**CHƯƠNG I: Tổng quan về Mật mã học**

**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 là **độ an toàn của thuật toán mã hóa**. 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?**

Phân loại mã hóa theo **đặc trưng của khoá**:

* Mã hóa **khóa đối xứng** (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** (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.

Phân loại mã hóa theo **đặc trưng xử lý thông điệp**

* Mã hóa dòng: là kiểu mã hóa mà từng bit (hoặc từng byte) của thông điệp được kết hợp với từng bit (hoặc từng byte) 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 **4 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**:

* **Mật khẩu** không bao giờ truyền dưới dạng rõ mà **luôn được mã hóa**.
* **Không yêu cầu** người dùng lặp đi **lặp lại** thao tác **nhập mật khẩu** trước khi truy cập vào các dịch vụ, giúp 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.
* **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**:

* **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?**

Krypto Knight **cung cấp dịch vụ xác thực và phân phối khóa** cho các ứng dụng và đối tượng giao tiếp trong môi trường 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**.

Krypto Knight **tránh** việc sử dụng **mã hóa hàng loạt**, khiến cho **kiến trúc** của nó trở nên **linh hoạt**.

KryptoKnight cung cấp **các dịch vụ**:

* Single Sign-On (SSO)
* Xác thực hai bên
* Phân phối khóa
* Xác thực nguồn gốc và nội dung dữ liệu

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.

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

PGP được chia làm **3 mô hình** chính:

* **Direct Trust**: người dùng tin tưởng rằng khóa là hợp lệ vì họ biết nó đến từ đâu.
* **Hierarchical Trust**: trong hệ thống phân cấp. sử dụng các **Root CA** có thể **tự xác thực** bản thân, hoặc có thể **xác thực** tới các **chứng chỉ khác**.
* **A Web of Trust**: bao gồm các mô hình an toàn khác. Chứng chỉ có thể được **tin cậy trực tiếp**, hoặc được **tin cậy trong chuỗi** (meta-introducers), hoặc **bởi một số nhóm users**.

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

Smart Card được chia thành **2 loại** chính:

* Thẻ thông minh **có tiếp xúc**: có một diện tích tiếp xúc. Khi 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**: **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).

**Chức năng và vai trò** 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 chỉ với thẻ thông minh mà không phải dùng thêm các công cụ khác như mật khẩu…
* 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 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.

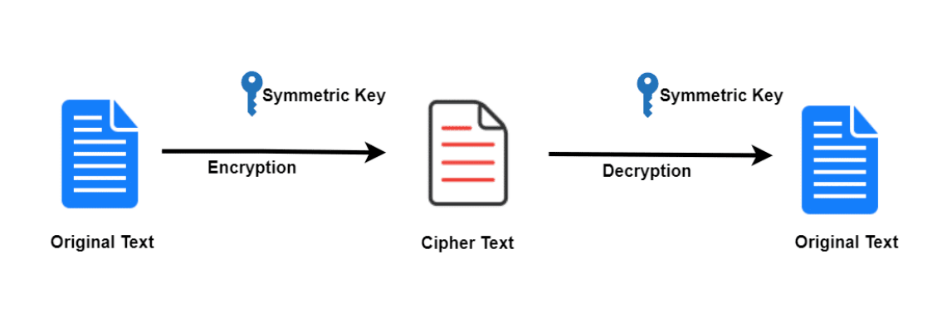
Trên thực tế, một hệ mật đgl an toàn về mặt tính toán nếu có một phương pháp tốt nhất phá hệ này nhưng yêu cầu thời gian lớn đến mức không chấp nhận được.

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

Nếu độ phức tạp thuật toán quan tâm đến cận trên của bài toán (hay độ phức tạp để giải được bài toán) thì độ phức tạp tính toán sẽ quan tâm đến cận dưới của bài toán (hay độ khó tối thiểu để giải một bài toán) thay vì tập trung vào việc tìm nghiệm.

Bài toán quyết định hiển nhiên không thể khó hơn bài toán tìm kiếm nên nếu ta chứng minh được bài toán quyết định là khó thì nghiễm nhiên bài toán tìm kiếm cũng khó theo.

**CHƯƠNG II: Mã hóa khóa đối xứng**

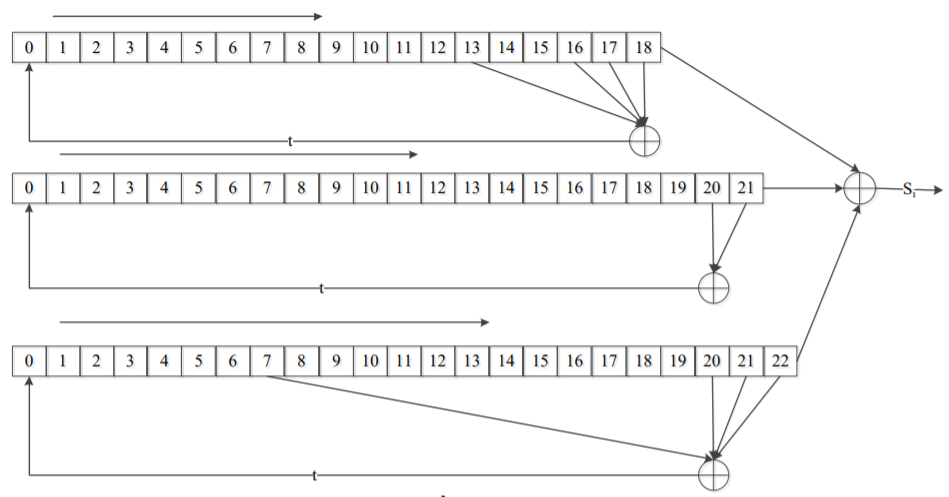
**Câu 1: Hãy trình bày đặc điểm chính của mã hóa khóa bí mật? Vẽ sơ đồ minh họa quy trình mã hóa và giải mã của kỹ thuật mã hóa khóa bí mật?**

Trong mã hóa khóa đối xứng, quá trình mã hóa và giải mã **sử dụng chung** 1 khóa, khóa này đgl **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 lần lượt là 19, 22 và 23 bit. Các bước quay X, Y, Z cụ thể như sau:

* Quay X gồm các thao tác:
  + t=x13 ⊕ x16 ⊕ x17 ⊕ x18
  + xj=xj-1 với j= 18, 17,1 6, 15, …4, 3, 2, 1
  + x0=t
* Quay Y gồm các thao tác:
  + t=y20 ⊕ y21
  + yj=yj-1 với j= 21, 20, …4, 3, 2, 1
  + y0=t
* Quay Z gồm các thao tác :
  + t=z7 ⊕ z20 ⊕ z21 ⊕ z22
  + zj=zj-1 với j= 22, 21,…6, 5, 4, 3, 2, 1
  + z0=t
* Hàm maj tính được trên 3 bit x8; y10; z10. Sau khi xoay xong bit sinh ra là si=x8 ⊕ y10 ⊕ z10



**Câu 3: Hãy mô tả các bước mã hóa RC4?**

Cơ chế hoạt động của RC4:

* 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;

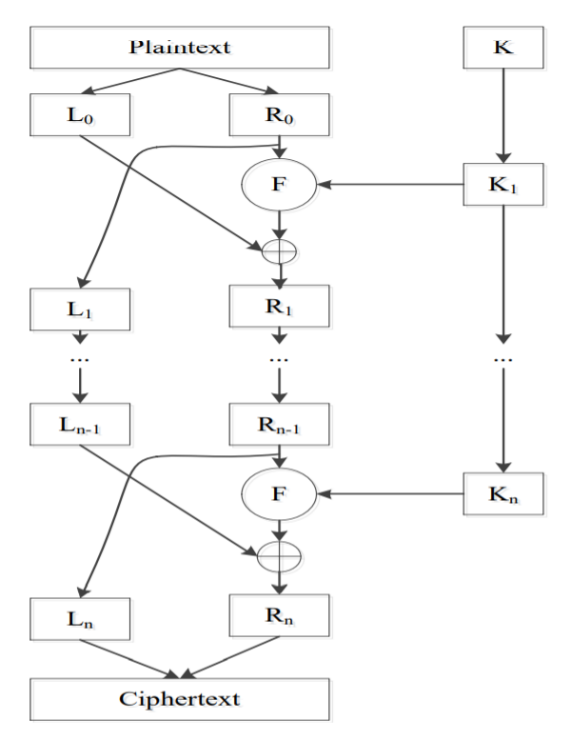
Swap (S[i], S[j]);

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

k = S[t];

end while;

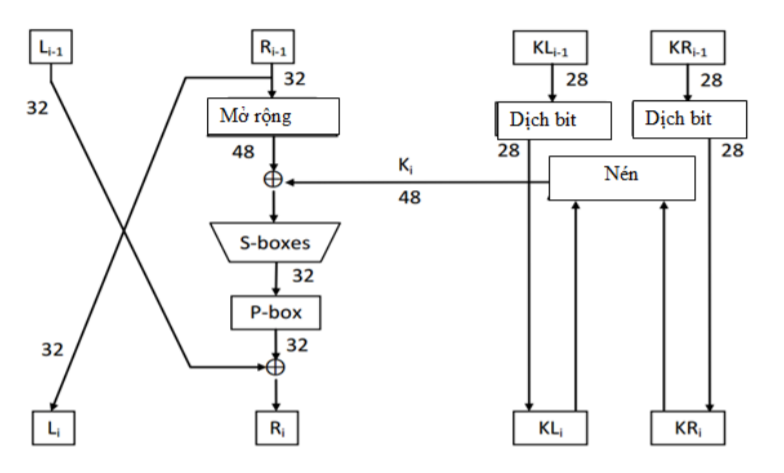
**Câu 4: Hãy mô tả cấu trúc khối Feistel? Hãy vẽ sơ đồ mã hóa theo nguyên tắc cấu trúc khối Feistel?**

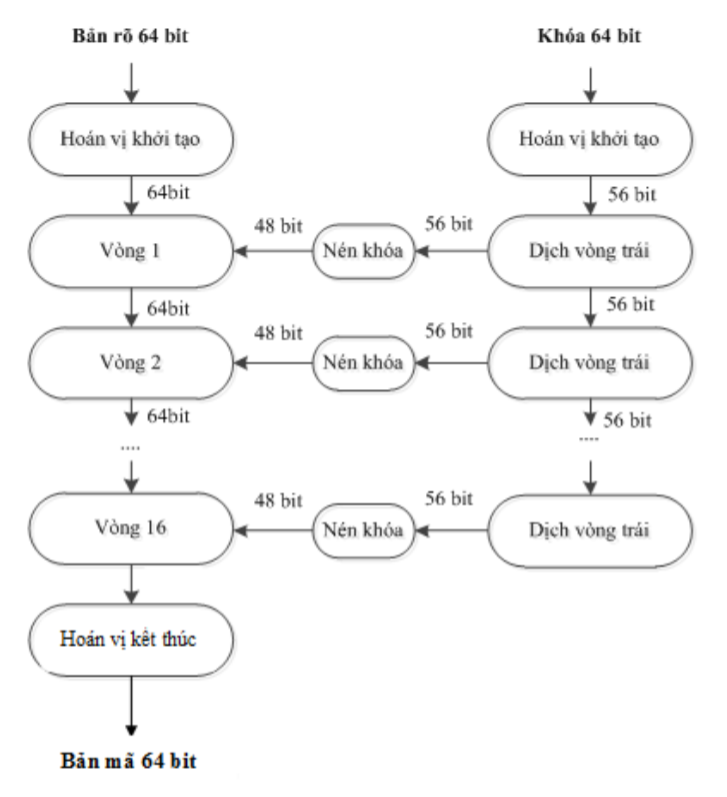
* Đầu vào của thuật toán mã hóa là khối văn bản gốc có chiều dài 2w bit và một khóa K. Khối thông điệp gốc được chia thành hai nửa, L0 và R0. Hai nửa này đi qua n vòng xử lý rồi tổ hợp để tạo ra khối bản mã hóa.
* Tất cả các vòng có cấu trúc tương tự nhau. Mỗi vòng i có đầu vào Li-1 và Ri-1 lấy từ vòng trước đó, 1 khoá con Ki lấy từ tổng thể K (các Ki khác nhau và khác K).
* Một thay thế được thực hiện trên một nửa trái của dữ liệu bằng cách áp dụng một hàm vòng F (có tham số là khóa con Ki) cho nửa bên phải của dữ liệu, và sau đó lấy XOR các đầu ra của hàm đó với nửa còn lại của dữ liệu.
* Sau khi thực hiện thay thế, một hoán vị được thực hiện màbao gồm việc trao đổi hai nửa của dữ liệu

**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?**

Thuật toán mã hóa DES tiến hành theo 4 bước chính:

* Hoán vị khởi tạo:
* Bản rõ được chia thành các khối 64 bit và lần lượt được đưa vào ma trận hoán vị IP
* Sinh khóa con 56 bit từ khóa 64 bit
* 16 vòng Feistel:
* Tại mỗi vòng, khóa và bản rõ đều được chia thành 2 phần có độ dài bằng nhau (Li = Ri = 32 bit và KLi = KRi = 28 bit)
* Ri sẽ đi qua hàm mở rộng để khuếch tán 32 bit -> 48 bit.
* Hai phần của khóa sau khi dịch vòng trái sẽ được gộp lại sau đó nén xuống 48 bit.
* Ri sau khi mở rộng sẽ XOR với Ki sau khi nén.
* Kết quả phép XOR được chia thành 8 phần 6 bit và đưa vào 8 S-Box.
* Mỗi S-Box biến đổi đầu vào 6 bit thành đầu ra 4 bit.
* 32 bit đầu ra từ 8 S-Box được hoán vị khi đi qua P-Box, sau đó XOR với Li để tạo thành R(i+1)
* L(i+1) là Ri ở đầu vòng Feistel.



* Hoán vị kết thúc: kết quả sau 16 vòng Feistel được đưa vào ma trận hoán vị

Thuật toán mã hóa DES yêu cầu 16 vòng lặp vì: 16 vòng lặp đảm bảo các phương thức tấn công sử dụng KPA cần 2^44 đến 2^47 cặp bản rõ – mã khác nhau (quá lớn) ~ brute với 2^56 trường hợp thử khóa => tương đối an toàn.

Ngược lại khi sử dụng hơn 16 vòng, mặc dù độ an toàn tăng lên nhưng đồng thời, thời gian và chi phí tính toán cũng tăng đáng kể => sử dụng 16 vòng lặp giúp cân bằng về cả độ an toàn lẫn hiệu năng.

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

Ưu điểm:

* Có tính xáo trộn và tính khuếch tán: mỗi bit của bãn mã dựa trên nhiều bit của khóa, và thay đổi mỗi bit của bản rõ làm thay đổi trung bình 1 nửa số bit của bản mã.
* Dễ cài đặt do cấu trúc Feistel không phức tạp và sử dụng chung 1 thuật toán cho quá trình giải mã và mã hóa.
* Giải mã bằng phương pháp phá mã tuyến tính cũng cần yêu cầu 2^43 bản rõ ~ tấn công vét cạn. (tuy nhiên với phần cứng hiện nay thì 2^43 cũng không phải vấn đề khó)

Nhược điểm:

* Thời gian mã hóa và giải mã lâu (với phần cứng hiện nay thì giải mã và mã hóa DES chỉ mất dưới 1 giây)
* Độ dài khóa ngắn: khóa có độ dài 64 bit và thực tế chỉ có 56 bit được sử dụng

**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

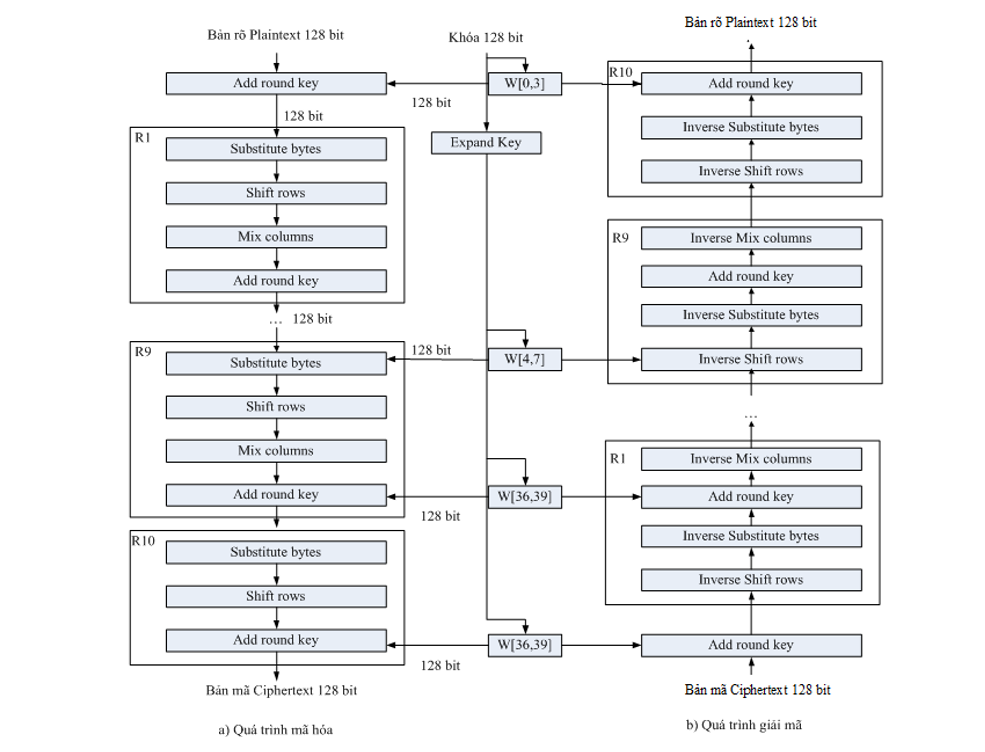
b(x)=b7x^7+b6x^6+b5x^5+b4x^4+b3x^3+b2x^2+b1x^1+1

=> 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?**

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 :
  + SubBytes: phép thế (phi tuyến) trong đó mỗi byte trong trạng thái sẽ được thế bằng một byte khác theo bảng tra (Rijndael S-box).
  + 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.
  + 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.
  + AddRoundKey .
* Vòng lặp cuối :
  + SubBytes
  + ShiftRows
  + AddRoundkey

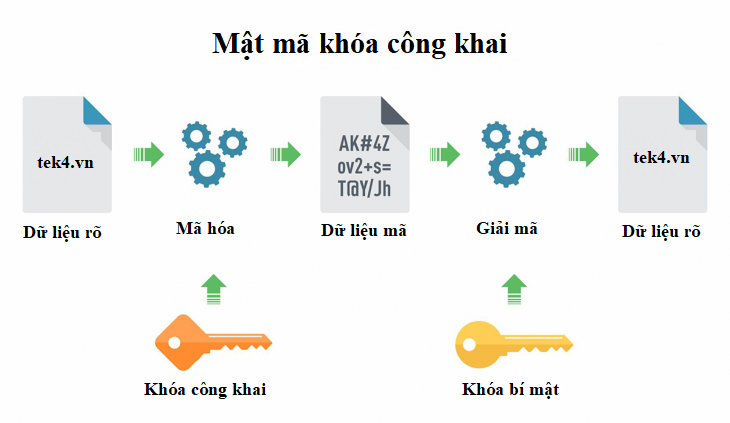


**CHƯƠNG III: Mã hóa khóa bất đối xứng**

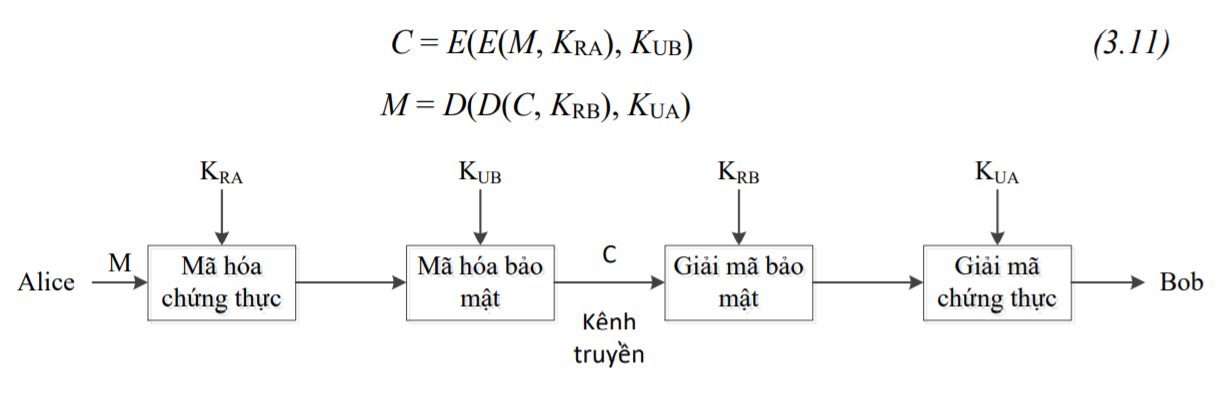
**Câu 1: Hãy trình bày đặc điểm chính của thuật toán mã hóa công khai? Vẽ sơ đô minh họa quy trình mã hóa và giải mã của thuật toán mã hóa công khai?**

Mã hóa khóa công khai sử dụng 1 cặp khóa gồm:

* Khóa dùng để mã khóa đgl khóa công khai. Khóa này được công khai với tất cả mọi, bất cứ ai cũng có thể sử dụng khóa này để mã hóa thông điệp.
* Khóa dùng để giải mã đgl khóa bí mật. Khóa này được giữ bí mật, chỉ có 1 người giữ khóa này mới có thể giải mã thông điệp được mã hóa bằng khóa công khải.

Khóa bí mật và khóa công khai phải là 1 cặp duy nhất, chỉ có sử dụng đúng khóa bí mật mới có thể giải mã thông điệp mã hóa bởi khóa công khai.

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



Các ký hiệu:

* Khóa công khai của Alice: Kua
* Khóa riêng của Alice: Kra
* Khóa công khai của Bob: Kub
* Khóa riêng của Bob: Krb

Trong trường hợp Alice muốn gửi tin cho Bob với đủ 2 yêu cầu:

* Thông tin phải bí mật, chỉ Bob mới có thể giải mã thông điệp.
* Bob chắc chắn người gửi là Alice, chứ không phải ai khác cũng mã hóa tin bằng khóa công khai của Bob (Kub)

Các bước:

1. Alice mã hóa chứng thực A bằng khóa riêng của mình (Kra), chứng thực này có thể được giải mã bằng khóa công khai của Alice (Kua) => Khi Bob giải mã chứng thực bằng Kua được thông điệp có nghĩa thì chắc chắn người gửi là Alice.
2. Alice mã hóa thông điệp muốn trao đổi và chứng thực đã mã hóa bằng khóa công khai của Bob (Kub) => Chỉ Bob mới có thể giải mã bằng khóa bí mật của mình (Krb).
3. Alice gửi thông điệp cho Bob.
4. Bob giải mã thông điệp bằng khóa riêng của mình (Krb) và nhận được 1 thông điệp và 1 bản mã.
5. Bob tách bản mã ra, giải mã nó bằng khóa công khai của Alice (Kua). Nếu giải mã ra thông điệp có nghĩa thì Bob chắc chắn được người gửi tin là Alice.

**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 với các tham số sinh khóa p và q

* Các số nguyên tố p và q phải được chọn sao cho việc phân tích n (n = p × q) là không khả thi về mặt tính toán.
* p và q nên có cùng độ lớn (tính bằng bit) và phải là các số đủ lớn. Độ lớn của p và q nên bằng khoảng ½ độ lớn của n. Hiện nay các tiêu chuẩn bảo mật cao như PCI DSS yêu cầu độ lớn tối thiểu của n là 4096 bit.
* Hiệu số p – q không nên quá nhỏ, do nếu p – q quá nhỏ, tức p ~ q và p ~ √𝑛. Như vậy, có thể chọn các số nguyên tố ở gần √𝑛 và thử. Khi có được p, có thể tính q và tìm ra d là khóa bí mật từ khóa công khai e và phi(n) = (p - 1)(q - 1). Nếu p và q được chọn ngẫu nhiên và p – q đủ lớn, khả năng hai số này bị phân tích từ n giảm đi.

Yêu cầu với số mũ mã hóa e:

* Không nên sử dụng e quá nhỏ. Tuy tốc độ mã hóa nhanh hơn khi e nhỏ, nhưng cũng vì thế chi phí cho việc phân tích ra số mũ giải mã d và tấn công vét cạn không quá lớn.
* Không nên sử dụng e quá lớn vì sẽ làm tốc độ mã hóa chậm hơn rất nhiều, làm giảm hiệu năng thuật toán.

=> Nên chọn e lớn vừa đủ và thêm chuỗi ngẫu nhiên vào bản rõ trước khi mã hóa để đảm bảo sự cân bằng giữa tốc độ và tính bí mật.

Yêu cầu với số mũ giải mã d:

* Không nên sử dụng số mũ giải mã d quá nhỏ. Tuy tăng tốc độ giải mã nhưng khi d nhỏ và gcd(p – 1, q - 1) cũng nhỏ thì có thể dễ dàng phân tích ra d từ (e. n) => Sử dụng d đủ lớn.

**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?**

**Quá trình sinh khóa RSA**:

1. Chọn 2 số nguyên p và q
2. Tính số modulo n = p\*q
3. Tính giá trị hàm ơ-le phi(n) = (p - 1)\*(q - 1)
4. Chọn số e sao cho 0 < e < phi(n) và gcd(e, phi) = 1
5. Chọn số d sao cho (e\*d) mod phi(n) = 1 (tức d và 1/e đồng dư trong modulo phi)

=> Khóa công khai là cặp (e, n) ; Khóa bí mật là cặp (d, n)

**Quá trình mã hóa RSA**:

* Mã hóa thông điệp: c = m^e mod n
* Mã hóa chứng thực c = m^d mod n

**Quá trình giải mã RSA**:

* Giải mã thông điệp: m = c^d mod n
* Giải mã chứng thực: m = c^e mod n

**Ví dụ**:

* Bãn rõ m = 32, p = 5, q = 7
* n = p \* q = 5 \* 7 = 35
* phi = (p - 1)\*(q – 1) = 4\*6 = 24
* Chọn số e: 0 < e < 24 và gcd(e, 24) = 1 => e = 5
* Chọn số d: e\*d mod 24 = 1 => d = 29
* Mã hóa: c = m^e mod n = 32^5 mod 35 = 2
* Giải mã: m = c^d mod n = 2 ^ 29 mod 35 = 32

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

Độ an toàn của thuật toán RSA dựa trên **độ khó** của việc **phân tích số nguyên lớn** thành các thừa số nguyên tố.

Khóa công khai của thuật toán RSA gồm 2 số e và n. Trong đó số n là quan trọng do để giải mã thông điệp cần khóa bí mật (d, n). Số mũ giải mã d là nghịch đảo modulo của e trong phi(n) – có thể tính được d khi có e và phi(n) bằng giải thuật Euclid mở rộng.

Vì p và q là 2 số nguyên tố nên giá trị hàm số ơ-le phi(n) = (p - 1)\*(q – 1). Nên nếu n không đủ lớn thì có thể dễ dàng phân tích ra 2 số nguyên tố q và p, từ đó có thể tìm ra khóa bí mật.

Ngày nay các chuẩn an toàn đối với các ứng dụng thanh toán ngân hàng như PCI DSS yêu cầu độ lớn tối thiểu của n là 4096 bit.

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

Ưu điểm:

* Độ an toàn cao do kích thước khóa lớn
* Việc quản lý và phân phối khóa dễ dàng hơn so với mã hóa khóa đối xứng.

Nhược điểm:

* Tốc độ mã hóa, giải mã chậm hơn so với mã hóa khóa 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: Hàm băm**

**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?**

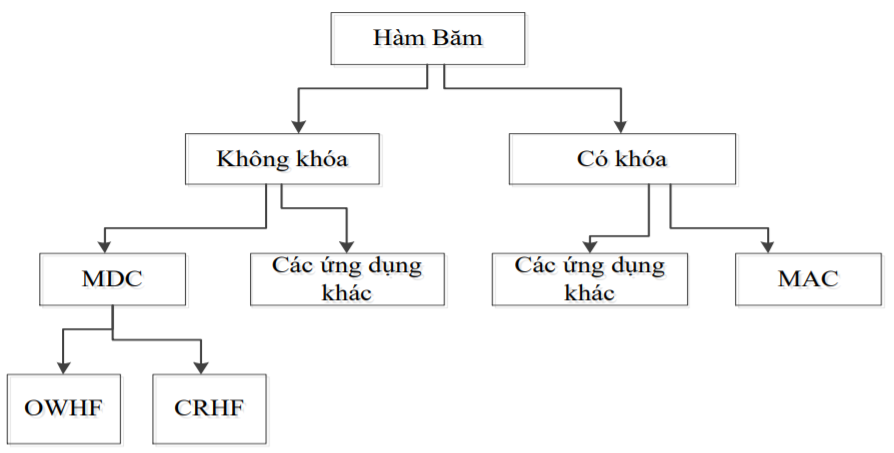
Hàm băm không khóa:

* 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 = H(m).
* 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)

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 khóa sử dụng:

* 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).

Theo chức năng:

* 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?**

Input : Chuỗi đầu vào x có độ dài r = 64t với t ≥ 2

Output : Chuỗi đầu ra sau khi băm có kích thước 128 bit.

Mô tả thuật toán:

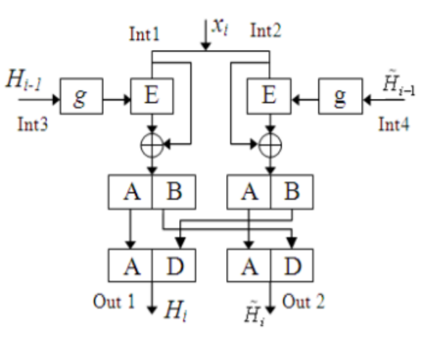
1. Phân xâu x ra làm các khối 64 bit xi : x1...x64
2. Chọn các hàng số đầu vào H0 từ một tập giá trị định trước (dạng HEXA).
   * 1. H0 = 0x5252525252525252
     2. H0 = 0x2525252525252525
3. Ký hiệu || là phép ghép và CiL, CiR là các nửa 32bit phải và trái của Ci

Đầu ra h(x) = Ht | |Ht được xác định như sau (1 ≤ i ≤ t)

ki = g(Hi-1)

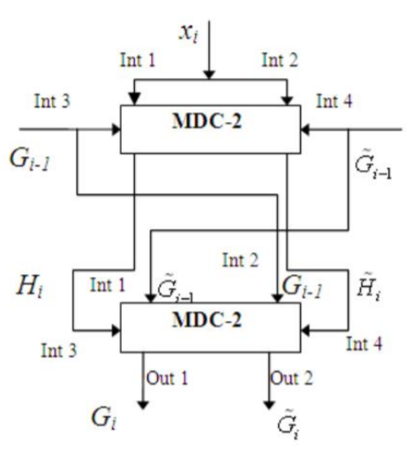
Ci = Eki(xi) ⊕ i

Hi = CiL || CiR



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

< include MDC 2 >



**Câu 6: Hãy mô tả thuật toán MAC?**

Input : Dữ liệu đầu vào x, hàm mã hóa khối E, khóa MAC bí mật k của E.

Output : n bit MAC trên x (n là độ dài khối của E)

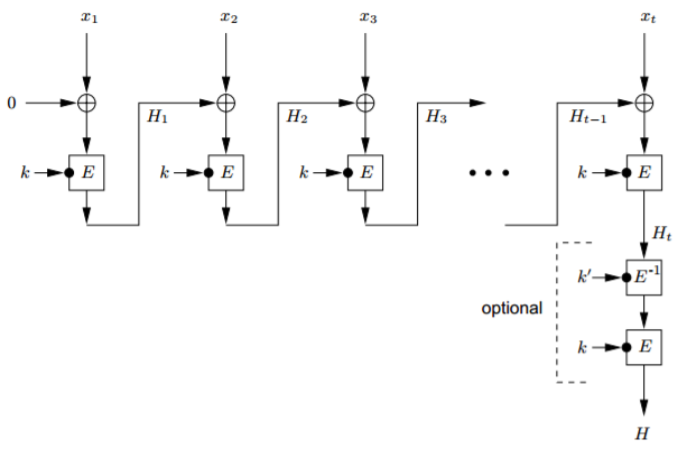
Mô tả thuật toán:

* Đệm và chia khối: Đệm thêm các bit vào x sao cho dữ liệu đầu vào chia thành từng khối n bit : x1,x2,...,xt.
* Xử lý theo chế độ CBC
* Ký hiệu Ek là phép mã hóa E với khóa k
* Tính khối Ht như sau:

H1 ← Ek(x1)

Hi ← Ek(Hi-1⨁ xi) với 2 ≤ i ≤ t

* Xử lý tăng thêm sức mạnh của MAC:
* Dùng một khóa bí mật k' ≠ k.
* Tính Ht’←Ek’-1 (Ht), Ht = Ek (Ht’)
* Hoàn thành. Hàm MAC là khối n bit H



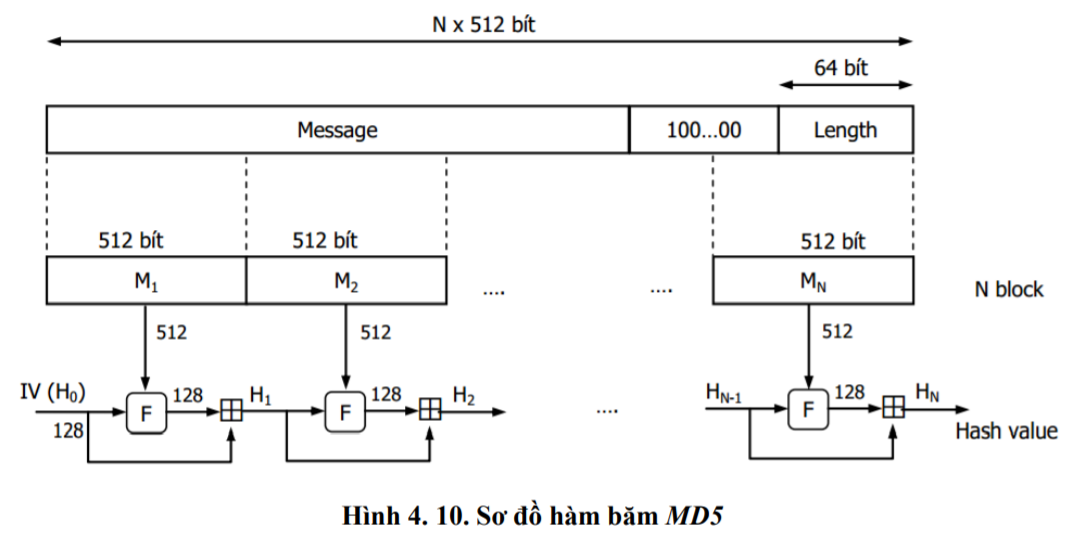
**Câu 7: Hãy trình bày về hàm băm MD5? Hãy vẽ sơ đồ minh họa về hàm băm MD5?**

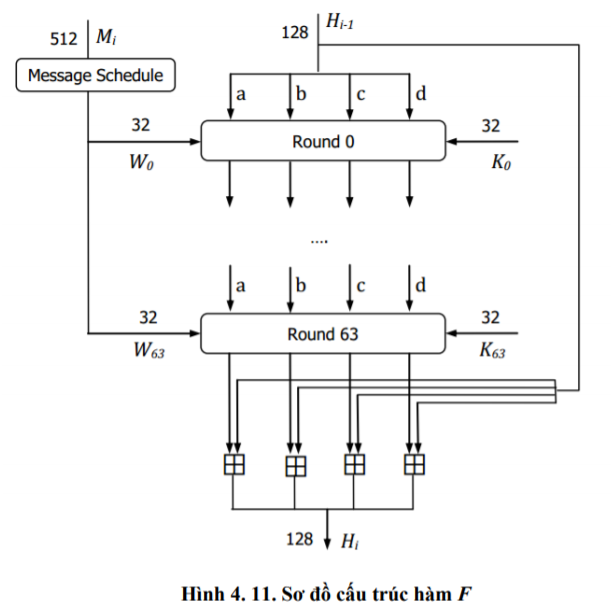
Đầu vào của thuật toán MD5 có độ dài tối đa bit. Chuỗi giá trị băm đầu ra của MD5 có độ dài 128 bit và thường được biểu diễn dưới dạng 32 số hexa.

Quá trình xử lý thông điệp của MD5 được chia thành 2 khâu: tiền xử lý và các vòng lặp xử lý:

* Tiền xử lý: Thông điệp được chia thành các khối 512 bit (16 từ 32 bit). Nếu kích thước thông điệp không là bội số của 512 thì nối thêm số bit còn thiếu.
* Các vòng lặp xử lý: Phần xử lý chính của MD5 làm việc trên state 128 bit, chia thành 4 từ 32 bit (A, B, C, D):
* Các từ A, B, C, D được khởi trị bằng một hằng cố định
* Từng phần 32 bit của khối đầu vào 512 bit được đưa dần vào để thay đổi state
* Quá trình xử lý gồm 4 vòng, mỗi vòng gồm 16 thao tác tương tự nhau
* Mỗi thao tác gồm: Xử lý bởi hàm F (4 dạng hàm khác nhau cho mỗi vòng), Cộng modulo và Quay trái.

|  |  |
| --- | --- |
|  |  |



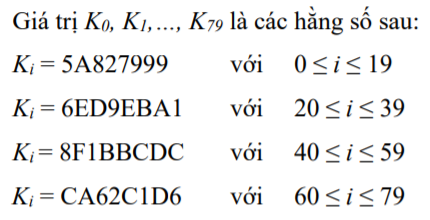


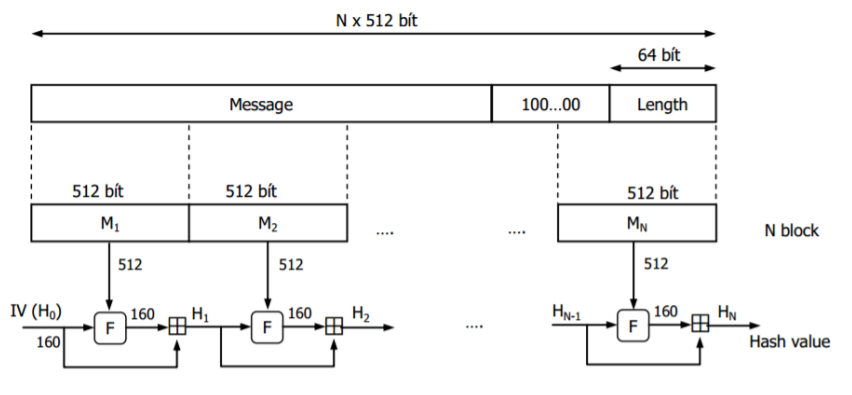
**Câu 8: Hãy trình bày về hàm băm SHA -1? Hãy vẽ sơ đồ minh họa về mà băm SHA-1?**

Chuỗi giá trị băm đầu ra của SHA1 có độ dài 160 bit và thường được biểu diễn dưới dạng 40 số hexa. Quá trình xử lý thông điệp của SHA1 tương tự MD5 được chia thành 2 khâu: tiền xử lý và các vòng lặp xử lý:

* Tiền xử lý: Thông điệp được chia thành các khối 512 bit (16 từ 32 bit). Nếu kích thước thông điệp không là bội số của 512 thì nối thêm số bit còn thiếu.
* Các vòng lặp xử lý: Phần xử lý chính của MD5 làm việc trên state 128 bit, chia thành 4 từ 32 bit (A, B, C, D):
* Các từ A, B, C, D được khởi trị bằng một hằng cố định
* Từng phần 32 bit của khối đầu vào 512 bit được đưa dần vào để thay đổi state
* Quá trình xử lý gồm 80 vòng, mỗi vòng gồm các thao tác: add, and, or, xor, rotate, mod.
* Mỗi thao tác gồm: Xử lý bởi hàm F (4 dạng hàm khác nhau cho mỗi vòng), Cộng modulo và Quay trái.

|  |  |
| --- | --- |
|  |  |





**CHƯƠNG V: Quản lý khóa**

**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?**

|  |  |
| --- | --- |
| KDC | KTC |
| Mỗi người dùng chỉ cần có 1 khóa chia sẻ với KDC (hoặc KTC) còn khóa dùng để chia sẻ dữ liệu giữa những người dùng sẽ do KDC (hoặc KTC) cung cấp. | |
| - A có khóa bí mật KA với KDC; - B có khóa bí mật KB với KDC; - KDC sẽ cung cấp khóa dùng để trao đổi dữ liệu giữa A và B (KAB). | - A sở hữu khóa dài hạn KAT – chia sẻ với KTC; - B sở hữu khóa dài hạn KBT – chia sẻ với KTC; - Trung tâm dịch khóa T là một máy chủ tin cậy, cho phép hai bên A và B không trực tiếp chia sẻ thông tin khóa thiết lập kênh truyền thông an toàn sử dụng hai khóa dài hạn KAT và KBT. |
| Quy trình trao đổi khóa diễn ra như sau: - A gửi yêu cầu muốn trao đổi dữ liệu với B cho KDC nhằm mục đích lấy được khóa chung KAB. Yêu cầu này không cần thiết phải mã hóa, nó chứa định danh của A và định danh của B; - KDC tạo ra một khóa bí mật KAB và mã hóa thành 2 bản: Một bản được mã hóa bằng khóa bí mật của A – E(KAB, KA); một bản được mã hóa bằng khóa bí mật của B –E(KAB, KB); - KDC gửi trả về cho A 2 bản mã này. A giải mã 1 bản bằng khóa bí mật KA của mình để lấy ra KAB và gửi bản còn lại cho B. B giải mã bằng khóa bí mật KB của B để lấy được KAB; - A và B trao đổi dữ liệu với nhau qua bằng khóa KAB. Kết thúc quá trình trao đổi dữ liệu, KAB sẽ được hủy bỏ. Nếu lần sau A muốn trao đổi dữ liệu với B thì KDC sẽ tạo ra một khóa KAB khác. | Các bước thực hiện cụ thể: - Đầu tiên, A mã hóa thông điệp bí mật M (M là 1 khóa phiên) và số định danh của B (người nhận) sử dụng khóa KAT và gửi thông điệp kèm theo số định danh của A cho T; - T nhận được thông điệp từ A. T giải mã thông điệp, xác định được người nhận là B. T mã hóa M sử dụng khóa KBT. Tiếp theo, T gửi lại thông điệp đã mã hóa cho A để A để chuyển cho B; - Sau khi B nhận được thông điệp từ A, B giải mã thông điệp sử dụng khóa KBT để có được M; - A và B sử dụng khóa phiên M để trao đổi dữ liệu với nhau. |

**4) Hãy nêu các bước chính trong quá trình trao đổi khóa của giao thức Needham-Schroeder?**

- **A → KDC: IDA || IDB || N1:** A gửi cho KDC định danh của A – IDA, định danh của B – IDB và nonce của A – N1 ;  
- **KDC → A: E(KS || IDB || N1 || E(KS || IDA, KB), KA):** KDC sẽ gửi cho A một bản tin được mã hóa bằng khóa bí mật của A với KDC (KA). Bản tin này chứa khóa phiên KS, IDB, N1 và 1 “vé” được mã hóa riêng dành cho B. Vé này chứa KS và IDA, được mã hóa bằng khóa bí mật của B với KDC (KB);  
- A giải mã sẽ lấy được KS và vé của B - E(KS || IDA, KB);  
- **A → B: E(KS || IDA, KB):** A gửi vé của B đến cho B;  
- **B → A: E(N2, KS):** B gửi đến cho A nonce của B được mã hóa bằng khóa phiên KS;  
- **A → B: E(f(N2), KS):** A gửi đến cho B giá trị f(N2) được mã hóa bằng KS. Hàm f là một hàm bất kỳ được chọn sẵn từ trước. Mục đích của bước này là để B xác nhận xem có đúng là A đang trao đổi với mình hay không;

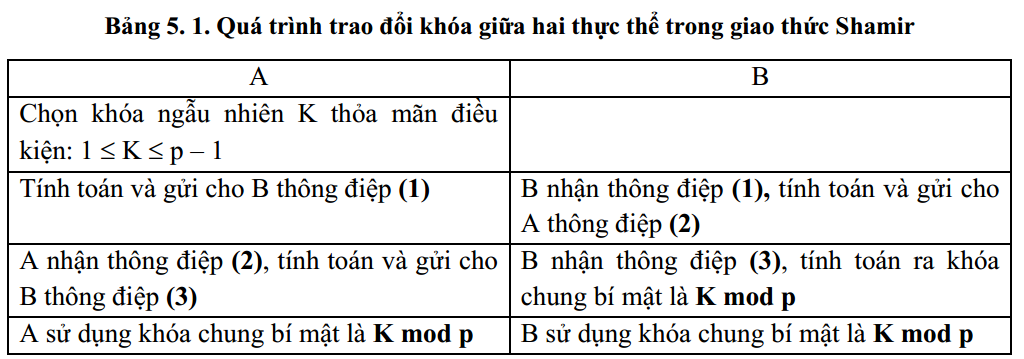
- Sau khi xác thực xong, A và B tiến hành trao đổi dữ liệu bằng KS.

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

- **A → B: M || IDA || IDB || E(M || IDA || IDB || NA, KA):** A gửi cho B một thông điệp bao gồm: nonce chung (M), định danh của A (IDA), định danh của B (IDB) và một “vé” được mã hóa bằng khóa bí mật của A với KDC (KA). Vé này chứa M, IDA, IDB, và nonce của A (NA) ;  
- **B → KDC: M || IDA || IDB || E(M || IDA || IDB || NA, KA) || E(M || IDA || IDB || NB, KB):** B tạo ra một “vé” tương tự bao gồm M, IDA, IDB, định danh của B (NA). Vé này được mã hóa bằng khóa bí mật của B với KDC (KB). B sẽ gửi đến KDC toàn bộ thông điệp nhận được từ A kèm theo vé vừa tạo;  
- **KDC → B: M || E(NA || KAB, KA) || E(NB || KAB, KB):** KDC tạo ra khóa phiên KAB, sau đó gửi cho B một thông điệp bao gồm:  
• Nonce chung M  
• Vé của A, được mã hóa bằng KA, chứa NA và KAB  
• Vé của B, được mã hóa bằng KB, chứa NB và KAB  
- **B → A: M || E(NA || KAB, KA):** B giữ lại vé của mình và gửi cho A thông điệp chứa M và vé của A; B giải mã vé của mình bằng KB để lấy được KAB; A giải mã vé của mình bằng KA để lấy được KAB;  
- A và B sử dụng KAB để trao đổi dữ liệu với nhau.

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

**-** Giao thức không khóa Shamir là giao thức cho phép 2 thực thể trao đổi thông tin mà không cần trao đổi trước khóa. Trong giao thức Shamir, hai bên không cần thỏa thuận  
trước khóa dùng chung mà chỉ cần tự lựa chọn cho mình tham số bí mật, tính toán và gửi  
cho bên liên quan giá trị tính toán cuối cùng. Độ an toàn của giao thức dựa trên bài toán  
logarit rời rạc với modulo của *p*.



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

**(Ngân hàng)**

**8) Hãy cho biết đặc điểm chung của các kỹ thuật phân phối khóa công khai?**

- Các kỹ thuật phân phối khóa công khai thường giả thiết các bên tham gia truyền thông sở hữu khóa công khai có tính xác thực (authentic public keys), tức là các khóa công khai được tạo ra và sử dụng hợp pháp. Việc phân phối khóa công khai cần đảm bảo tính xác thực của chủ thể khóa công khai.

Quá trình sinh khóa và truyền tin diễn ra như sau:  
- B sinh ra một cặp khóa: khóa công khai và khóa bí mật. Sau đó, B gửi cho A khóa công khai của mình qua một kênh truyền an toàn (chỉ dùng để xác thực);  
- A sau khi nhận được khóa công khai của B. A dùng khóa công khai của B để mã hóa bản rõ, sau đó gửi bản mã cho B qua một kênh truyền (không cần là kênh an toàn);  
- B nhận được bản mã sẽ dùng khóa bí mật của mình để giải mã và thu được bản rõ. Cũng giống như kỹ thuật phân phối khóa bí mật, trong kỹ thuật phân phối khóa  
công khai cũng có nhiều phương pháp phân phối khóa.

**9) Hãy trình bày về chứng chỉ xác thực khóa công khai X.509?**

X.509 (v3) là chứng chỉ xác thực khóa công khai được sử dụng phổ biến nhất hiện nay, do ITU đưa ra lần đầu tiên vào năm 1988. Dịch vụ xác thực X.509 được hầu hết các nhà cung cấp PKI hiện nay triển khai. Các thành phần của X.509 bao gồm:  
- *Version:* xác định phiên bản của chứng chỉ.  
- *Serial Number:* do CA cấp, là định danh duy nhất.  
- *Signature Algorithm:* chỉ ra thuật toán CA sử dụng để kí chứng chỉ.  
- *Issuer Name:* tên của CA thực hiện cấp chứng chỉ này.  
- *Validity Period:* chỉ ra khoảng thời gian chứng chỉ có hiệu lực, gồm 2 giá trị: “not before” – thời gian chứng chỉ bắt đầu có hiệu lực và “not after” – thời gian chứng chỉ hết  
hiệu lực.  
- *Subject Name:* xác định thực thể mà khoá công khai của thực thể này được xác nhận. Tên của subject phải là duy nhất đối với mỗi thực thể được CA xác nhận.  
- *Public Key:* chứa khoá công khai và những tham số liên quan; xác định thuật toán (ví dụ RSA) được sử dụng cùng với khoá.  
- *Issuer Unique ID:* là trường không bắt buộc, trường này cho phép sử dụng lại tên người cấp. Trường này hiếm được sử dụng trong triển khai thực tế.  
- *Subject Unique ID:* là trường tùy chọn, cho phép sử dụng lại tên của Subject khi quá hạn. Trường này cũng hiếm được sử dụng trong thực tế.  
- *Extensions:* chỉ có trong chứng chỉ X.509v3.  
- *Signature:* gồm có 3 phần. Phần 1 chứa tất cả những trường còn lại của chứng chỉ. Phần 2 chứa bản tóm tắt của phần 1 được mã hóa bằng khóa công khai của CA. Phần 3 gồm các thuật toán được sử dụng trong phần 2.  
Trong X.509 bao gồm 3 thủ tục xác thực tùy chọn**:**- *Xác thực một chiều (One-way Authentication*): giúp xác nhận danh tính của A và  
bản tin đúng là từ A gửi đi.

- *Xác thực hai chiều (Two-way Authentication):* Xác thực thực thể với tem thời gian

- *Xác thực ba chiều (Three-way Authentication)*: Xác thực thực thể sử dụng giao  
thức Thách thức – Trả lời.

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

- Phương pháp mã hóa khóa công khai có đặc điểm là thời gian mã hóa và giải mã chậm hơn phương pháp mã hóa khóa đối xứng. Chính vì thế, trong phân phối khóa, có một phương pháp kết hợp sử dụng khóa công khai để thiết lập khóa bí mật dùng cho mỗi phiên trao đổi dữ liệu.

Các bước thực hiện cụ thể như sau:  
- A gửi chứng chỉ xác thực CA của mình cho B;  
- B gửi chứng chỉ xác thực CB của mình cho A;  
- Sau khi đã xác thực với nhau, A tạo ra 1 khóa phiên KS và tiến hành 2 bước mã hóa:  
• Mã hóa KS bằng khóa bí mật KRA của A: E(KS, KRA);  
• Mã hóa E(KS, KRA) bằng khóa công khai của B: E(E(KS, KRA), KUB);  
A gửi cho B thông điệp vừa được mã hóa.  
- B nhận được thông điệp sẽ tiến hành 2 bước giải mã:  
• Dùng khóa bí mật của B để giải mã thông điệp, thu được E(KS, KRA);  
• Dùng khóa công khai của A để tiếp tục giải mã E(KS, KRA), thu được khóa phiên KS;  
Như vậy, A và B đã có thể dùng khóa phiên KS để tiến hành trao đổi thông tin. Sau khi kết thúc việc trao đổi thông tin, KS sẽ bị hủy bỏ.

**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?**

Các bước thực hiện**:**• Đầu tiên, Alice và Bob thỏa thuận dùng chung một số nguyên tố *p* và một số căn  
nguyên thủy *g;*• Alice chọn số ngẫu nhiên bí mật *a* (0 ≤ a ≤ p-2), tính:  
*A = ga mod p*Alice gửi cho Bob giá trị *A*

• Bob chọn số ngẫu nhiên bí mật *b (0 ≤ b ≤ p-2),* tính:  
*B = gb mod p*Bob gửi cho Alice giá trị B  
• Alice tính *s = Ba mod p*• Bob tính *s = Ab mod p*• Alice và Bob có khóa chung là *s* được sử dụng để trao đổi thông tin.

**-Lưu ý:** giao thức này không giới hạn việc thỏa thuận khóa chỉ cho hai bên tham gia. Bất kỳ số lượng người sử dụng nào cũng có thể tham gia vào giao thức để tạo khóa bí mật chung bằng cách thực hiện lặp lại các bước trao đổi thông tin và tính toán trong giao thức.