**C1: 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**.

**1. Kerberos:**

- Giao thức xác thực và ủy quyền trong mạng máy tính.

- Sử dụng mã hóa và chứng thực giữa các bên để ngăn chặn tấn công giả mạo và đánh cắp thông tin.

- Cung cấp phiên làm việc an toàn trên mạng.

**2. X.509:**

- Chuẩn xác thực và phân phối chứng chỉ số công khai (public key).

- Sử dụng hệ thống chứng thực tập trung, nơi mà một tổ chức tin cậy phát hành và quản lý các chứng chỉ số công khai.

- Đảm bảo tính toàn vẹn, xác thực và bảo mật trong quá trình trao đổi thông tin.

**3. SSL (Secure Sockets Layer) / TLS (Transport Layer Security):**

- Giao thức bảo mật lớp giao vận trên Internet.

- Sử dụng mã hóa để đảm bảo bí mật và xác thực trong quá trình truyền dữ liệu giữa máy khách và máy chủ.

- Bảo vệ khỏi các cuộc tấn công như đánh cắp thông tin và sửa đổi dữ liệu.

**4. PGP (Pretty Good Privacy) và S/MIME (Secure/Multipurpose Internet Mail Extensions):**

- Cung cấp chữ ký số và mã hóa cho việc bảo mật email.

- PGP sử dụng cặp khóa công khai và khóa bí mật để mã hóa và giải mã dữ liệu.

- S/MIME cung cấp chứng thực và mã hóa dựa trên chứng chỉ số công khai.

**5. IPSET:**

- Công cụ quản lý tập hợp các quy tắc tường lửa trong hệ thống Linux.

- Cho phép quản lý danh sách đen (blacklist) và danh sách trắng (whitelist) để kiểm soát quyền truy cập từ các địa chỉ IP hoặc mạng cụ thể.

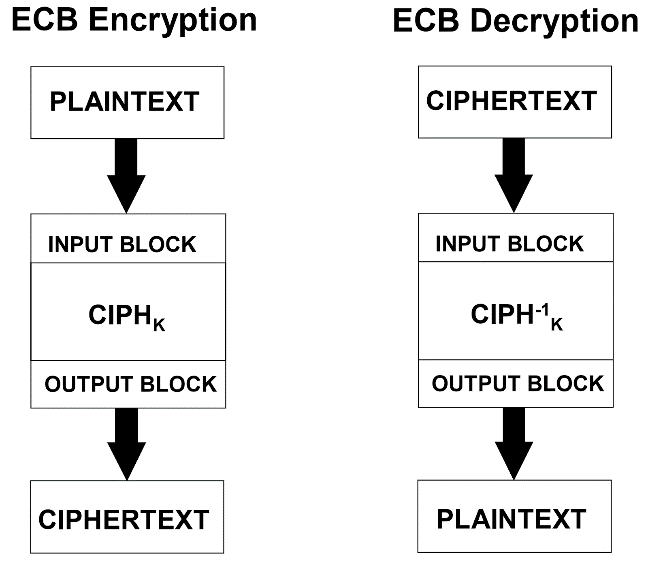
- Ngăn chặn các cuộc tấn công từ các địa chỉ IP không an toàn.

Các thức bảo vệ: khái niệm Control Access (kiếm 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.**

**1. ECB (Electronic Codebook):**

- Mô hình ECB: **Các khối dữ liệu được mã hóa độc lập và riêng biệt.**



- Ưu điểm:

- Đơn giản và dễ triển khai.

- Không cần đồng bộ hóa giữa bên gửi và nhận.

- Cho phép mã hóa và giải mã đồng thời nhiều khối dữ liệu.

- Nhược điểm:

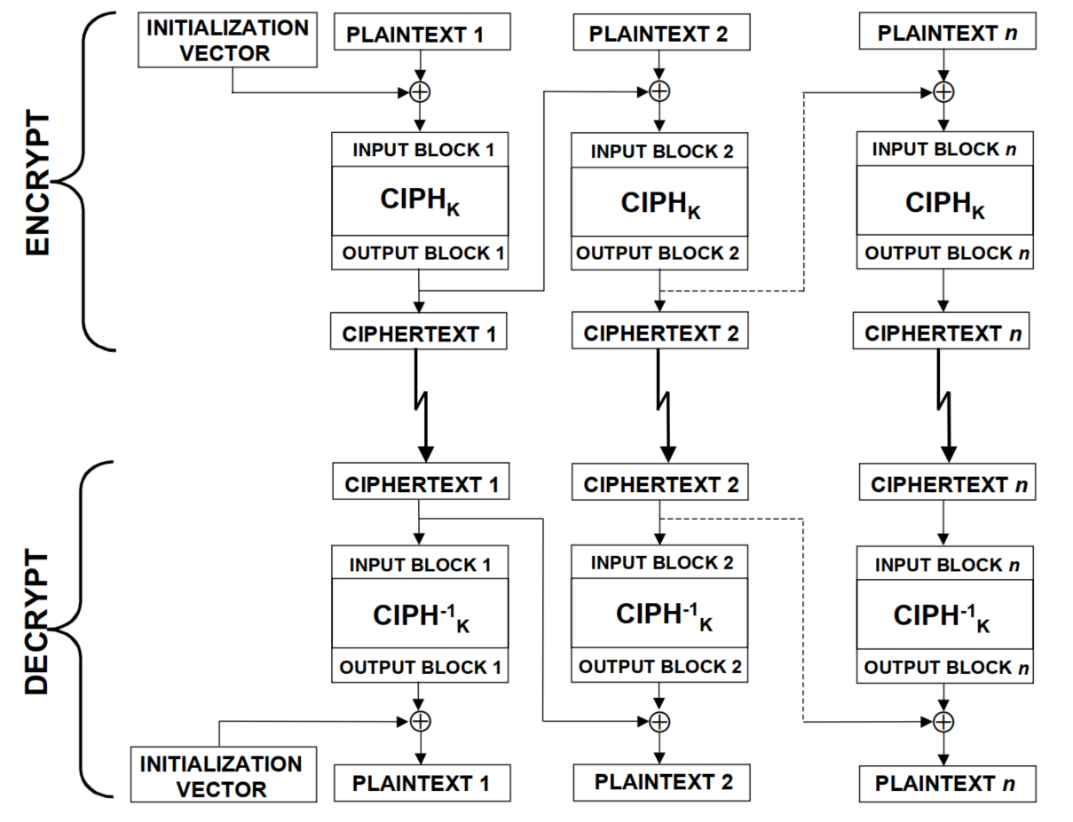
- Mỗi khối dữ liệu được mã hóa thành một khối mã riêng biệt, dẫn đến sự **tương tự** giữa các khối dữ liệu tương ứng.

- **Dễ bị tấn công** thông qua phân tích **tần suất và cấu trúc khối mã.**

- **Không** đảm bảo tính **bảo mật cao** khi mã hóa các bản rõ lớn và có tính cấu trúc rõ ràng.

**2. CBC (Cipher Block Chaining):**

- Mô hình CBC: Các khối dữ liệu được mã hóa **theo chuỗi** và phụ thuộc vào các **khối mã trước đó.**



**- Ưu điểm:**

- Đảm bảo **tính toàn vẹn của dữ liệu** và ngăn **chặn tấn công** thay đổi dữ liệu.

- Tăng cường tính bất định trong việc mã hóa các khối dữ liệu giống nhau.

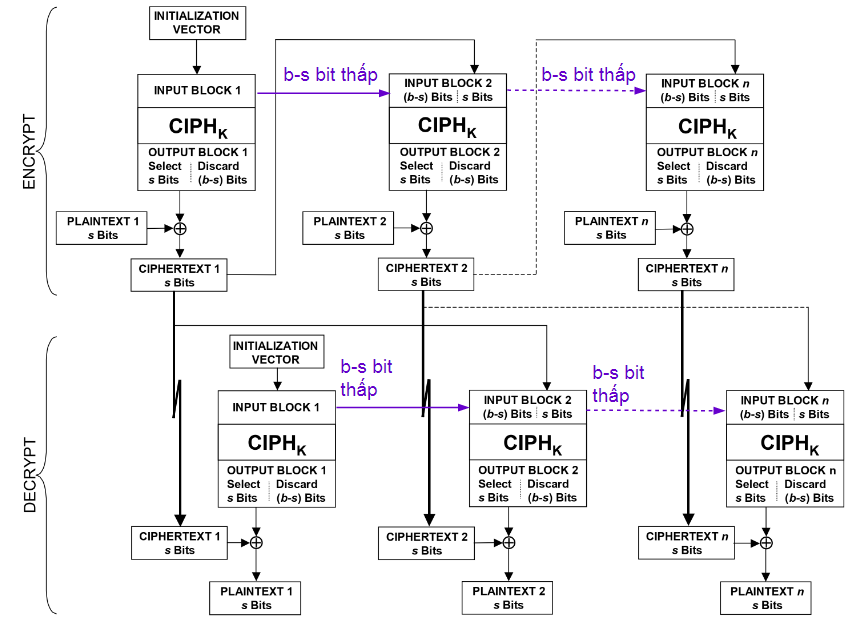
**- Nhược điểm:**

- Đòi hỏi việc đồng bộ hóa đúng giữa bên gửi và nhận.

- Không thể mã hóa và giải mã đồng thời nhiều khối dữ liệu.

**3. CFB (Cipher Feedback):**

- Mô hình CFB: Sử dụng khối mã hóa trước đó để tạo ra một chuỗi dữ liệu ngẫu nhiên để kết hợp với bản rõ.



- Ưu điểm:

- Cho phép mã hóa các khối dữ liệu nhỏ hơn kích thước khối mã.

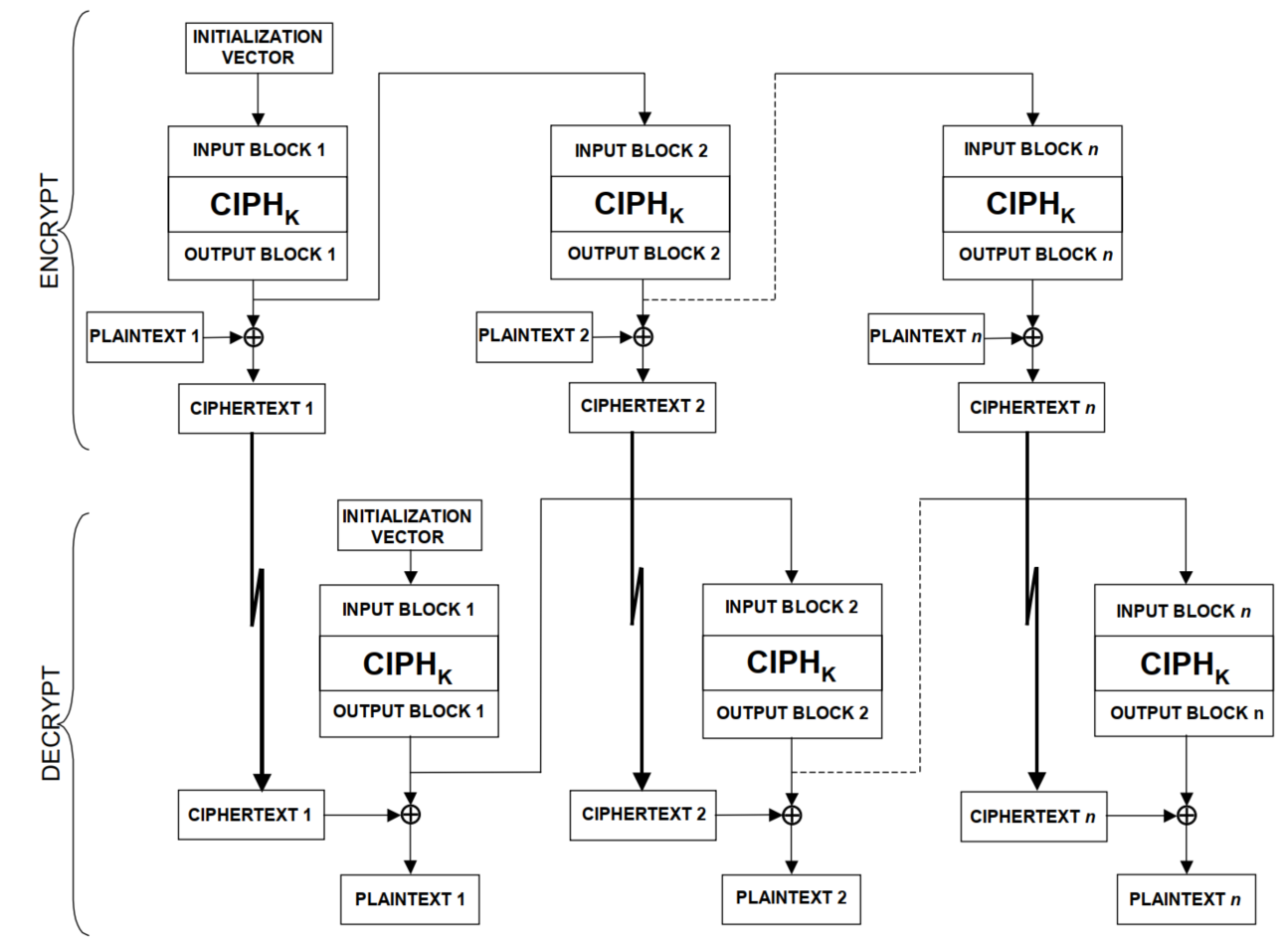
- Không yêu cầu đồng bộ hóa đúng giữa bên gửi và nhận.

- Nhược điểm:

- Hiệu suất mã hóa và giải mã thấp hơn so với ECB và CBC.

**4. OFB (Output Feedback):**

- Mô hình OFB: Sử dụng khối mã hóa trước đó để tạo ra một chuỗi dữ liệu ngẫu nhiên, không phụ thuộc vào bản rõ.



- Ưu điểm:

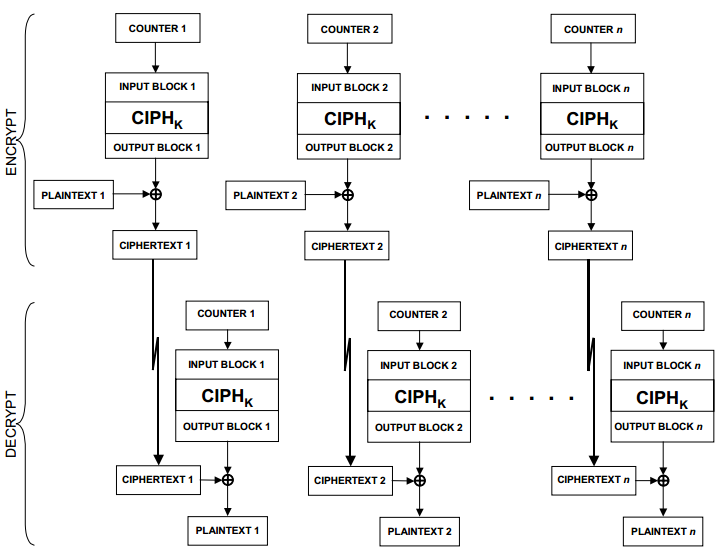
- Không yêu cầu đồng bộ hóa đúng giữa bên gửi và nhận.

- Cho phép mã hóa các khối dữ liệu nhỏ hơn kích thước khối mã.

- Nhược điểm:

- **Không đảm bảo tính toàn vẹn của dữ liệu, nghĩa là một lỗi truyền thông có thể lan truyền và ảnh hưởng đến các khối sau đó.**

**5. CTR (Counter):**



- Mô hình CTR: Sử dụng một bộ đếm để tạo ra chuỗi dữ liệu ngẫu nhiên để kết hợp với bản rõ.

- Ưu điểm:

**- Cho phép mã hóa và giải mã đồng thời nhiều khối dữ liệu.**

**- Hiệu suất mã hóa và giải mã cao.**

- Nhược điểm:

- Không đảm bảo tính toàn vẹn của dữ liệu, tương tự như OFB.

**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.**

**1. Thay đổi thông điệp (Message Modification):**

- Mục tiêu của tấn công là thay đổi hoặc sửa đổi nội dung của thông điệp được truyền đi.

- Ví dụ: Một kẻ tấn công có thể chèn thêm hoặc thay đổi nội dung trong một email, làm thay đổi ý nghĩa ban đầu của thông điệp.

**2. Mạo danh (Spoofing):**

- Tấn công này nhằm làm giả mạo địa chỉ IP, địa chỉ email, hoặc thông tin nhận dạng của người gửi hoặc nhận.

- Ví dụ: Kẻ tấn công có thể sử dụng kỹ thuật IP spoofing để thay đổi địa chỉ IP nguồn của một gói tin, để che đậy danh tính và gây hiểu lầm cho người nhận.

**3. Phát lại thông điệp (Replay Attack):**

- Tấn công này liên quan đến việc ghi lại và phát lại lại các thông điệp đã được truyền trước đó.

- Ví dụ: Một kẻ tấn công ghi lại một gói tin chứa thông tin đăng nhập và sau đó gửi lại gói tin đó để giả mạo người dùng và xâm nhập vào hệ thống.

**4. Ngăn chặn thông tin (Denial of Service - DoS):**

- Tấn công này nhằm làm cho dịch vụ hoặc hệ thống trở nên không khả dụng cho người dùng hợp lệ.

- Ví dụ: Kẻ tấn công sử dụng tấn công DDoS (Distributed Denial of Service) để gửi lượng lớn yêu cầu không hợp lệ đến một dịch vụ hoặc máy chủ, gây quá tải và làm cho dịch vụ không thể hoạt động.

**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: Nêu nhược điểm của mã hóa khóa công khai?**

Mã hóa khóa công khai, còn được gọi là mã hóa bất đối xứng, là một phương pháp mã hóa trong đó có hai khóa: khóa công khai (public key) và khóa bí mật (private key). Trong mã hóa khóa công khai, khóa công khai được chia sẻ công khai cho tất cả mọi người, trong khi khóa bí mật chỉ được giữ bí mật bởi người sở hữu. Mã hóa khóa công khai có nhược điểm sau:

1. **Tốn tài nguyên tính toán**: Mã hóa và giải mã trong mã hóa khóa công khai yêu cầu tính toán phức tạp hơn so với mã hóa đối xứng (symmetric encryption). Quá trình mã hóa và giải mã có thể đòi hỏi nhiều tài nguyên tính toán, đặc biệt là khi làm việc với các khối dữ liệu lớn.

2. **Hiệu suất chậm hơn:** Do tính toán phức tạp hơn, mã hóa khóa công khai có hiệu suất chậm hơn so với mã hóa đối xứng. Việc mã hóa và giải mã dữ liệu lớn có thể trở nên rất chậm và làm giảm tốc độ truyền thông.

3. **Độ dài khóa lớn**: Để đảm bảo tính bảo mật, khóa công khai trong mã hóa khóa công khai thường có độ dài lớn hơn khóa bí mật. Việc quản lý và truyền khóa có độ dài lớn có thể tạo ra thách thức bảo mật và ảnh hưởng đến hiệu suất.

4. **Nguy cơ tấn công qua từ điển**: Một nhược điểm của mã hóa khóa công khai là khóa công khai có thể được công khai, điều này tạo ra nguy cơ tấn công qua từ điển (dictionary attack). Kẻ tấn công có thể thử tất cả các khóa công khai có thể có để tìm ra khóa bí mật tương ứng.

5. **Nguy cơ tấn công bằng cách phá vỡ toán học**: Mã hóa khóa công khai dựa trên các thuật toán toán học phức tạp. Nếu có một phương pháp hiệu quả để phá vỡ tính toán trong các thuật toán này, thì toàn bộ hệ thống mã hóa khóa công khai có thể bị đánh sập.

**Câu 6: Trình bày quá trình tạo khóa và mã hóa của RSA ?**

Quá trình tạo khóa và mã hóa trong RSA bao gồm các bước sau:

**1. Tạo khóa:**

a. Bước 1: Chọn hai số nguyên ngẫu nhiên lớn và nguyên tố p và q.

b. Bước 2: Tính tích n = p \* q, được gọi là modulus.

c. Bước 3: Tính hàm Euler của n: φ(n) = (p-1) \* (q-1), trong đó φ(n) là số nguyên tố tương đối cùng với n.

d. Bước 4: Chọn một số nguyên e, sao cho 1 < e < φ(n) và e là số nguyên tố tương đối cùng với φ(n). Số e sẽ được sử dụng làm khóa công khai.

e. Bước 5: Tính số nguyên d sao cho (d \* e) % φ(n) = 1. Số d sẽ được sử dụng làm khóa bí mật.

**2. Mã hóa:**

a. Bước 1: Chuyển đổi thông điệp cần mã hóa thành một số nguyên M, trong đó M < n.

b. Bước 2: Tính toán mã hóa bằng cách sử dụng khóa công khai (e): C = M^e mod n. Kết quả C là thông điệp đã được mã hóa.

Quá trình mã hóa của RSA sử dụng khóa công khai (e) để mã hóa thông điệp. Sau khi thông điệp được mã hóa, nó trở thành một số nguyên C.

**3. Giải mã:**

a. Bước 1: Nhận số nguyên C đã được mã hóa.

b. Bước 2: Tính toán giải mã bằng cách sử dụng khóa bí mật (d): M = C^d mod n. Kết quả M là thông điệp gốc đã được giải mã

Quá trình giải mã của RSA sử dụng khóa bí mật (d) để giải mã thông điệp đã mã hóa. Kết quả là thông điệp ban đầu M.

**Câu 7: Giải thích tính an toàn của giải pháp trao đổi khoá bí mật sử dụng hệ mã hoá công khai?**

- Giải pháp trao đổi khoá bí mật sử dụng hệ mã hoá công khai đặc biệt nhờ vào các tính chất sau:

1. **Khoá công khai và khoá bí mật độc lập**: Trong hệ mã hoá công khai, cặp khoá bao gồm khoá công khai và khoá bí mật là độc lập. Khoá công khai có thể được công khai cho mọi người trong khi khoá bí mật được giữ bí mật chỉ cho người sở hữu.
2. **Khoá công khai không tiết lộ khoá bí mật**: Dù khoá công khai bị lộ thì cũng không thể lộ ra khoá bí mật tương ứng.
3. **Tính không thể đoán trước của khoá bí mật:** Việc tính toán khóa bí mật từ khoá công khai là rất khó khăn.
4. **Bất khả xâm phạm của khoá bí mật:** Với giải pháp trao đổi khoá bí mật sử dụng hệ mã hoá công khai, người gửi không cần phải truyền khoá bi mật cho người nhận.
5. **An toàn trước tấn công brute-force:** Một ưu điểm quan trong của hệ mã hoá công khai là tính an toàn trước các cuộc tấn công brute-force.