Câu 1: Hãy trình bày các giao thức thực hiện bảo mật, cách thức bảo vệ hệ thống khỏi sự xâm nhập và phá hoại từ bên ngoài.

Gợi ý: trình bày các giao thức thực hiện bảo mật (Keberos, X509, SSL, PGP và S/MIME, IPSET).

1. **Ker**

2. **3beros** là một giao thức mật mã dùng để xác thực trong các mạng máy tính hoạt động trên những đường truyền không an toàn. Giao thức Kerberos có khả năng chống lại việc nghe lén hay gửi lại các gói tin cũ và đảm bảo tính toàn vẹn của dữ liệu. Mục tiêu khi thiết kế giao thức này là nhằm vào mô hình client - server và đảm bảo xác thực cho cả hai chiều. Giao thức được xây dựng dựa trên mã hoá đối xứng và cần đến một bên thứ ba mà cả hai phía tham gia giao dịch tin tưởng.
3. **X.509** là một định dạng chuẩn cho chứng chỉ khóa công khai, các tài liệu kỹ thuật số liên kết an toàn các cặp khóa mật mã với các danh tính như trang web, cá nhân hoặc tổ chức.

   Các ứng dụng phổ biến của chứng chỉ X.509 bao gồm:

   - SSL/TLS và HTTPS để duyệt web xác thực và mã hóa
   - Email đã ký và được mã hóa thông qua S/MIME giao thức
   - Ký mã
   - Ký văn bản
   - Xác thực ứng dụng khách
   - ID điện tử do chính phủ cấp
   - Các ứng dụng phổ biến của chứng chỉ X.509 bao gồm SSL/TLS và HTTPS để duyệt web được xác thực và mã hóa, email đã ký và mã hóa qua S/MIME giao thức, kỹ mã, ký văn bản, xác thực ứng dụng khách và ID điện tử do chính phủ cấp
3. **SSL** là chữ viết tắt của Secure Sockets Layer là giao thức mã hóa dữ liệu được truyền tải từ máy khách đến server Hosting và ngược lại thông qua trình duyệt. Tất cả dữ liệu truyền điều được mã hóa. SSL CHỈ có tác dụng BẢO MẬT ĐƯỜNG TRUYỀN DỮ LIỆU (Bảo mật các gói tin được gửi đi trong quá trình vận chuyển - tránh việc chặn gói tin và giải mã chúng khi đang vận chuyển) chứ không phải cứ có SSL là website của Bạn không bị hack**.**
   - Xác thực website, giao dịch.

- Nâng cao hình ảnh, thương hiệu và uy tín doanh nghiệp.
- Bảo mật các giao dịch giữa khách hàng và doanh nghiệp, các dịch vụ truy nhập hệ thống.
- Bảo mật webmail và các ứng dụng như Outlook Web Access, Exchange, và Office Communication Server.
- Bảo mật các ứng dụng ảo hó như Citrix Delivery Platform hoặc các ứng dụng điện toán đám mây.
- Bảo mật dịch vụ FTP.
- Bảo mật truy cập control panel.
- Bảo mật các dịch vụ truyền dữ liệu trong mạng nội bộ, file sharing, extranet.
- Bảo mật VPN Access Servers, Citrix Access Gateway …

4. **Mã hóa PGP** (Pretty Good Privacy) là một hệ thống được sử dụng cho việc mã hóa email và mã hóa các file nhạy cảm.

   Cách hoạt động:

Đầu tiên, PGP tạo session key ngẫu nhiên bằng cách sử dụng một trong hai thuật toán chính. Key này là một con số khổng lồ không thể đoán được, và chỉ được sử dụng một lần.

- Tiếp theo, session key này được mã hóa. Điều này được thực hiện bằng cách sử dụng public key của người nhận thư. Public key gắn liền với danh tính của một người cụ thể và bất kỳ ai cũng có thể sử dụng key này để gửi tin nhắn cho họ.
- Người gửi sẽ gửi PGP session key được mã hóa của họ cho người nhận và họ có thể giải mã bằng private key của họ. Sử dụng session key này, người nhận bây giờ có thể giải mã tin nhắn.

5. **IP Security (IPSec – Internet Protocol Security)** là một giao thức được chuẩn hoá bởi IETF (Internet Engineering Task Force) từ năm 1998 nhằm mục đích nâng cấp các cơ chế mã hoá và xác thực thông tin cho chuỗi thông tin truyền đi trên mạng bằng giao thức IP. Hay nói cách khác, IPSec là sự tập hợp của các chuẩn mở được thiết lập để đảm bảo sự cẩn mật dữ liệu, đảm bảo tính toàn vẹn dữ liệu và chứng thực dữ liệu giữa các thiết bị mạng.
6. **IPSEC**

- Bảo vệ kết nối từ các mạng chi nhánh đến mạng trung tâm thông qua Internet.
- Bảo vệ kết nối truy cập từ xa (Remote Access).

- Thiết lập các kết nối Intranet và Extranet .
- Nâng cao tính bảo mật của các giao dịch thương mại điện tử.

1.2.1 Ưu điểm

- Khi IPSec được triển khai trên bức tường lửa hoặc bộ định tuyến của một mạng riêng, thì tính năng an toàn của IPSec có thể áp dụng cho toàn bộ vào ra mạng riêng đó mà các thành phần khác không cần phải xử lý thêm các công việc liên quan đến bảo mật.
- IPSec được thực hiện bên dưới lớp TCP và UDP, đồng thời nó hoạt động trong suốt đối với các lớp này. Do vậy không cần phải thay đổi phần mềm hay cấu hình lại các dịch vụ khi IPSec được triển khai.
- IPSec có thể được cấu hình để hoạt động một cách trong suốt đối với các ứng dụng đầu cuối, điều này giúp che giấu những chi tiết cấu hình phức tạp mà người dùng phải thực hiện khi kết nối đến mạng nội bộ từ xa thông qua mạng Internet.

1.2.2 Hạn chế

- Tất cả các gói được xử lý theo IPSec sẽ bị tăng kích thước do phải thêm vào các tiêu đề khác nhau, điều này làm cho thông lượng hiệu dụng của mạng giảm xuống. Vấn đề này có thể được khắc phục bằng cách nén dữ liệu trước khi mã hóa, song các kĩ thuật như vậy vẫn còn đang nghiên cứu và chưa được chuẩn hóa.
- IPSec được thiết kế chỉ để hỗ trợ bảo mật cho lưu lượng IP, không hỗ trợ các dạng lưu lượng khác.
- Việc tính toán nhiều giải thuật phức tạp trong IPSec vẫn còn là một vấn đề khó đối với các trạm làm việc và máy PC năng lực yếu.
- Việc phân phối các phần cứng và phần mềm mật mã vẫn còn bị hạn chế đối với chính phủ một số quốc gia.

Đa dụng Internet Mail Extension (S / MIME) là một bảo vệ nâng cấp lên tiêu chuẩn định dạng e-mail Internet MIME dựa trên công nghệ của RSA Data Security

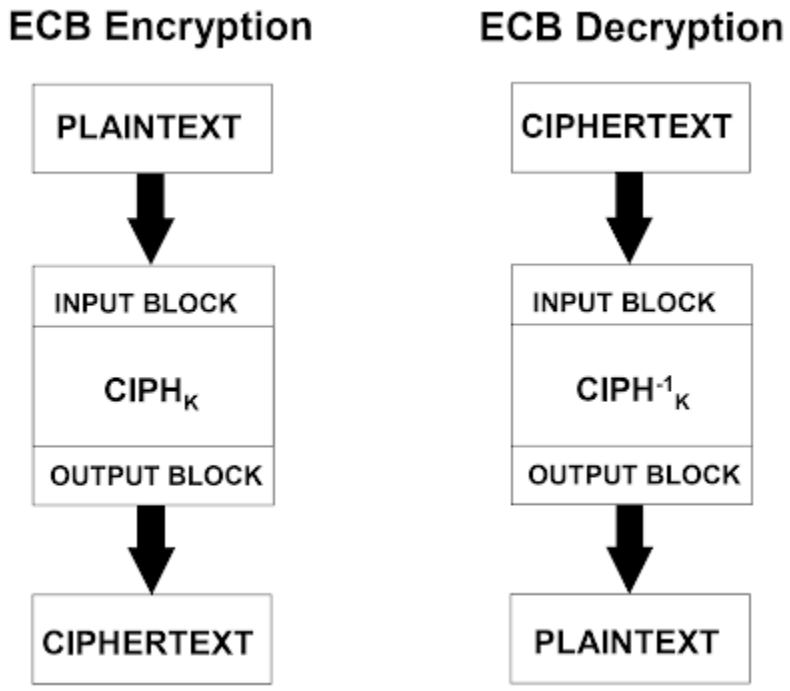
Cách thức bảo về hệ thống

Các thức bảo vệ: khái niệm Control Access (kiểm soát truy cập) dùng cho việc bảo vệ này (chứng thực và phân quyền), đồng thời sử dụng Firewall hoặc các hệ thống phát hiện chống xâm nhập IDS/IPS, kiểm lỗi phần mềm.

Câu 2: Trình bằng mô hình mã và giải mã khối Electronic Codebook – ECB, những ưu điểm và nhược điểm của ECB, CBC, CFB, OFB, CTR.

ECB (Electronic Codebook)

ECB là chế độ mã hóa từng khối bit độc lập. Với cùng một khóa mã K, mỗi khối plaintext ứng với một giá trị ciphertext cố định và ngược lại.



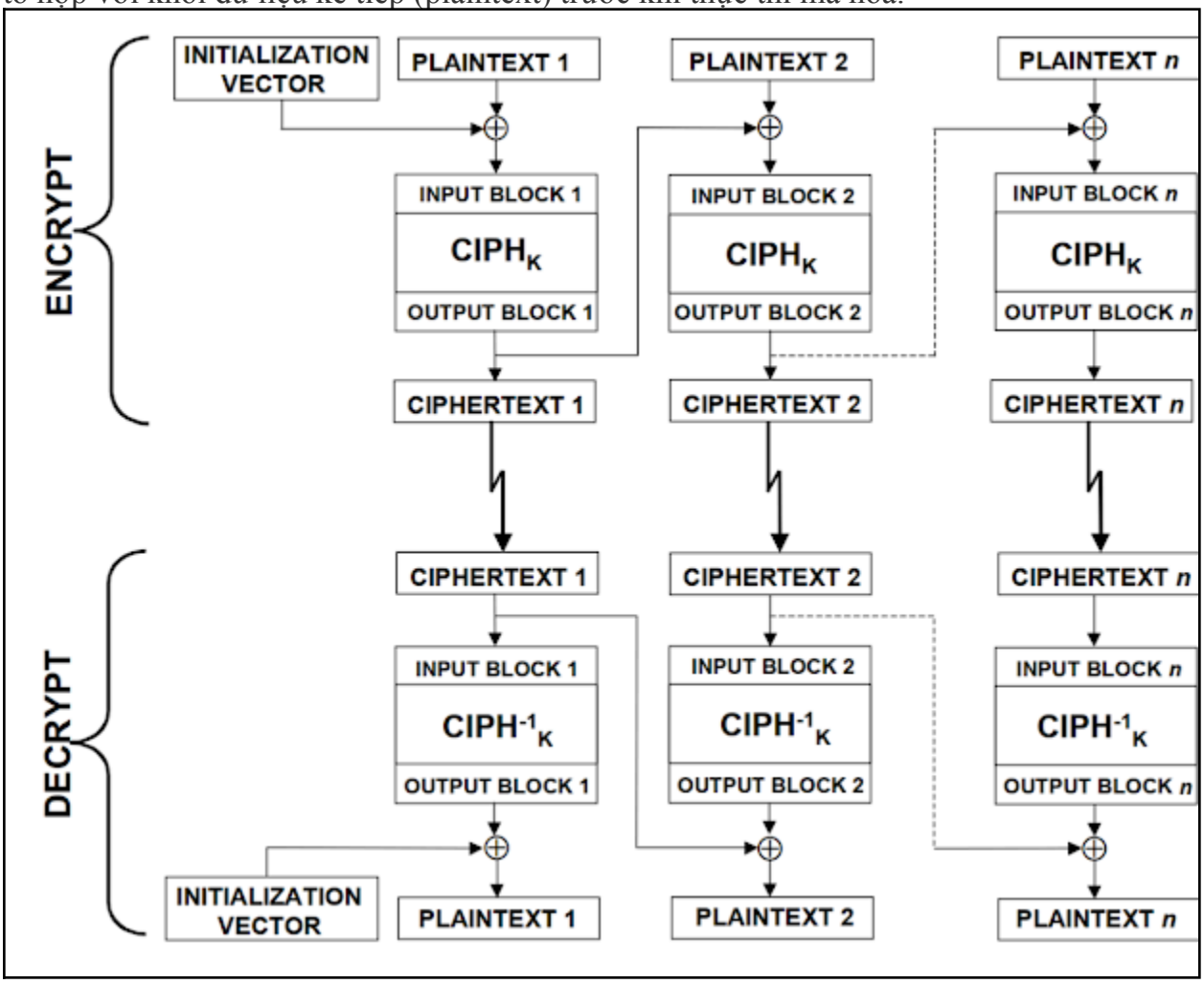
Ưu điểm:

- *Đơn giản*
- *Không cần đồng bộ hóa giữa bên gửi và nhận, nếu bên nhận không nhận đủ các khối, thì vẫn có thể giải mã các khối nhận được.*
- *Các bit lỗi sẽ không được đưa vào các khối kế sau.*
- *Vì các khối được mã hóa và giải mã hoàn toàn độc lập với nhau nên ECB cho phép mã hóa và giải mã đồng thời nhiều khối nếu có đủ phần cứng thực thi.*

Nhược điểm:

- *ECB về bản chất giống hệt với các mật mã bảng chữ cái cổ điển, chỉ có điều bảng chữ cái của ECB phức tạp hơn.*
- *Các khối bản rõ giống nhau sẽ được ánh xạ thành khối bản mã giống nhau (nếu dùng cùng 1 loại khóa), dẫn đến dễ tấn công bằng phương pháp thống kê tần suất.*
- *ECB dễ dàng bị phá nếu bản rõ lớn và có tính cấu trúc rõ ràng, từ đó ECB thường dùng để mã hóa những bản rõ ngắn như khóa bí mật.*
- *ECB song song hóa được, có cấu trúc quy luật -> độ an toàn yếu.*

CBC là chế độ mã hóa chuỗi, kết quả mã hóa của khối dữ liệu trước (ciphertext) sẽ được tổ hợp với khối dữ liệu kế tiếp (plaintext) trước khi thực thi mã hóa.



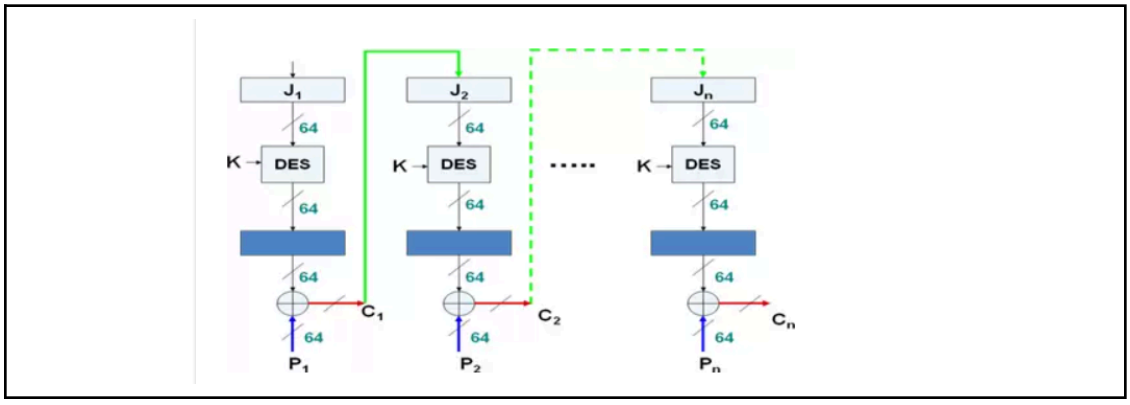
Ưu điểm:

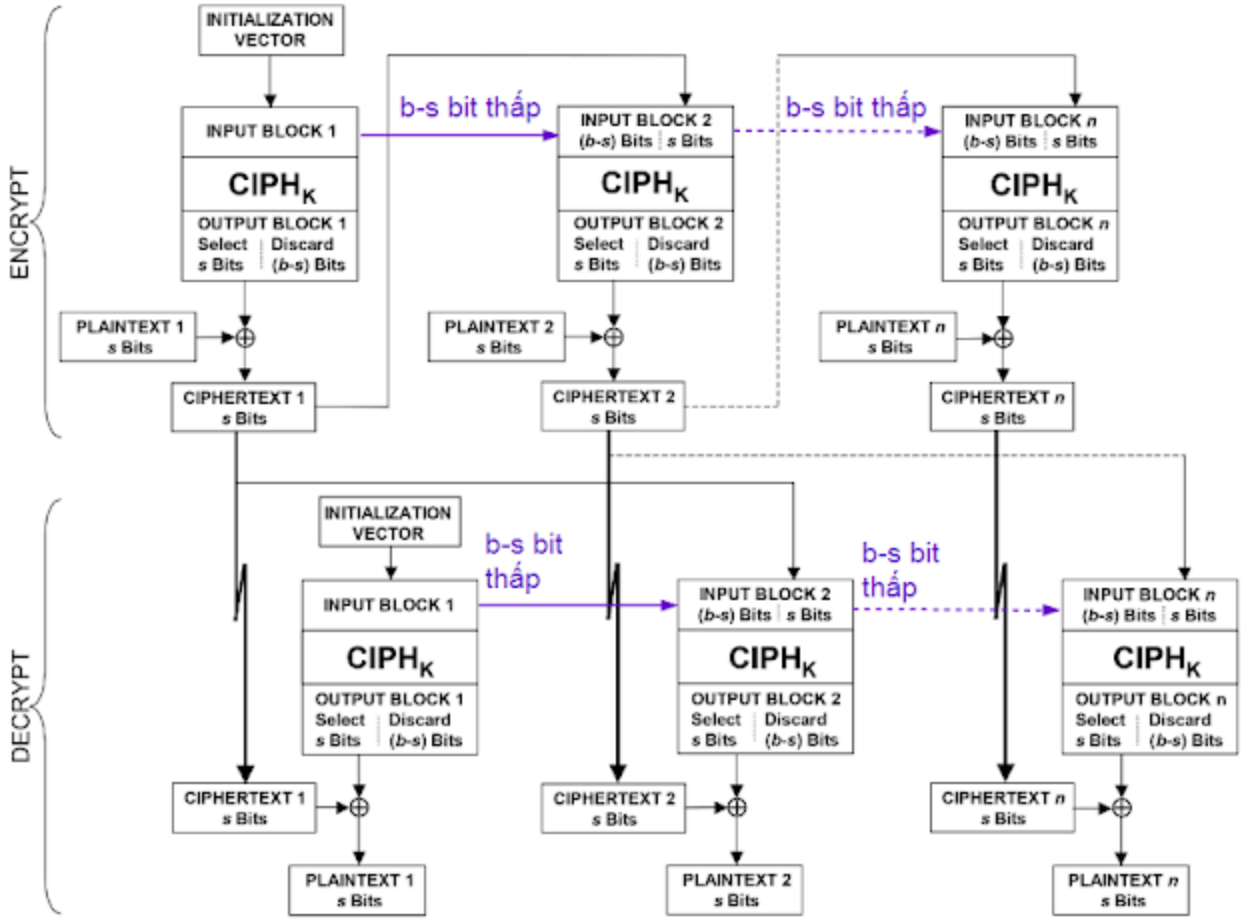
- Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào ***IV*** hoặc giá trị mã hóa (ciphertext) của khối dữ liệu liền trước.
- Quá trình giải mã (mã hóa nghịch) vẫn có thể thực hiện song song nhiều khối dữ liệu.

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.

CFB là chế độ mã hóa mà ciphertext của lần mã hóa hiện tại sẽ được phản hồi (feedback) đến đầu vào của lần mã hóa tiếp theo. Nghĩa là, ciphertext của lần mã hóa hiện tại sẽ được sử dụng để tính toán ciphertext của lần mã hóa kế tiếp. Mô tả có vẻ giống CBC nhưng quá trình trực hiện lại khác.





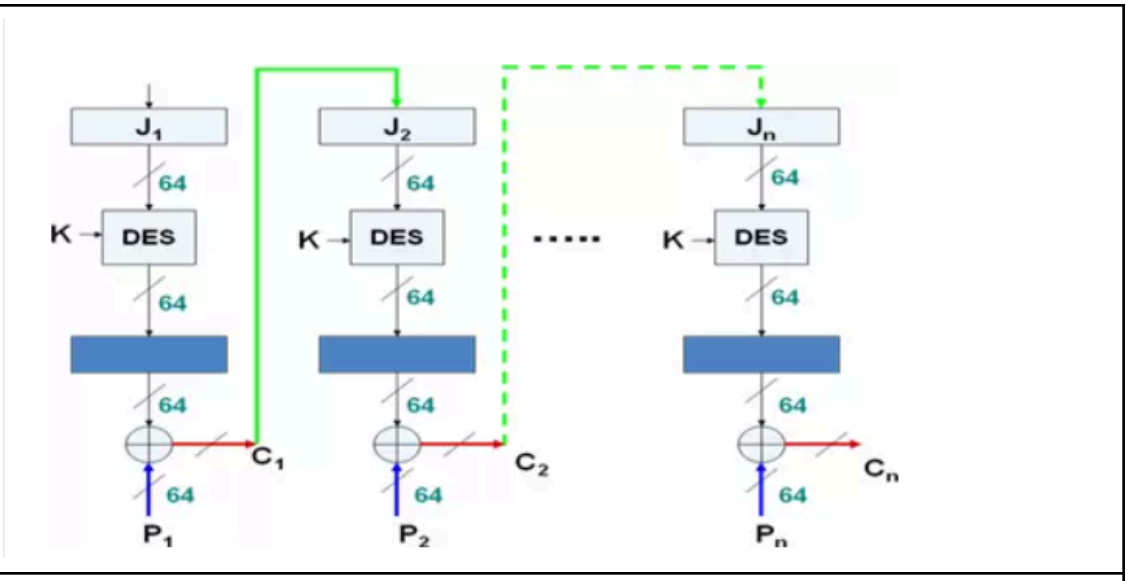
Ưu điểm:

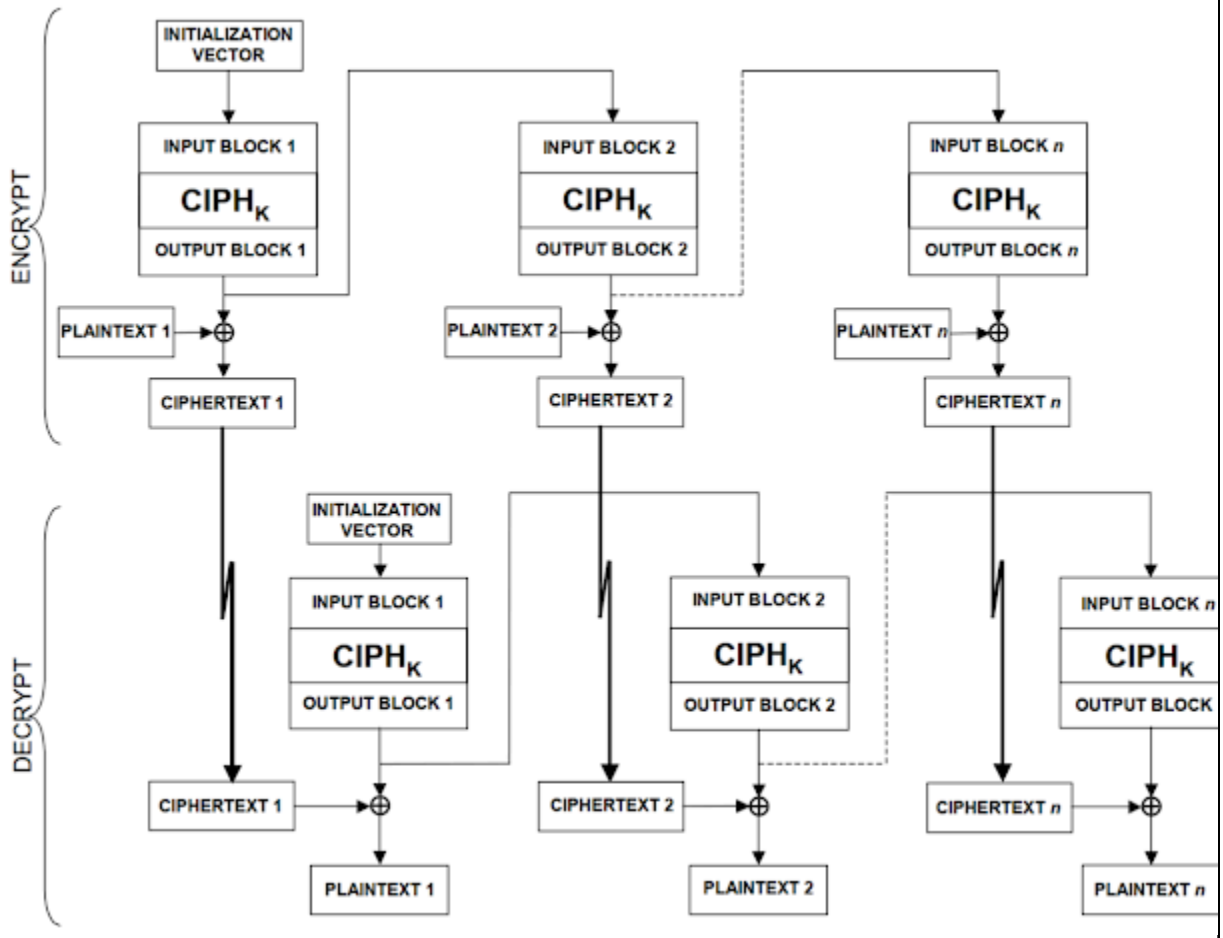
- Khả năng bảo mật cao hơn ECB. Ciphertext của một khối dữ liệu plaintext có thể khác nhau cho mỗi lần mã hóa vì nó phụ thuộc vào **IV** hoặc giá trị mã hóa (ciphertext) của khối dữ liệu liền trước.
- Quá trình giải mã (mã hóa nghịch) vẫn có thể thực hiện song song nhiều khối dữ liệu.
- Tùy biến được độ dài khối dữ liệu mã hóa, giải mã thông qua thông số **s**

Nhược điểm:

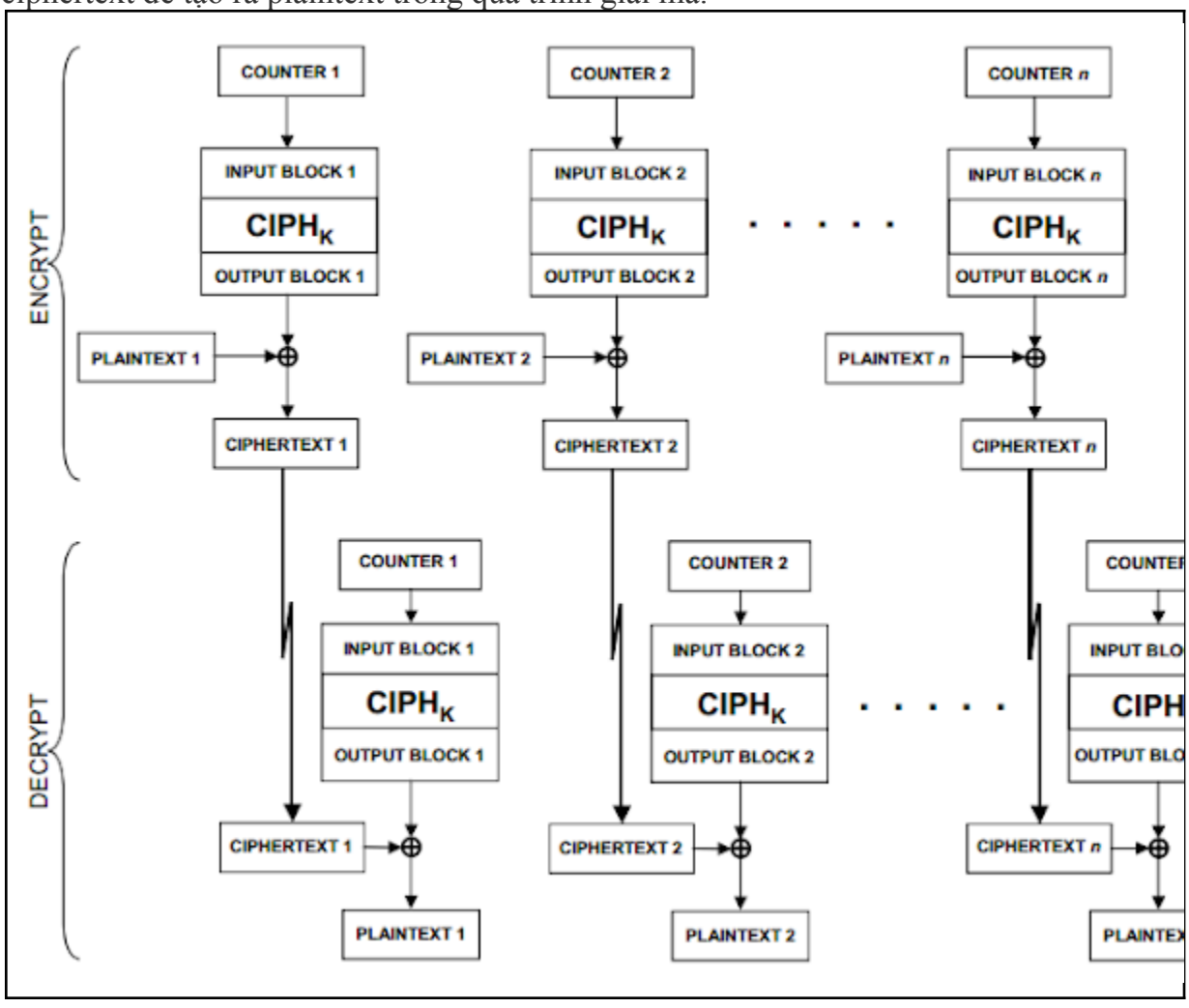
- Thiết kế phần cứng phức tạp hơn CBC. Ngoài những thành phần logic như CBC, CFB cần thêm logic để chọn số bit cần được xử lý nếu **s** là thông số cấu hình được.
- Lỗi bit bị lan truyền. Nếu một lỗi bit xuất hiện trên ciphertext của một khối dữ liệu thì nó sẽ làm sai kết quả giải mã của khối dữ liệu 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

OFB là chế độ mã hóa mà giá trị ngõ ra của khối thực thi thuật toán mã hóa, **không phải ciphertext**, của lần mã hóa hiện tại sẽ được phản hồi (feedback) đến ngõ vào của lần mã hóa kế tiếp.


J1
J2
Jn
64
K
DES
C1
C2
Cn
P1
P2
Pn


ENCRYPT
DECRYPT
INITIALIZATION VECTOR
INPUT BLOCK 1
INPUT BLOCK 2
INPUT BLOCK n
CIPHK
OUTPUT BLOCK 1
OUTPUT BLOCK 2
OUTPUT BLOCK n
PLAINTEXT 1
PLAINTEXT 2
PLAINTEXT n
CIPHERTEXT 1
CIPHERTEXT 2
CIPHERTEXT n
INITIALIZATION VECTOR
INPUT BLOCK 1
INPUT BLOCK 2
INPUT BLOCK n
CIPHK
OUTPUT BLOCK 1
OUTPUT BLOCK 2
OUTPUT BLOCK
CIPHERTEXT 1
CIPHERTEXT 2
CIPHERTEXT n
PLAINTEXT 1
PLAINTEXT 2
PLAINTEXT n

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 khối ngõ ra của lần mã hóa trước đó.
Lỗi bit không bị lan truyền. Khi một lỗi bit xuất hiện trên một ciphertext, nó chỉ ảnh hưởng đến kết quả giải mã của khối dữ liệu hiện tại
Thiết kế phần cứng đơn giản hơn CFB.
Nhược điểm:
Không thể thực hiện mã hóa/giải mã song song nhiều khối dữ liệu vì lần mã hóa/giải mã sau phụ thuộc vào khối ngõ ra của lần mã hóa/giải mã liền trước nó.
CTR là chế độ mã hóa sử dụng một tập các khối ngõ vào, gọi là các counter, để sinh ra một tập các giá trị ngõ ra thông qua một thuật toán mã hóa. Sau đó, giá trị ngõ ra sẽ được XOR với plaintext để tạo ra ciphertext trong quá trình mã hóa, hoặc XOR với ciphertext để tạo ra plaintext trong quá trình giải mã.



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 count không lặp lại.

Câu 3: Nêu các hình thức tấn công trong quá trình truyền thông tin trên mạng máy tính, cho ví dụ với từng hình thức tấn công.

- *Thay đổi thông điệp*
- *Mạo danh*
- *Phát lại thông điệp*
- *Ngăn chăn thông tin*

Câu 4: Hãy trình bày các yêu cầu của một hệ thống truyền thông tin an toàn và bảo mật, cho biết vai trò của mật mã học trong việc bảo vệ thông tin trên mạng.

Gợi ý:

Tính bí mật (Confidentiality): bảo vệ dữ liệu không bị lộ ra ngoài một cách trái phép.

Tính toàn vẹn (Integrity): Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.

Tính sẵn sàng (Availability): Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu

Tính chống thoái thác (Non-repudiation): Khả năng ngăn chặn việc từ chối một hành vi đã làm

Vai trò: Mật mã hay mã hóa dữ liệu (cryptography), là một công cụ cơ bản thiết yếu của bảo mật thông tin. Mật mã đáp ứng được các dịch vụ như xác thực, bảo mật, toàn vẹn dữ liệu, chống chối bỏ

Câu 5: Định nghĩa, định lý và tính chất của hàm Euler.

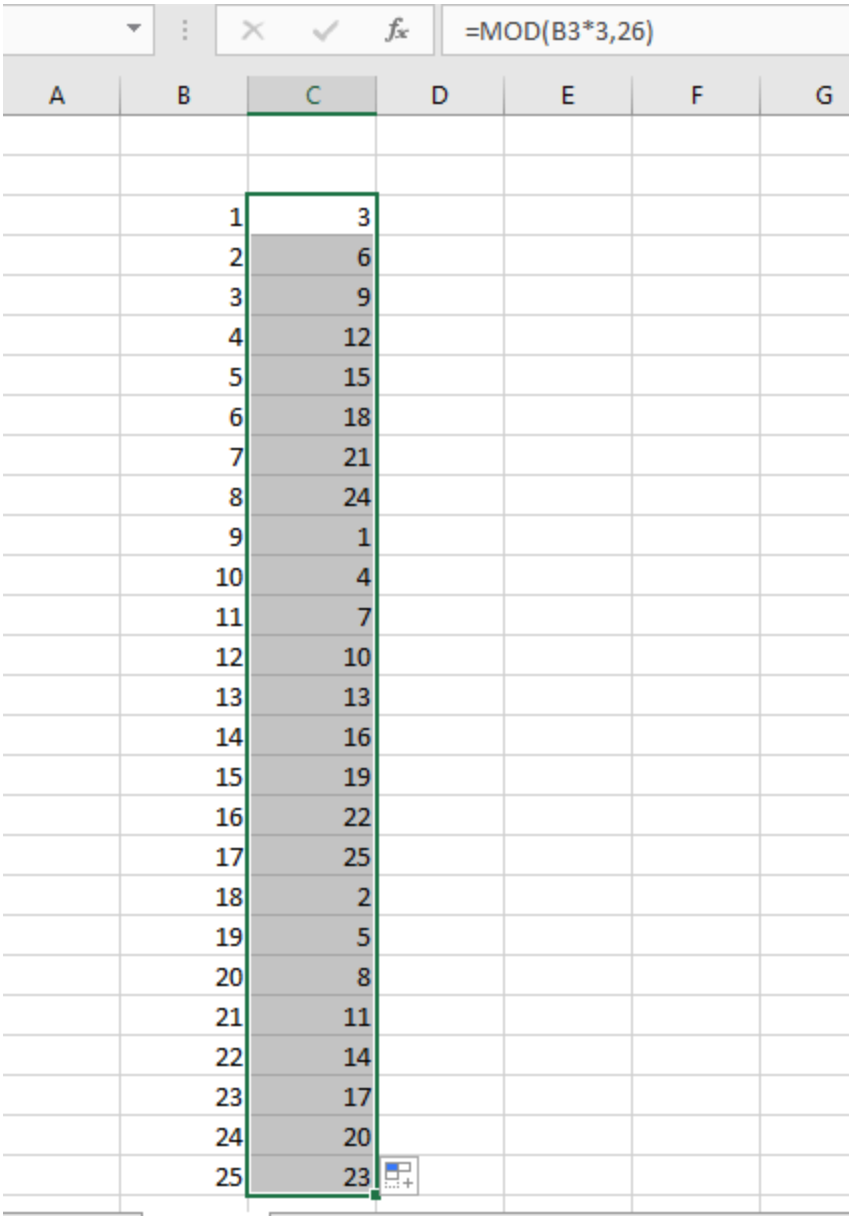
- Hàm phi euler
- Nếu n=pn=p là số nguyên tố, dễ thấy φ(p)=p−1φ(p)=p−1.
- Nếu n=pkn=pk thì φ(pk)=pk−pk−1
- Nếu n=p1p2n=p1p2 (với p1≠p2p1≠p2) thì φ(p1p2)=φ(p1)×φ(p2)

https://www.youtube.com/watch?v=re-zp5ObjXE

Câu 6: Học thuộc tập Z_{26}, N là gì?*

- Tìm phần tử nghịch đảo của 1 số trong tập 26

Mod(1->25*socantim,26) = 1



Video tham khảo

https://www.youtube.com/watch?v=D47Rya_CAgk

Câu 7: Tìm tổng khả nghịch của 1 số có công thức

$$a \times b \equiv 1 \pmod{n}$$

Câu 8: Định lý fermat và tính bài toán:

Dạng 1: Nếu P là số nguyên tố và a>0 không chia hết cho P thì a^{p-1} mod P dư 1

Dạng 2: nếu P là số nguyên tố và a>0 thì a^{p} mod P dư a

Và triển khai nhớ áp dụng các

First Property:	$(a + b) \bmod n = [(a \bmod n) + (b \bmod n)] \bmod n$
Second Property:	$(a - b) \bmod n = [(a \bmod n) - (b \bmod n)] \bmod n$
Third Property:	$(a \times b) \bmod n = [(a \bmod n) \times (b \bmod n)] \bmod n$

*Câu 9: Trao đổi khóa **Diffie Hellman***

-Yêu cầu:

Là sơ đồ trao đổi khoá mật dùng khoá công khai:

- Không thể dùng để trao đổi mẩu tin bất kỳ.
- Tuy nhiên nó có thể thiết lập khoá chung.
- Chỉ có hai đối tác biết đến.
- Giá trị khoá phụ thuộc vào các đối tác (và các thông tin về khoá công khai và khoá riêng của họ).
- Dựa trên phép toán lũy thừa trong trường hữu hạn (modulo theo số nguyên tố hoặc đa thức) là bài toán dễ.
- Độ an toàn dựa trên độ khó của bài toán tính logarit rời rạc (giống bài toán phân tích ra thừa số) là bài toán khó.

5.4.2 Khởi tạo Diffie Hellman

- Mọi người dùng thỏa thuận dùng tham số chung:

- Số nguyên tố rất lớn q hoặc đa thức.
- α là căn nguyên tố của mod q.

- Mỗi người dùng (A chẳng hạn) tạo khoá của mình:

Chọn một khoá mật (số) của A: $x_A < q$ Tính khoá công khai của A: $y_A = \alpha^{xA} \mod q$. Mỗi người dùng thông báo công khai khoá của mình y_A **5.4.3 Trao đổi khoá Diffie Hellman**

- Khoá phiên dùng chung cho hai người sử dụng A, B là K_{AB}

$KAB = \alpha^{xA.xB} \mod q$

$= yA^{xB} \mod q$ (mà **B** có thể tính)

$= yB^{xA} \mod q$ (mà **A** có thể tính)

- K_{AB} được sử dụng như khoá phiên trong sơ đồ khoá riêng giữa A và B
- A và B lần lượt trao đổi với nhau, họ có khoá chung K_{AB} cho đến khi họ chọn khoá mới.

Kẻ thám mã cần x, do đó phải giải tính logarit rời rạc

Ví dụ:

Câu 3: Trình bày chi tiết các bước trao đổi khóa Diffie Hellman. Cho q = 17, α = 10, x_A = 7, x_B = 5. Tính y_A ; y_B và khoá chung K_{AB}.

Y_a = 10^7 mod 17 = 5 = α^{xA} mod q

Y_b = 10^5 mod 17 = 6 = α^{xB} mod q

((7^10 mod 71)*(7^2 mod 71)) mod 71🐟

Tính khóa chung của A: 6^7 mod 17 =14 = Ya^{xA} mod q

B: 5^5 mod 17 = 14 = Yb^{xb} mod q

Câu 10: Nêu nhược điểm của mã hóa khóa công khai?

Nhược điểm của mã hóa đối xứng:

- Các hệ thống khóa công khai có thể rất chậm do số lượng lớn dữ liệu được mã hóa 1 cách thường xuyên
- Mã hóa công khai chỉ bảo vệ được một phần của một hệ thống tổng thể
- Vấn đề trao đổi khóa giữa người gửi và người nhận: Phải truyền khóa trên kênh an toàn để giữ bí mật. Ngay nay điều này tỏ ra không hợp lý vì khối lượng thông tin luân chuyển trên khắp thế giới là rất lớn.
- Tính bí mật của khóa (Tính không từ chối): Vì khóa 2 người dùng chung nên khi khóa bị lộ không có cơ sở quy trách nhiệm cho ai.

Câu 11: Trình bày quá trình tạo khóa và mã hóa của RSA?

Cụ thể, khóa của RSA được tạo ra như sau:

- Chọn 2 số nguyên tố p và q
- Tính n = pq. Sau này, n sẽ được dùng làm modulus trong cả public key và private key.
- Tính một số giả nguyên tố bằng phi hàm Carmichael như sau: λ(n) = BCNN(λ(p), λ(q)) = BCNN(p − 1, q − 1). Giá trị này sẽ được giữ bí mật.
- Chọn một số tự nhiên e trong khoảng (1, λ(n)) sao cho ƯCLN(e, λ(n)) = 1, tức là e và λ(n) nguyên tố cùng nhau.
- Tính toán số d sao cho d ≡ 1/e (mod λ(n)) hay viết dễ hiểu hơn thì de ≡ 1 (mod λ(n)). Số d được gọi là số nghịch đảo modulo của e (theo modulo mod λ(n)).

Mã hóa

-Lấy khóa công khai (n,e) theo thuật toán trên

-Cho một bản rõ x trong khoảng [1,n-1]

-Tính:y=x^e mod n

-Nhận được bản mã y

Câu 12: Trình bày các giải pháp trao đổi khóa công khai? Cho biết hoàn cảnh áp dụng từng giải pháp?

Giao thức From Alice to Bob

1. Alice tạo ra khóa K ngẫu nhiên; mã hóa {K}KAT; và gửi cho Trent: Alice, Bob, {K}KAT

2. Trent tìm khóa KAT, KBT; giải mã {K}KAT để lấy K rồi mã hóa lại {K}KBT; và gửi cho Bob: Alice, Bob, {K}KBT

3. Bob giải mã {K}KBT để lấy K; và bắt đầu nói chuyện với Alice: {Hello Alice, I'm Bob!}K

Giao thức Session Key from Trent"

1. Alice gửi cho Trent: Alice, Bob

2. Trent tìm khóa KAT, KBT; tạo khóa K ngẫu nhiên; và gửi cho Alice: {K}KAT , {K}KBT

3. Alice giải mã {K}KAT; và gửi cho Bob: Trent, Alice, {K}KBT

4. Bob giải mã {K}KBT được K; và bắt đầu nói chuyện với Alice: {Hello Alice, I'm Bob!}K

Giao thức Message Authentication"

1. Alice gửi cho Trent: Alice, Bob

2. Trent tìm khóa KAT, KBT; tạo khóa K ngẫu nhiên; và gửi cho Alice: {Bob, K}KAT , {Alice, K}KBT

3. Alice giải mã {Bob, K}KAT và kiểm tra danh định của Bob; rồi gửi cho Bob: Trent, {Alice, K}KBT

4. Bob giải mã {Alice, K}KBT và kiểm tra danh định của Alice; bắt đầu nói chuyện với Alice: {Hello Alice, I'm Bob!}K

Or

Trao đổi khóa Diffie-Hellman là một trong những phát triển quan trọng nhất trong mật mã khóa công khai và nó vẫn được thực hiện thường xuyên trong một loạt các giao thức bảo mật khác nhau ngày nay.

Nó cho phép hai bên trước đây chưa gặp nhau thiết lập một cách an toàn một khóa mà họ có thể sử dụng để bảo mật thông tin liên lạc của họ.

Mục đích chính của trao đổi khóa Diffie-Hellman là để phát triển an toàn các bí mật được chia sẻ có thể được sử dụng để lấy khóa. Các khóa này sau đó có thể được sử dụng với các thuật toán khóa đối xứng để truyền thông tin theo cách được bảo vệ. Các thuật toán đối xứng có xu hướng được sử dụng để mã hóa phần lớn dữ liệu vì chúng hiệu quả hơn các thuật toán khóa công khai.

Là một trong những phương pháp phổ biến nhất để phân phối khóa an toàn, trao đổi khóa Diffie-Hellman là thường xuyên được thực hiện trong các giao thức bảo mật như TLS, IPsec, SSH, PGP và nhiều giao thức khác.

Câu 13: Giải thích tính an toàn của giải pháp trao đổi khóa bí mật sử dụng hệ mã hóa công khai?

Hệ mã công khai sử dụng hai khóa có quan hệ toán học với nhau, tức là một khóa này được hình thành từ khóa kia: Người muốn nhận bản mã (Alice) tạo ra một khóa mật (private key) và từ khóa mật tính ra khóa công khai (public key) với một thủ tục không phức tạp, còn việc tìm khóa mật khi biết khóa công khai là bài toán khó giải được. Khóa công khai sẽ đưa đến cho người gởi bản tin (Bob) qua kênh công cộng. Và bản tin được Bob mã hóa bằng khóa công cộng. Bản mã truyền đến Alice, và nó được giải mã bằng khóa mật.

Câu 14: Các phương pháp Ceasar, mã hóa đơn bảng, đa bảng, one-time pad dùng nguyên tắc gì để mã hóa?

Trả lời:

-Phương pháp Ceaser:Dùng nguyên tắc mã hóa đối xứng

-Mã hóa đơn bảng:Sử dụng nguyên tắc thay thế

-Đa bảng:

-One-time pad:Nguyên tắc mật mã cổ điển

Câu 15: Phương pháp hoán vị dùng nguyên tắc gì để mã hóa?

Về bản chất thì kỹ thuật hoán vị chỗ chính là trường hợp đặc biệt của kỹ thuật thay thế. Trong kỹ thuật này, tập hợp các ký tự của bản nguồn sẽ không thay đổi so với bản mã mà chỉ thay đổi vị trí của các ký tự.

Câu 16: Tại sao phương pháp mã hóa đơn bảng có thể bị tấn công phá mã dùng thống kê tần suất?

Câu 17: Định lý RSA, cách phát sinh khóa RSA, mã hóa và giải mã trong RSA?

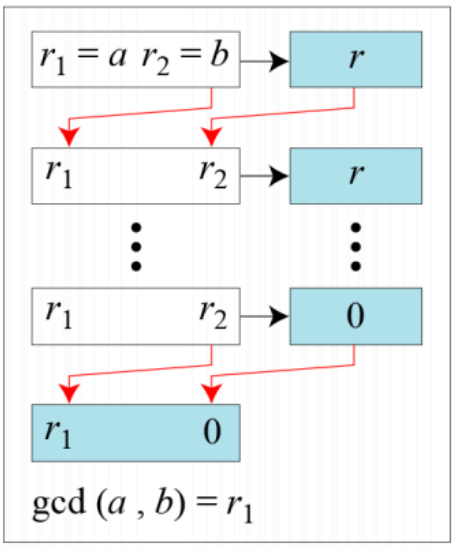
Trả lời:

Định lí: RSA là một trong những hệ thống mã hoá bất đối xứng được sử dụng rộng rãi, Ý tưởng then chốt để đảm bảo tính an toàn của RSA là dựa trên sự khó khăn trong việc phân tích nhân tử của 2 số nguyên tố lớn

Giải mã

Sử dụng khóa bí mật d để giải mã:x=yˆd mod n

Câu 18: Sử dụng thuật toán Euclidean để tìm tổng khả nghịch:



a. Process

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$ (Initialization)

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$

}

gcd (a, b) $\leftarrow r_1$

b. Algorithm

Ví dụ:

Find the greatest common divisor of 2740 and 1760?

Find the greatest common divisor of 25 and 60?

Câu 19: thuật toán euclidean mở rộng (Extended Euclidean Algorithm)

$r_1 \leftarrow a;$ $r_2 \leftarrow b;$

$s_1 \leftarrow 1;$ $s_2 \leftarrow 0;$ (Initialization)

$t_1 \leftarrow 0;$ $t_2 \leftarrow 1;$

while ($r_2 > 0$)

{

$q \leftarrow r_1 / r_2;$

$r \leftarrow r_1 - q \times r_2;$

$r_1 \leftarrow r_2;$ $r_2 \leftarrow r;$ (Updating r's)

$s \leftarrow s_1 - q \times s_2;$

$s_1 \leftarrow s_2;$ $s_2 \leftarrow s;$ (Updating s's)

$t \leftarrow t_1 - q \times t_2;$

$t_1 \leftarrow t_2;$ $t_2 \leftarrow$ t; (Updating t's)

}

gcd (a , b) $\leftarrow r_1;$ $s \leftarrow s_1;$ $t \leftarrow t_1$

Ví dụ:

Given a = 161 and b = 28, find gcd (a, b) and the values of s and t

Câu 20: Hàm Euler-Phi:

(φ (1)=0,

φ (p) = p-1: nếu p là số nguyên tố, (DL1)

φ (a*b) = φ a * φ b (a và b là 2 số nguyên tố cùng nhau, (DL2)

φ (P^a) = P^a – P^a-1 nếu P là số nguyên tố và a là số nguyên dương) (DDL3)

Câu 21: **Định lý Euler:**

Dạng 1: nếu a và n là số nguyên tố cùng nhau thì a ^ φ (n) == 1 (mod n)

Dạng 2: Nếu a và n là 2 số nguyên thì a^(φ (n)+1) ==a (mod n)

Câu 22: Định lý nhỏ Fermat:

Nếu P là số nguyên tố, a số bất kỳ >0 và không chia hết cho P thì có a^p-1 mod p = 1.

Nếu P là số nguyên tố, a>0 thì a^P mod P = a.

Câu 23: Mã hóa **Ceasar: Ý tưởng lấy từng ký tự của bảng rõ + với khóa K để ra bản mã**

mã hóa: **C** = (**p** + **k**) **mod** 26

Giải mã: **p** = (**C** – **k**) **mod** 26

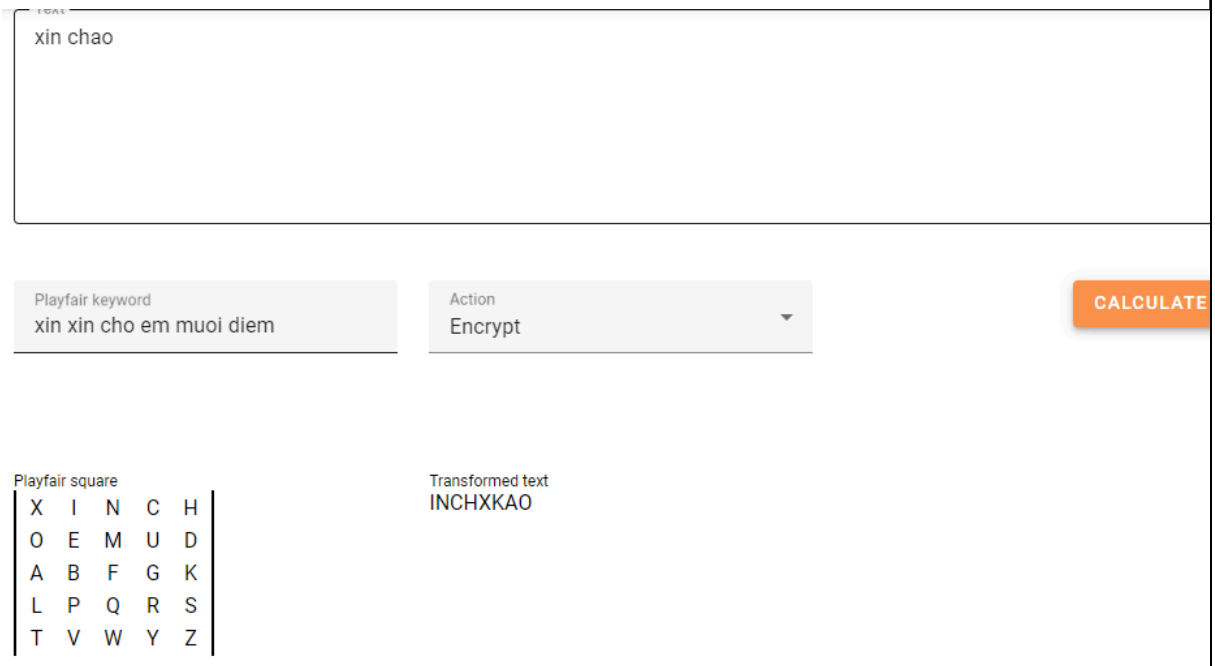
Ví dụ: meet me after the toga party

K=3

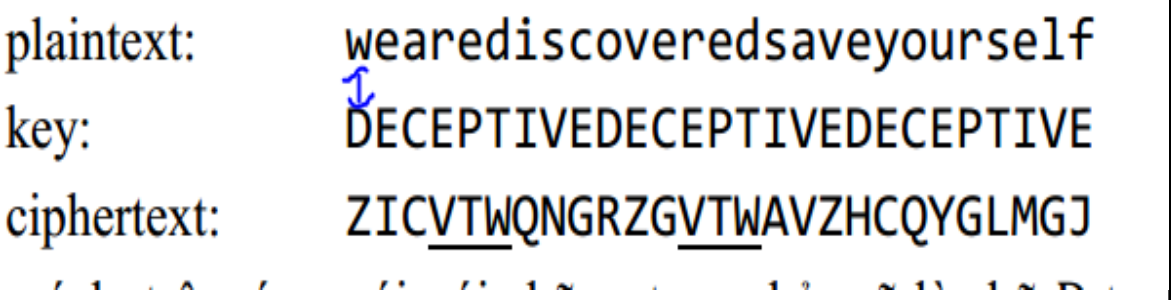
Z26 = A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Bảng mã: PHHW PH DIWHU WKH WRJD SDUWB

Câu 24: Mã Playfair: Mã hóa Playfair xem hai ký tự đứng sát nhau là một đơn vị mã hóa, hai ký tự này được thay thế cùng lúc bằng hai ký tự khác. Playfair dùng một ma trận 5x5 các ký tự keyword như sau: (chỉ lấy những ký tự không trùng nhau trong khóa, khi mã hóa lấy từng cặp của bảng rõ đi so sánh trong bảng 5x5 theo nguyên tắc: 2 ký tự cùng hàng thì sẽ lấy 2 ký tự kế tiếp, nếu cùng cột thì 2 ký tự kế tiếp trong cột, nếu là đường chéo thì lấy đường chéo lại)



Câu 25: Mã hóa **Vigenere: Tạo ra bảng 26x26 chữ cái. Cho bảng rõ và khóa (khóa sẽ được lặp lại cho đến khi bằng chiều dài bảng rõ). Sau đó lấy ký tự bảng rõ (Cột) so với khóa (dòng) để tìm ký tự giao nhau:**



Câu 26: Mã Rail Fence: Ý tưởng ghi các ký tự theo từng hàng trong bảng có số cột bằng khóa. Ghi từ trên xuống

Ví dụ:

CHAOCACBANHOCMONANTOANBAOMATTHONGTIN

1	2	3	4	5	6
C	H	A	O	C	A
C	B	A	N	H	O
C	M	O	N	A	N
T	O	A	N	B	A
O	M	A	T	T	H
O	N	G	T	I	N

Bảng mã C = CCCTOO HBMOMN …..

Câu 27: Thuật toán RSA

Câu 28: Thuật toán DES

Câu 29: Thuật toán AES

Bài tập:

Câu 1: gián các số cho các ký tự (in hoa) (A = 0, B = 1, …, Z = 25), tìm và giải thích:

- ✔ (A + N) mod 26 = (0+13) mod 26 = 13 => N
- ✔ (A + 6) mod 26
- ✔ (Y − 5) mod 26
- ✔ (C − 10) mod 26 =
- ✔ ((K − 2) mod 26 + (T − 10) mod 26) mod 26
- ✔ ((G − 10) mod 26 + (X − 17) mod 26 + (L − 15) mod 26)mod 26

Câu 2: Liệt kê các cặp số theo tổng khả nghịch (multiplicative inverse) modulus 20, 40, 30…
modulus 20: (1,1),(3,7),(9,9), (11,11),(13,17),(19,19)
Các giải: euclidean, Dùng excel mod(1-25*1-25,26)=1
Câu 3: Sử dụng hàm Euler-Phi, tìm:

- ✔ φ(29) = 28 (29 is prime)
- ✔ φ(100) (định lý 2) = φ(4*25) = φ(2^2*5^2) = φ(2^2)* φ (5^2) = 2^2-2^1 * 5^2-5^1 = 2*20=40
- ✔ φ(6) = φ(2*3)

Câu 4: Sử dụng định lý nhỏ Fermat, tìm:

✔ $(5^{15} \bmod 13) = (5^{13+2} \bmod 13) = ((5^{13} \bmod 13)* (5^2 \bmod 13))\bmod 13 = (5*12)\bmod 13$

$=8$

$20^{35} \bmod 161 =$

✔ $(15^{18} \bmod 17)$

✔ $(7^{51} \bmod 18)$

✔ $(15^{59} \bmod 23)$

$159^{137} \bmod 31 = 16$

Câu 5: Alice chọn **p=11 & q=3**, e = 3 hãy tính khóa K_{RU} và K_{RA}, Đồng thời mã hóa và giải mã với M =15 (theo mật mã bảo mật và mật mã chứng thực).

Tính N = q*P = 11*3 = 33

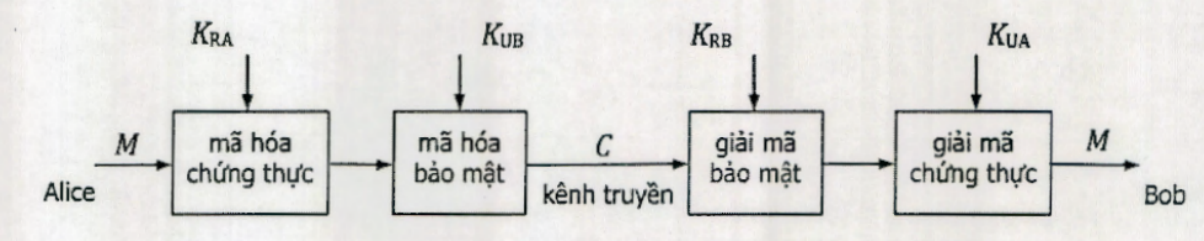
B2: φ(n)=(p-1)*(q-1) = 20

B3: ng ta cho biết e rồi = 3

B4: d : d.e mod φ(n) dư 1 => d.3 mode 20 dư 1 -> d =7

B5: khóa công khai Ku=(e,N) = (3,33), khóa riêng bí mật Kr = (d,p,e) = (7,11,3)

Ý 2: B1: mã hóa chứng thực



C’ = E(M,Kra(alice)) = M^{da} mod N = 15^7 mod 33 = 27

B2: mã hóa bảo mật

$$C = E(C',Kua(alice)) = C'^{ea} \mod N = 27^3 \mod 33 = 15$$

B3: giải mã bảo mật

$$M' = D(C,Kra(alice)) = C^d \mod N = 15^7 \mod 33 = 27$$

B4: giải mã chứng thực

$$M'' = D(M',Kua(alice)) = M'^e \mod N = 27^3 \mod 33 = 15$$

- M và M'' bằng nhau nên mã hóa và giải mã thành công.

Câu 6: Alice chọn **p=15 & q=8**, e = 6 hãy tính khóa K_{RU} và K_{RA}, Đồng thời mã hóa và giải mã với M =15 (theo mật mã bảo mật và mật mã chứng thực).

Câu 7: Cho p = 5, q= 11, e = 7. Tính khóa riêng (d, N) trong phương pháp RSA.

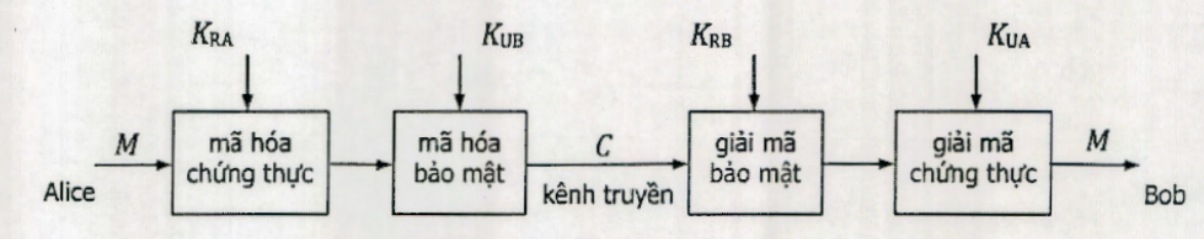
Câu 8: Cho p = 11, q= 13, e = 11. Tính khóa riêng (d, N) trong phương pháp RSA.

Câu 9: Thực hiện mã hóa và giải mã bằng phương pháp RSA với p = 3, q = 11, e = 7, M = 5 theo hai trường hợp mã hóa bảo mật và mã hóa chứng thực.

Câu 10: Alice chọn p = 7, q = 11, e = 17, Bob chọn p = 11, q = 13, e = 11:

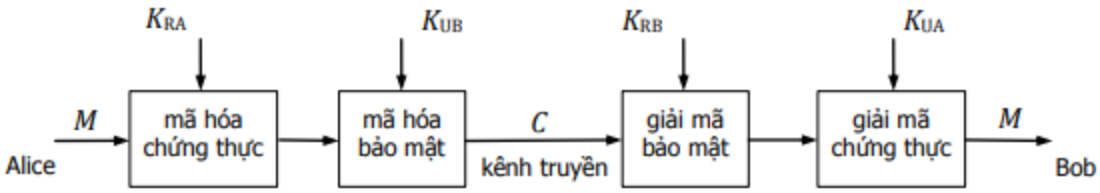
a. Tính khóa riêng KRA của Alice và KRB của Bob

b. Alice muốn gởi cho Bob bản tin M = 9 vừa áp dụng chứng thực và bảo mật như ở sơ đồ dưới. Hãy thực hiện quá trình mã hóa và giải m.



$$C = E(E(M, K_{RA}), K_{UB})$$

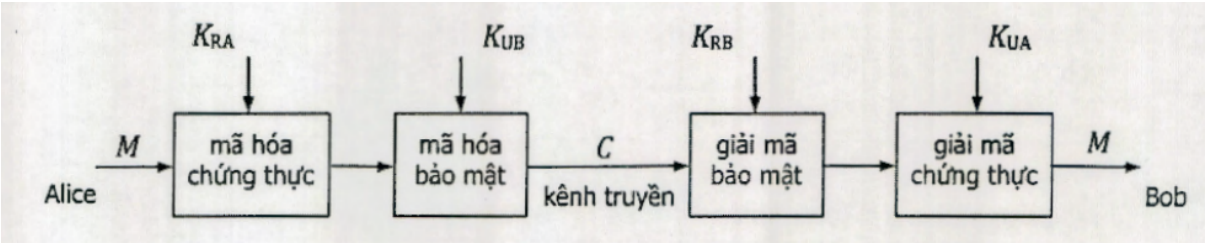
$$M = D(D(C, K_{RB}), K_{UA})$$



Câu 11: Alice chọn p = 7, q = 11, e = 17, Bob chọn p = 11, q = 3, e = 3:

a. Tính khóa riêng KRA của Alice và KRB của Bob

b. Alice muốn gửi cho Bob bản tin M = 9 vừa áp dụng chứng thực và bảo mật như ở sơ đồ dưới. Hãy thực hiện quá trình



mã hóa và giải m.

Câu 12: cho q = 71, anpha = 7, $X_A = 5$, $X_B = 12$ hãy tính Y_A, Y_B và khóa chung K_{AB}.

Câu 13: cho q = 11, anpha = 2, $X_A = 9$, $X_B = 3$ hãy tính Y_A, Y_B và khóa chung K_{AB}.

Câu 14: cho q = 17, anpha = 10, $X_A = 7$, $X_B = 5$ hãy tính Y_A, Y_B và khóa chung K_{AB}.