút). Nếu không đảm bảo điều này, cơ chế xác thực dựa trên thời hạn sử dụng sẽ không hoạt động.

- Với cơ chế đăng nhập một lần trên một máy tính, nếu máy tính đó rơi vào tay những kẻ tấn công mạng thì toàn bộ dữ liệu người dùng sẽ bị đánh cắp và gây nguy cơ cho toàn bộ hệ thống.

**Câu 5: Hãy trình bày khái quát về Krypto Knight?**

- KryptoKnight được phát triển bởi Phòng thí nghiệm nghiên cứu IBM Zurich và Yorktown. KryptoKnight cung cấp dịch vụ xác thực và phân phối khóa cho các ứng dụng và đối tượng giao tiếp trong môi trường mạng.

- Mục tiêu của KryptoKnight là cung cấp dịch vụ bảo mật mạng với tính bền và độ linh hoạt cao. Tính bền vững trong các thông điệp của KryptoKnight cho phép nó trở thành giao thức bảo mật truyền thông ở mọi tầng, có thể đảm bảo tính bí mật thông tin mà không cần sử dụng thêm bất kì giao thức nào khác. Mặt khác, KryptoKnight tránh việc sử dụng mã hóa hàng loạt, khiến cho kiến trúc của nó trở nên linh hoạt. KryptoKnight cung cấp các dịch vụ nhằm:

- Hỗ trợ người sử dụng ủy thác danh tính của mình cho đối tượng khác.

- Hỗ trợ các thực thể tham gia giao tiếp xác thực lẫn nhau bằng cách cung cấp ủy thác từ người sử dụng hợp pháp.

- Cho phép các thực thể xác thực nguồn gốc và nội dung dữ liệu được trao đổi.

Các dịch vụ mà Kryptoknight cung cấp bao gồm: Single Sign-On (SSO); Xác thực hai bên; Phân phối khóa; Xác thực nguồn gốc và nội dung dữ liệu.

Câu 6: Hãy trình bày về các mô hình hoạt động của PGD?

Mô hình hoạt động của PGP được chia làm 3 mô hình chính như sau:

* Mô hình Direct Trust: Là mô hình đơn giản nhất. Trong mô hình này, người dùng tin tưởng rằng khóa là hợp lệ vì họ biết nó đến từ đâu.
* Mô hình Hierarchical Trust: Trong một hệ thống phân cấp, có một số các ‘root CA’ gọi là chứng chỉ gốc. Các root CA này có thể tự xác thực bản thân, hoặc có thể xác thực tới các chứng chỉ khác.
* Mô hình A Web of Trust: Một mô hình web of trust bao gồm cả các mô hình an toàn khác. Do đó nó là một mô hình tin cậy phức tạp nhất. Chứng chỉ có thể được tin cậy trực tiếp, hoặc được tin cậy trong chuỗi (meta-introducers), hoặc bởi một số nhóm người giới thiệu (users).

**Câu 7: Thẻ thông minh được chia làm mấy loại? Hãy nêu chức năng và vai trò của thẻ thông minh?**

Thẻ thông minh được chia thành 2 loại chính như sau:

* Thẻ thông minh có tiếp xúc: Loại thẻ thông minh có tiếp xúc có một diện tích tiếp xúc, bao gồm một số tiếp điểm mạ vàng, và có diện tích khoảng 1 cm vuông. Khi được đưa vào máy đọc, con chip trên thẻ sẽ giao tiếp với các tiếp điểm điện tử và cho phép máy đọc thông tin từ chip và viết thông tin lên nó.
* Thẻ thông minh không tiếp xúc: Đây là loại thẻ mà chip trên nó liên lạc với máy đọc thẻ thông qua công nghệ cảm ứng RFID (với tốc độ dữ liệu từ 106 đến 848 kbit/s).

Một số chức năng và vai trò của thẻ thông minh trong vấn đề xác thực và bảo mật thông tin:

- Cho phép thực hiện các giao dịch kinh doanh một cách hiệu quả theo một cách chuẩn mực, linh hoạt và an ninh mà trong đó con người ít phải can thiệp vào.

- Giúp thực hiện việc kiểm tra và xác nhận chặt chẽ mà không phải dùng thêm các công cụ khác như mật khẩu…Chính vì thế, có thể thực hiện hệ thống dùng cho việc đăng nhập sử dụng máy tính, máy tính xách tay, dữ liệu bảo mật hoặc các môi trường kế hoạch sử dụng tài nguyên của công ty như SAP, v.v..với thẻ thông minh là phương tiện kiểm tra và xác nhận duy nhất.

Ngoài ra, thẻ thông minh cung cấp một số tính năng có thể được sử dụng để cung cấp hoặc tăng cường bảo vệ quyền riêng tư trong hệ thống.

**Câu 8: Hãy nêu định nghĩa về độ an toàn tính toán của hệ mật trong hệ thống xác suất?**

Độ an toàn tính toán: Độ đo này liên quan đến những nỗ lực tính toán cần thiết để phá một hệ mật. Một hệ mật là an toàn về mặt tính toán nếu một thuật toán tốt nhất để phá nó cần ít nhất N phép toán, N là số rất lớn nào đó.

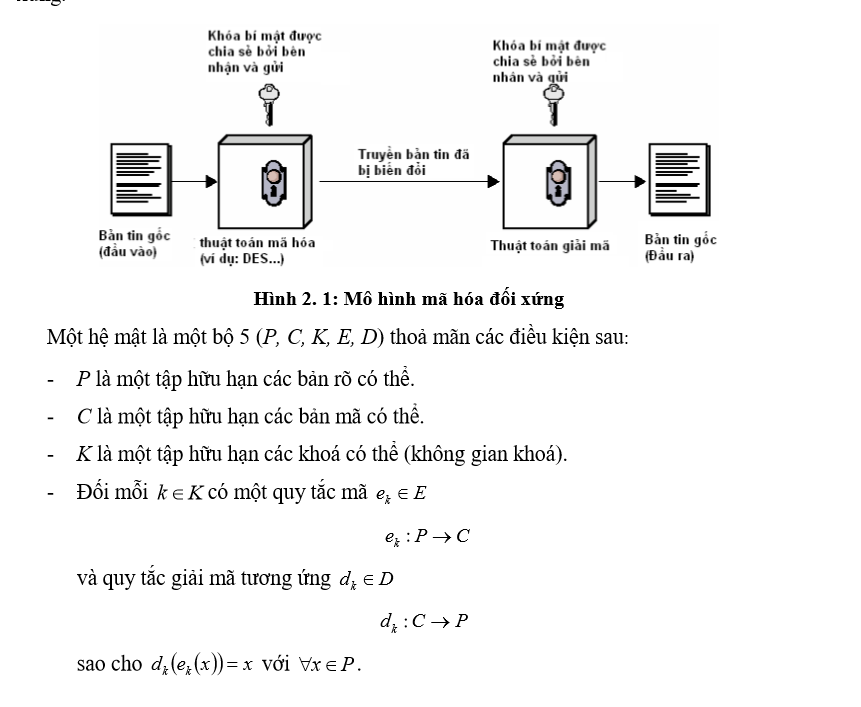
**Câu 9: Hãy nêu định nghĩa về độ phức tạp tính toán?**

Độ phức tạp của một thuật toán được đo bằng số các phép tính bit. Phép tính bit là một phép tính logic hay số học thực hiện trên các số một bit 0 và 1. Để ước lượng độ phức tạp của thuật toán dùng khái niệm bậc O lớn.

Định nghĩa: Giả sử f[n] và g[n] là hai hàm xác định trên tập hợp các số nguyên dương. Nói f[n] có bậc O lớn của g[n] và viết f[n] =O(g[n]), nếu tồn tại 1 số C>0 sao cho với n đủ lớn, các hàm f[n] và g[n] đều dương thì f[n] < C g[n].

**CHƯƠNG II**

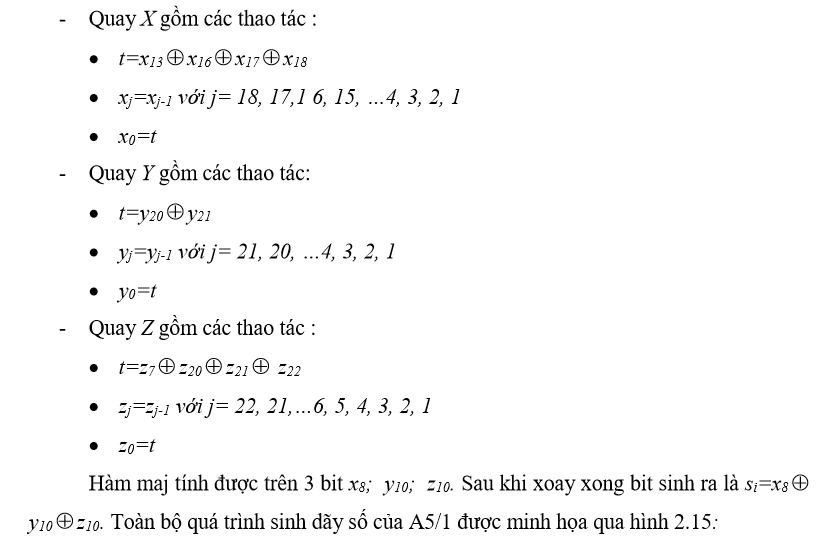
**Câu 1: Hãy trình bày đặc điểm chính của mã hóa khóa bí mật?. Vẽ sơ đồ minh họa quy trình mã hóa và giải mã của kỹ thuật mã hóa khóa bí mật?**

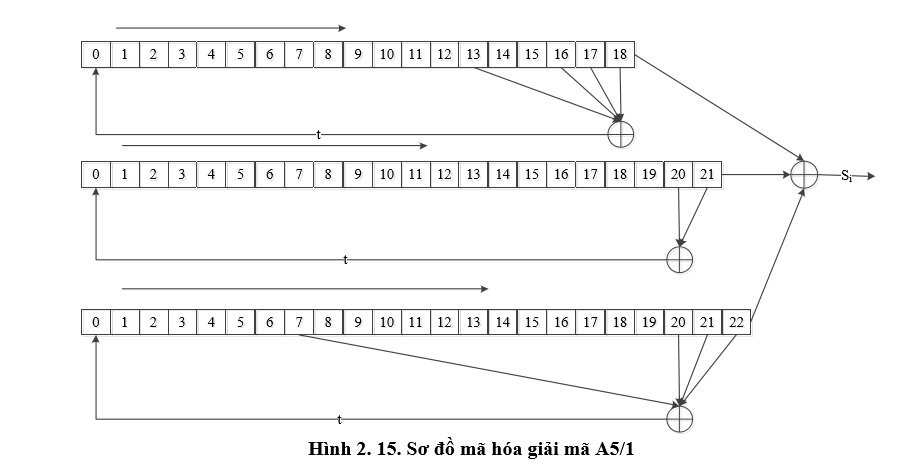


Câu 2: Hãy mô tả các bước mã hóa A5/1? (Ngân hàng)

- Bộ sinh số gồm 3 thanh ghi: X,Y,Z.

- Kích thước thanh ghi X, Y, Z lần lượt là 19, 22 và 23 bit. Các bước quay X, Y, Z cụ thể như sau:





Câu 3: Hãy mô tả các bước mã hóa RC4?

Cơ chế hoạt động của RC4 cũng giống như TinyRC4 với các đặc tính sau:

- Đơn vị mã hóa của RC4 là một byte 8 bit.

- Mảng S và T gồm 256 số nguyên 8 bit.

- Khóa K là một dãy gồm N số nguyên 8 bit với N có thể lấy giá trị từ 1 đến 256.

- Bộ sinh số mỗi lần sinh ra một byte để sử dụng trong phép XOR.

Hai giai đoạn của RC4 là:

* Giai đoạn khởi tạo:

/\* Khoi tao day S va T\*/

for i = 0 to 255 do

S[i] = i;

T[i] = K[i mod N]; next i

/\* Hoan vi day S \*/

j = 0;

for i = 0 to 255 do

j = (j + S[i] + T[i]) mod 256;

Swap(S[i], S[j]);

next i

* Giai đoạn sinh số :

i, j = 0;

while (true)

i = (i + 1) mod 256;

j = (j + S[i]) mod 256;

Swap (S[i], S[j]);

t = (S[i] + S[j]) mod 256;

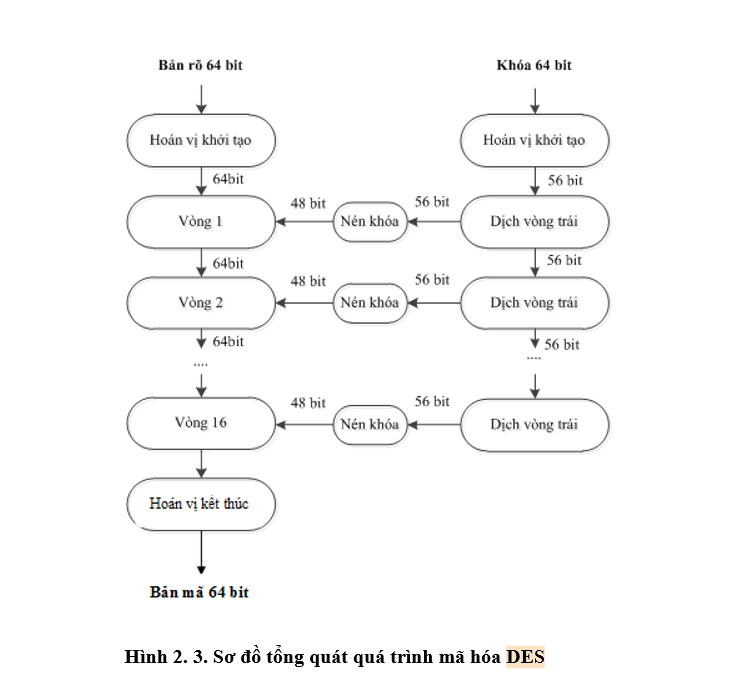
k = S[t];

end while;

**Câu 4: Hãy mô tả cấu trúc khối Feistel ?. Hãy vẽ sơ đồ mã hóa theo nguyên tắc cấu trúc khối Feistel ? (Ngân hàng)**

**Câu 5: Hãy mô tả các bước chính của thuật toán mã hóa DES?. Vẽ sơ đồ minh họa về thuật toán mã hóa DES?. Giải thích tại sao thuật toán mã hóa DES lại yêu cầu 16 vòng lặp?**

* Quy trình giải thuật mã hóa DES :
* DES mã hóa một xâu bit x của bản rõ có độ dài 64 bit bằng một khóa 56 bit . bản mã nhận được cũng có độ dài 64 bit .
* Thuật toán tiến hành theo 3 bước :



Sơ đồ mã hóa DES gồm 3 phần, phần thứ nhất là các hoán vị khởi tạo và hoán vị kết thúc. Phần thứ hai là các vòng Feistel, phần thứ ba là thuật toán sinh khóa con.

**(Giống ngân hàng)**

Thuật toán mã hóa DES yêu cầu 16 vòng lặp bởi vì:

**Câu 6: Hãy trình bày ưu nhược điểm của mã hóa DES?**

- Ưu điểm: Thuật toán mã hoá DES tốc độ mã hoá dữ liệu rất nhanh.

- Nhược điểm: Do DES có kích cỡ của không gian khoá 256 là quá nhỏ, không đủ an toàn, cho nên những máy có mục đích đặc biệt có thể sẽ bẻ gãy và dò ra khoá rất nhanh.

**Câu 7: Hãy trình bày cơ sở toán học của thuật toán mã hóa AES?**

* Phép cộng trên trường GF(2^8): Chính là phép XOR hay phép cộng theo modulo 2 giữa các bit tương ứng giữa 2 byte. Nghĩa là:

Giả sử: A=a7a6a5a4a3a2a1a0

B=b7b6b5b4b3b2b1b0

C=A+B=c7c6c5c4c3c2c1c0

trong đó: ci=(ai+bi)mod 2 (0<=i<=7)

* Phép nhân trên trường GF(2^8): Phép nhân được thực hiện trên trường GF(2^8) bằng cách nhân hai đa thức rút gọn theo modulo của một đa thức bất khả quy m(x). Đa thức bất khả quy là đa thức chỉ có ước là 1 và chính nó. Trong AES đa thức bất khả quy này là:

m(x)=x^8+x^4+x^3+x+1 Giả sử: a(x)=a7x^7+a6x^6+a5x^5+a4x^4+a3x^3+a2x^2+a1x^1+1

b(x)=b7x^7+b6x^6+b5x^5+b4x^4+b3x^3+b2x^2+b1x^1+1

=> c(x)=a(x).b(x) mod m(x)

**Câu 8: Hãy mô tả các bước chính của thuật toán mã hóa AES? Hãy vẽ sơ đồ minh họa của thuật toán mã hóa AES?**

\*Các bước chính của thuật toán mã hóa AES

Quá trình mã hóa gồm các bước :

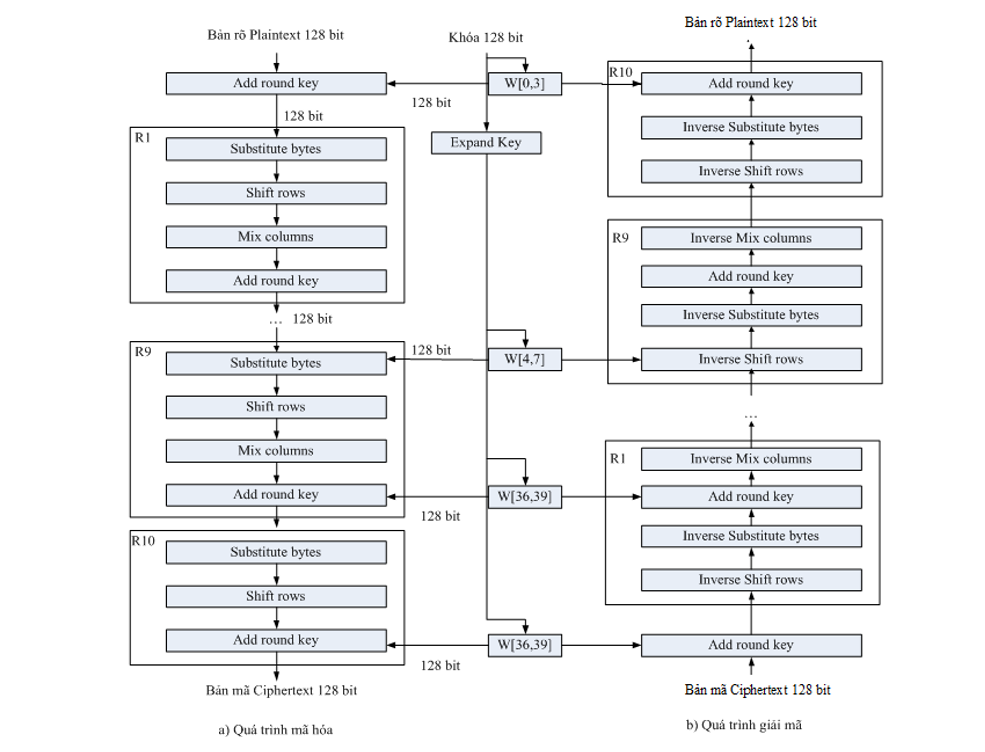
* Mở rộng khóa : các khóa phụ dùng trong các vòng lặp được sinh ra từ khóa chính AES sử dụng thủ tục sinh khóa Rijndael.
* Vòng khởi tạo :

AddRoundKey : Mỗi byte của khối được kết hợp với khóa con , các khóa con này được tạo ra từ quá trình tạo khóa con Rijndael. Mỗi khóa con có độ dài giống như các khối . quá trình kết hợp được thực hiện = cách XOR từng bit của khóa con với khối dữ liệu .

* Vòng lặp :
  1. SubBytes : đây lag phép thế (phi tuyến ) trong đó mỗi byte trong trạng thái sẽ được thế bằng một byte khác theo bảng tra (Rijndael S-box).
  2. ShiftRows : dịch chuyển , các hàng trong trạng thái sẽ được dịch vòng theo số bước khác nhau. Hàng đầu được giữ nguyên , mỗi byte của hàng thứ 2 được dịch vòng trái 1 vị trí. Tương tự dòng 3,4 dịch 2 và 3 vị trí . Do vậy mỗi khối đầu ra của bước này sẽ bao gồm các byte ở đủ 4 cột khối đầu vào . Đối với Rijndael với độ dài khối khác nhau thì số vị trí dịch chuyển cũng khác nhau.
  3. MixColumns : quá trình trộn làm việc theo các cột trong khối theo một phép biến đổi tuyến tính. Bốn byte trong từng cột được kết hợp lại theo một phép biến đổi tuyến tính khả nghịch. Mỗi khối 4 byte đầu vào sẽ cho một khối 4 byte ở đầu ra với tính chất là mỗi byte ở đầu vào đều ảnh hưởng tới cả 4 byte đầu ra. Cùng với bước ShiftRows, MixColumns đã tạo ra tính chất khuếch tán cho thuật toán.
  4. AddRoundKey .
* Vòng lặp cuối :
  1. SubBytes
  2. ShiftRows
  3. AddRoundkey

Tại chu trình cuối thì bước MixColumns không thực hiện.

Sơ đồ minh họa :

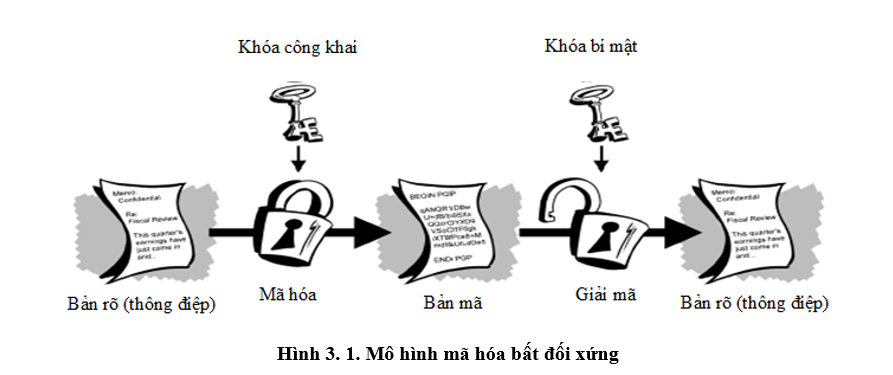


**CHƯƠNG III**

**Câu 1: Hãy trình bày đặc điểm chính của thuật toán mã hóa công khai? Vẽ sơ đô minh họa quy trình mã hóa và giải mã của thuật toán mã hóa công khai?**

Mã hóa công khai hay còn gọi là mã hóa bất đối xứng là các phương pháp mà quy trình mã hóa và giải mã sử dụng các khóa khác nhau. Khóa dùng để mã hóa là khóa công khai và khóa dùng để giải mã là khóa bí mật.

mã hóa khóa bất đối xứng sử dụng một cặp khóa: **khóa công khai** (**public key**) và **khóa bí mật** (**private key**). Hai khóa này được xây dựng sao cho từ một khóa, rất khó có cách sinh ra được khóa còn lại. Một khóa sẽ dành để mã hóa, khóa còn lại dùng để giải mã.



*Quy trình mã hóa và giải mã của mô hình mã hóa khóa công khai.*

**Câu 2: Hãy trình bày về chứng thực trong mô hình mã hóa bất đối xứng?**

**Câu 3: Hãy nêu các yêu cầu cơ bản trong thủ tục sinh khóa trong thuật toán mã hóa RSA?. Hãy phân tích các yêu cầu cơ bản đó?**

Yêu cầu cơ bản trong các bước tạo khóa :

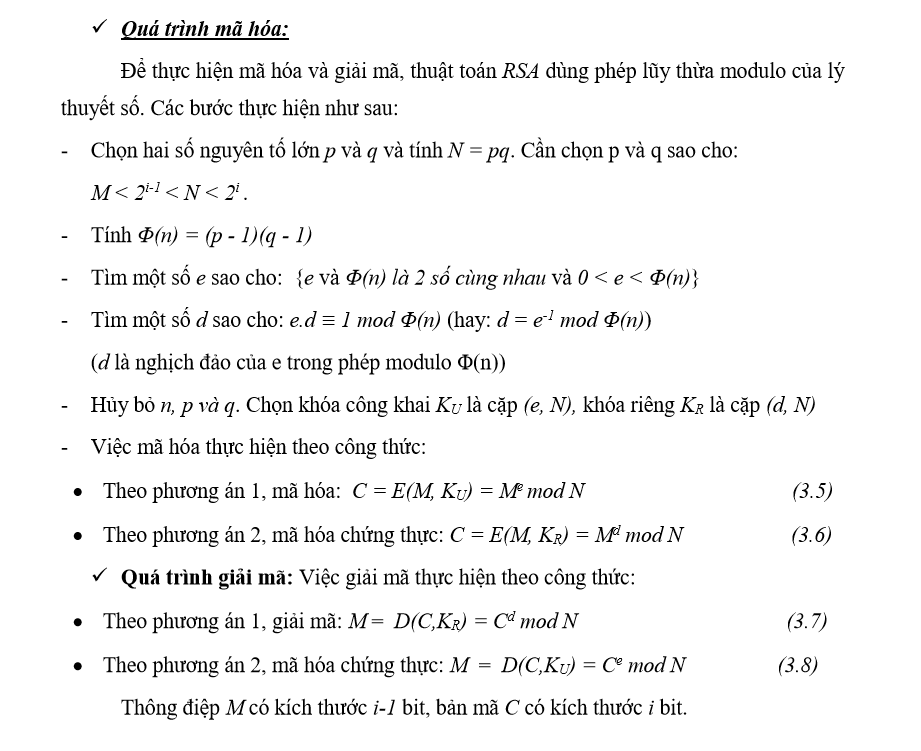
1. Chọn 2 số nguyên tố lớn p và q . với p khác q , lựa chọn ngẫu nhiên và độc lập . yêu cầu là p , q đủ lớn và hiệu p- q không quá lớn và không quá bé để tránh bị phát hiện bằng phương pháp dò số .
2. Tính n = p.q
3. Tính giá trị hàm số Ω(n) = (p-1)(q-1).
4. Chọn một số tự nhiên e sao cho 1<e<Ω(n) và là số nguyên tố cùng nhau với Ω(n).
5. Tính d sao cho d.e = 1(mod Ω(n)).

Khi đó :

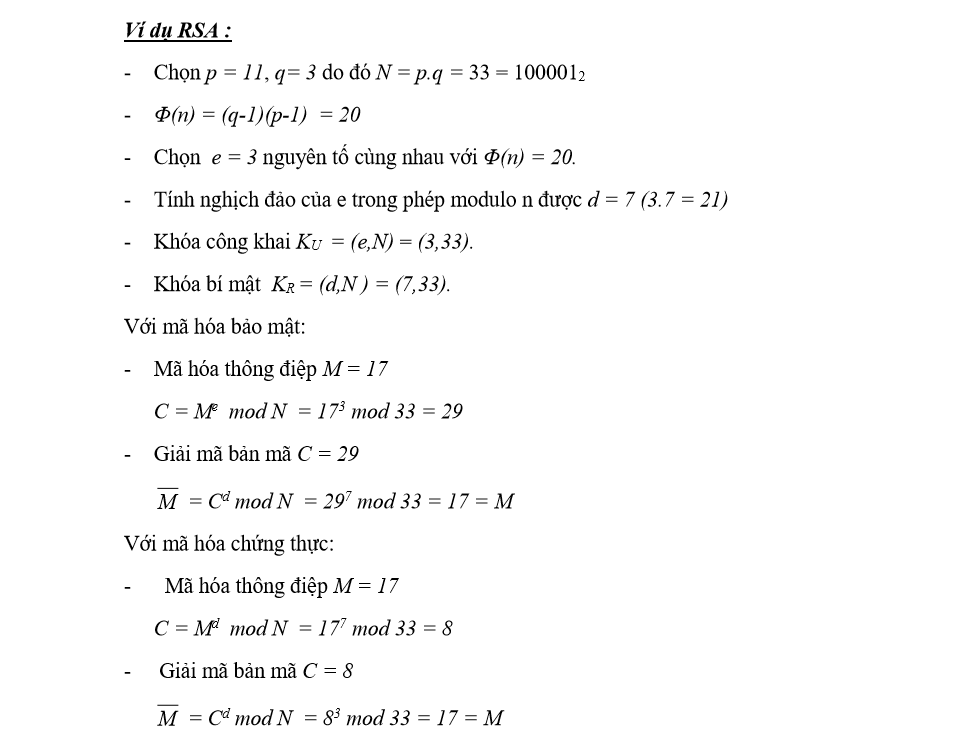
* Khóa công khai : (n,e)
* Khóa bí mật : (n,d)

**Câu 4: Hãy trình bày về quá trình mã hóa và giải mã của thuật toán RSA?. Hãy lấy ví dụ minh họa về quá trình mã hóa và giải mã của thuật toán RSA?**

Qúa trình mã hóa và giải mã cả thuật toán RSA



*Ví dụ*



**Câu 5: Hãy phân tích mức độ an toàn của thuật toán RSA?**

Có hai vấn đề về độ phức tạp tính toán trong phương pháp mã hóa RSA. Đó là các phép tính sinh khóa và các phép tính mã hóa/giải mã.

* Phép tính mã hóa và giải mã: Phép tính mã hóa và giải mã dùng phép lũy thừa modulo. Để an toàn, thường phải chọn N, e, d, M lớn.
* Phép tính sinh khóa: Phép tính sinh khóa là chọn p và q nguyên tố để tính N. Để phân tích số N thành tích hai thừa số nguyên tố p, q, chỉ có một cách duy nhất là thử từng số p và q. Do đó phải chọn p, q đủ lớn để việc thử là không khả thi. Dựa vào lý thuyết số nguyên tố, người ta ước tính rằng cần thử trung bình khoảng 70 số lẻ để tìm ra một số nguyên tố lớn chừng 2200. Vì đã chọn e trước là 65537 (hay 3 hoặc 17 …), do đó cần kiểm tra xem e có nguyên tố cùng nhau với Φ(n) = (p-1)(q-1) hay không. Nếu không phải thử lại với p và q khác. Sau khi đã tìm p và q thích hợp, cần tìm d sao cho e.d = 1 mod Φ(n).

**Câu 6: Hãy trình bày về ưu nhược điểm của mã hóa bất đối xứng**

Ưu điểm:

* Kích thước khóa lớn, độ an toàn cao;
* Việc quản lý và phân phối khóa dễ dàng hơn so với mã hóa đối xứng.

Nhược điểm:

* Tốc độ mã hóa, giải mã chậm hơn so với mã hóa đối xứng.

**Câu 7: Hãy nêu vài ứng dụng của mã hóa bất đối xứng**

Ứng dụng cơ bản của các thuật toán mã hóa bất đối xứng nói chung bao gồm:

- Bí mật trong truyền tin (Confidentiality);

- Chứng thực;

- Kết hợp tính bí mật và tin cậy.

Ứng dụng thực tế của các thuật toán mã hóa bất đối xứng:

- Dùng để vận chuyển và bảo mật khóa bí mật cho mã hóa đối xứng;

- Mã hóa email hoặc xác thực người gửi email (OpenPGP hay S/MIME);

- Mã hóa hoặc nhận thực văn bản

- Xác thực người dùng ứng dụng (Đăng nhập bằng thẻ thông minh; nhận thực người dùng trong SSL);

- Ứng dụng trong chữ ký số, chứng chỉ số.

**CHƯƠNG IV**

**Câu 1: Hãy nêu định nghĩa về hàm băm?**

Hàm băm là hàm chuyển đổi một thông điệp (chuỗi bit) có độ dài bất kỳ hữu hạn thành một dãy bit có độ dài cố định n bit (n > 0). Dãy bit đầu ra của hàm băm được gọi là giá trị băm hay mã băm.

**Câu 2: Hãy trình bày các tính chất của hàm băm có khóa và hàm băm không khóa?**

**Hàm băm không khóa:**

- Tính khó tính toán nghịch ảnh: Với bất kỳ giá trị băm h, không thể tính được x sao cho H(x)=h. Hay H được gọi là hàm một chiều.

- Tính bền xung đột yếu (weak collision resistance): với bất kỳ giá trị x, không thể tính được y ≠ x sao cho H(y) = H(x).

- Tính bền xung đột mạnh (strong collision resistance): Không thể tính được một cặp (x, y) sao cho H(x) = H(y).

- Kháng tiền ảnh (Pre-image resistance): Với một mã băm h bất kỳ, khó tìm được một thông điệp m nào mà h=hash(m). Trong góc độ hàm số toán học, mã băm là ảnh còn thông điệp là tạo ảnh của mã băm, hay gọi là tiền ảnh. Sức kháng cự tấn công từ ảnh ngược về tiền ảnh gọi là kháng tiền ảnh. Một hàm băm có kháng tiền ảnh yếu là lỗ hổng cho các cuộc tấn công tiền ảnh.

- Kháng tiền ảnh thứ hai (Second pre-image resistance) Với một thông điệp m1 bất kỳ, khó tìm được một thông điệp thứ hai m2 sao cho m1 ≠ m2 và hash(m1) = hash(m2). Xác suất xảy ra biến cố có thông điệp m2 như thế tương tự biến cố “Cùng ngày sinh như bạn”. Một hàm băm có kháng tiền ảnh thứ hai yếu là lỗ hổng cho các cuộc tấn công tiền ảnh thứ hai.

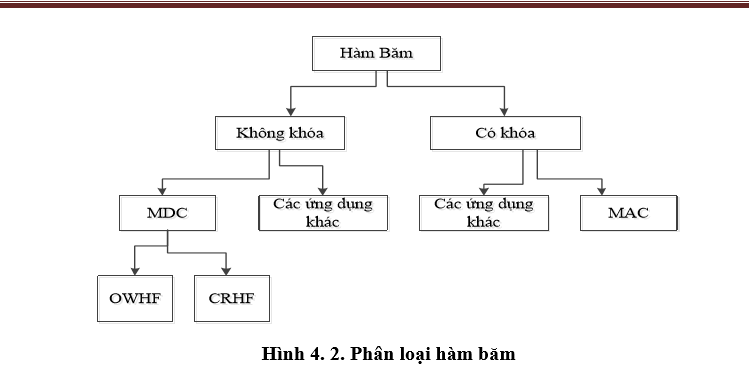
**Hàm băm có khóa:**

-Tính chất nén: với Hk đã biết và giá trị k cho trước và một đầu vào x, thì dễ dàng tính toán được Hk (x) (Hk (x) được gọi là giá trị MAC).

- Tính chất dễ dàng tính toán: Hk ánh xạ một đầu vào x có độ dài bit hữu hạn thì dễ dáng tính được đầu ra Hk (x) có độ dài bit n cố định

- Tính khó tính toán: Với các cặp giá trị đầu vào là x và xi với x ≠xi thì không có khả năng tìm được cặp Hk(x) và Hk(xi) thỏa mãn Hk(x) = Hk(xi). Nếu tính chất này không được thỏa mãn thì thông điệp bị coi là giả mạo.

**Câu 3: Hãy trình bày về phương pháp phân loại hàm băm?**



Theo đó, một số cách để phân loại hàm băm như sau:

Cách 1. Theo khóa sử dụng: hàm băm được chia thành 2 loại:

- Hàm băm không khóa (unkeyed): đầu vào chỉ là thông điệp x với hàm băm h,

- Hàm băm có khóa (keyed): đầu vào gồm thông điệp và khóa bí mật (theo dạng h(x, K), với hàm băm h và thông điệp x và K là khóa bí mật).

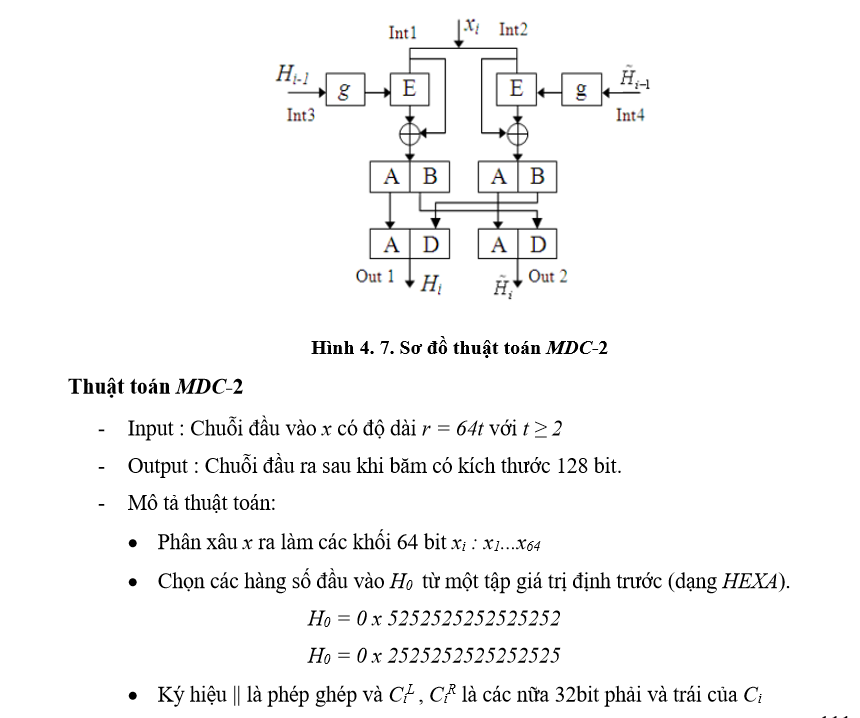
Cách 2. Theo chức năng: có thể chia các hàm băm thành 2 loại chính:

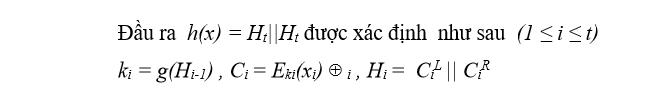
- Mã phát hiện sửa đổi (MDC - Modification Detection Code): MDC thường được sử dụng để tạo chuỗi đại diện cho thông điệp và dùng kết hợp với các kỹ thuật khác như chữ ký số để đảm bảo tính toàn vẹn của thông điệp. MDC thuộc loại hàm băm không khóa. MDC gồm 2 loại nhỏ:

* Hàm băm một chiều (OWHF - One-way hash functions): Với hàm băm một chiều, việc tính giá trị băm là dễ dàng, nhưng việc khôi phục thông điệp từ giá trị băm là rất khó khăn;
* Hàm băm chống đụng độ (CRHF - Collision resistant hash functions): Với hàm băm chống đụng độ, sẽ là rất khó để tìm được 2 thông điệp khác nhau nhưng có cùng giá trị băm.

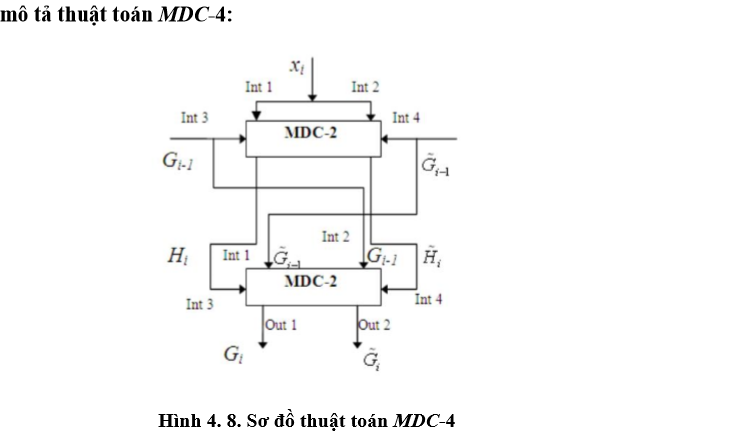
- Mã xác thực thông điệp (MAC - Message Authentication Code): MAC cũng được dùng để đảm bảo tính toàn vẹn của thông điệp mà không cần một kỹ thuật bổ sung nào khác. MAC là loại hàm băm có khóa

**Câu 4: Hãy mô tả thuật toán MDC-2?**

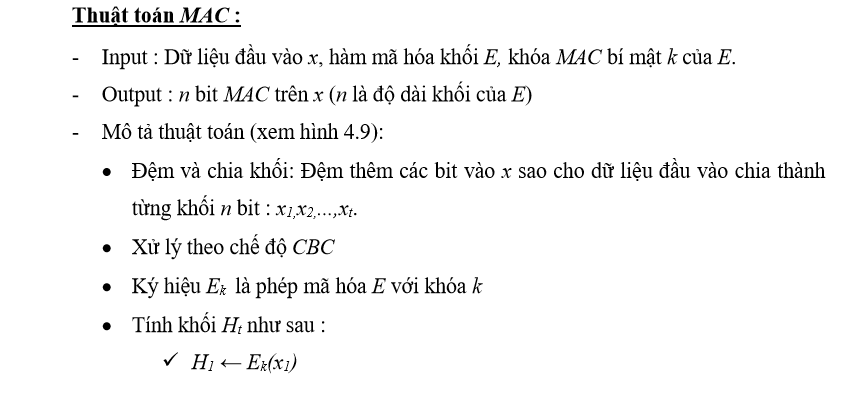


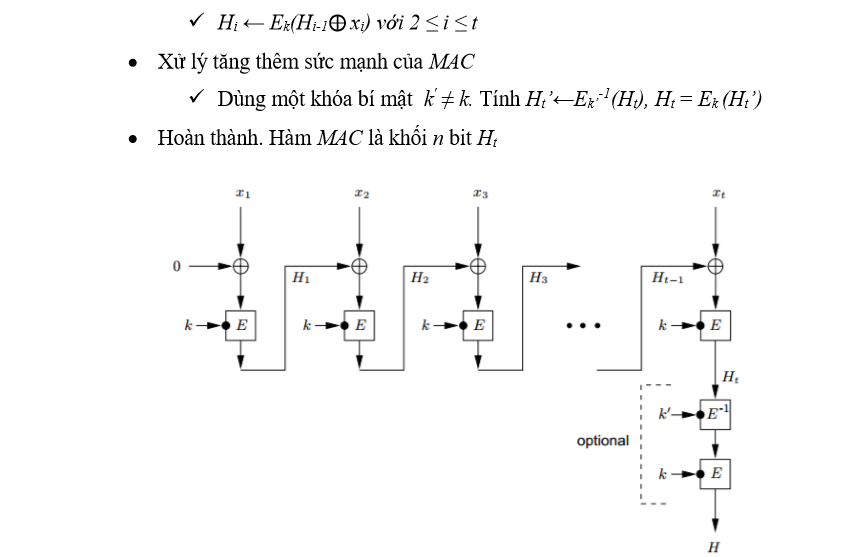


**Câu 5: Hãy mô tả thuật toán MDC – 4?**

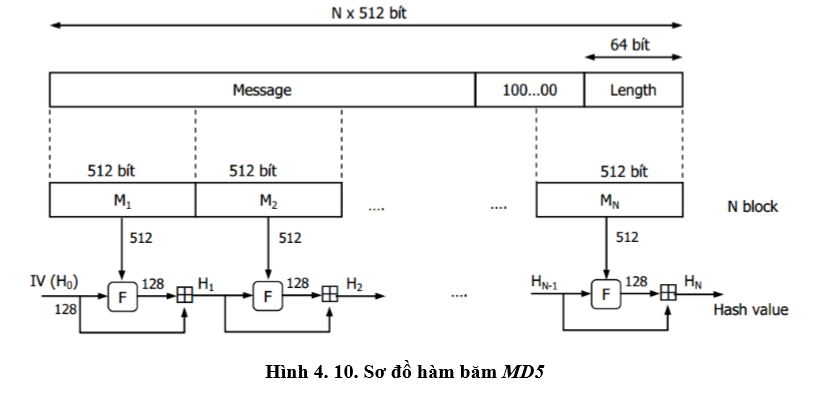


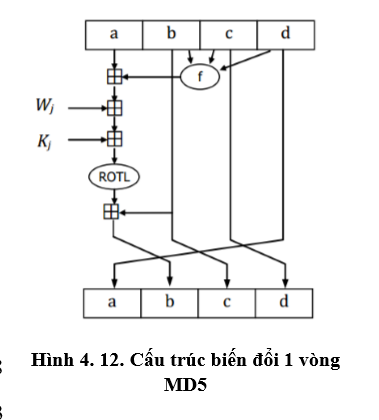
**Câu 6: Hãy mô tả thuật toán MAC?**



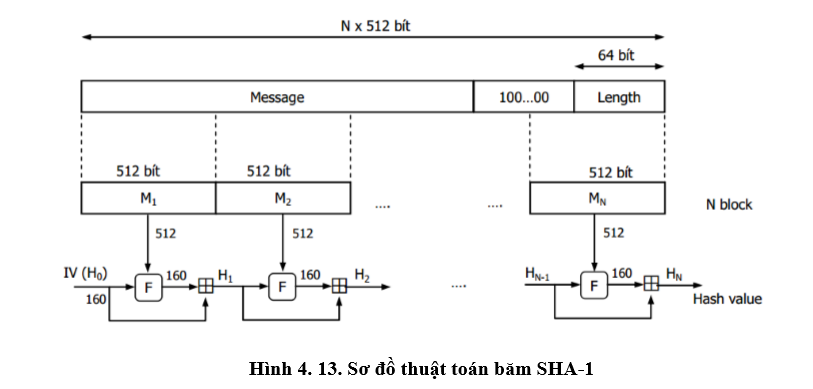


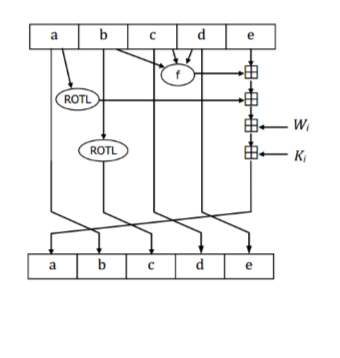
**Câu 7: Hãy trình bày về hàm băm MD5? Hãy vẽ sơ đồ minh họa về hàm băm MD5? (Giống ngân hàng)**





**Câu 8: Hãy trình bày về hàm băm SHA -1? Hãy vẽ sơ đồ minh họa về mà băm SHA-1? (Giống ngân hàng)**





**CHƯƠNG V**

**Câu 1: Hãy trình bày khái niệm về quản lý khóa?. Quản lý khóa cung cấp các tính năng gì?. Các mối đe dọa mà quản lý khóa có thể gặp phải?**

* Quản lý khóa (Key management): là một tập các kỹ thuật cho phép thiết lập và duy trì các quan hệ khóa giữa các bên có thẩm quyền.
* Quản lý khóa đóng vai trò rất quan trọng trong việc đảm bảo các yêu cầu an toàn cần thiết của một hệ truyền tin. Cụ thể, quản lý khóa cung cấp các tính năng:

- Tính bí mật;

- Toàn vẹn;

- Xác thực;

- Không thể chối bỏ;

- Chữ ký số.

* Một số mối đe dọa cụ thể như sau:

- Các khóa bí mật bị lộ;

-Tính xác thực của các khóa bí mật và công khai bị thỏa hiệp (compromise).

- Sử dụng trái phép các khóa bí mật và công khai:

 Sử dụng các khóa đã hết hiệu lực;

 Sử dụng các khóa sai mục đích;

**Câu 2: Hãy cho biết đặc điểm chung của các kỹ thuật phân phối và thỏa thuận khóa bí mật?**

Đặc điểm chung của các kỹ thuật phân phối và thỏa thuận khóa bí mật là chỉ có một khóa duy nhất KS (secret key) được sinh ra, được gửi đến cho cả 2 bên qua một kênh truyền an toàn.

**Câu 3: Hãy trình bày về KDC và KTC?Hãy so sánh 2 kỹ thuật này?**

**4) Hãy nêu các bước chính trong quá trình trao đổi khóa của giao thức NeedhamSchroeder?.**

**5) Hãy nêu các bước chính trong quá trình trao đổi khóa của giao thức Otway-Rees?.**

**6) Hãy trình bày về giao thức không khóa Shamir?.**

**7) Hãy nêu các bước hoạt động chính của giao thức Kerberos?.**

**8) Hãy cho biết đặc điểm chung của các kỹ thuật phân phối khóa công khai?. 9) Hãy trình bày về chứng chỉ xác thực khóa công khai X.509?.**

**10) Hãy trình bày về kỹ thuật phân phối và thỏa thuận khóa kết hợp?.**

**11) Hãy nêu các bước chính trong giao thức thỏa thuận khóa Diffie-Hellman?. Các điểm cần lưu ý khi sử dụng giao thức này?.**