**AN TOÀN THÔNG TIN**

**Phần I: Trắc nghiệm**

**Bài 1:**

**Câu 1:** Dịch vụ xác thực nguồn gốc thông điệp sử dụng những cơ chế ATTT:

- Bảo mật, ký số.

**Câu 2:** Chọn những ý cho thấy sự khác nhau giữa tấn công thụ động và tấn công chủ động vào hệ thống thông tin là:

- Tấn công chủ động thay đổi dữ liệu và hoạt động của hệ thống.

- Tấn công thủ động không làm thay đổi hoạt động và dữ liệu hệ thống.

**Câu 3:** Kiến trúc an toàn thông tin OSI tập trung vào các vấn đề:

- Tấn công, cơ chế an toàn thông tin, dịch vụ an toàn thông tin.

**Câu 4:** Những dạng tấn công là chủ động:

- Tấn công từ chối dịch vụ, giả mạo thông tin.

- Sửa đổi nội dung, chặn giữ thông điệp.

- Tấn công phát lại, tấn công mạo danh.

**Câu 5:** Phân loại các dạng tấn công thụ động:

- Phát lộ nội dung thông điệp.

- Phân tích lưu lượng luồng truyền tải.

**Câu 6:** Lựa chọn những chức năng ATTT trong mô hình an toàn thông tin hệ thống:

- Ngăn chặn tấn công, phát hiện tấn công, phát hiện lỗ hổng hệ thống.

**Câu 7:** Bên thứ ba được ủy quyền trong mô hình an toàn truyền tải dữ liệu có chức năng:

- Chia sẻ thông tin bí mật cho các bên.

- Xác nhận các bên tham gia trao đổi thông tin.

- Cấp phát chứng nhận các bên.

- Quản trị và trao đổi khóa bí mật.

**Câu 8:** Bộ tạo số ngẫu nhiên trong mô hình hệ mật khóa đối xứng có tác dụng:

- Tăng tính nhập nhằng trong mã hóa.

**Câu 9:** Tính mật thực tiễn phụ thuộc vào:

- Thời gian cần giữ bí mật thông điệp.

- Giá trị của nội dung thông điệp.

**Câu 10:** Cấu trúc hệ mật khóa đối xứng gồm những thành phần nào dưới đây:

- Khối mã hóa, khối giải mã.

- Nguồn tin.

- Nhận tin.

- Khối tạo sinh khóa.

- Khối tạo số ngẫu nhiên.

- Kênh mặt phân phối khóa.

**Câu 11:** Phương pháp DES có:

- Khóa ngắn hơn bản rõ.

**Câu 12:** Thuật toán mật mã cần đủ mạnh để chống lại dạng tấn công:

- Tấn công “bản rõ đã biết”.

**Câu 13:** Điều kiện cần để hệ mật hoàn hảo:

- Bản mật và bản rõ độc lập thống kê.

**Câu 14:** Làm thế nào để tăng tính an toàn của hệ mật không hoàn hảo:

- Khóa có độ dài bằng độ dài bản tin rõ.

- Khóa sử dụng một lần.

- Nén bản tin rõ.

**Câu 15:** Những câu nào dưới đây có trong mô tả cấu trúc mã khối:

- Hàm thay thế dùng để tăng tính nhập nhằng.

- Cấu trúc nhập nhằng dựa trên hàm phi tuyến.

- Thông tin bản rõ được khuếch tán vào tất cả các bit của bản tin mật.u\

**Câu 16:** Cho hệ mã Caesar mở rộng C=E([n,k],p) = np + k mod 26, p là ký tự bản rõ. Hãy thực hiện mã chuỗi ký tự “affine” với n = 5, k = 7. Chuỗi ký tự mã “rveqbo” tương ứng với bản rõ nào? Ghi kết quả cách nhau bằng dấu “,”. (***hggvub, cipher***)

**Bài 2:**

**Câu 1:** Cơ sở của các hệ mật khóa công khai dựa trên:

- Bài toán khó, hàm một chiều, thông tin cửa bẫy.

**Câu 2:** Quá trình xác thực nguồn gốc thông điệp trong truyền tin từ A đến B:

- Sử dụng khóa riêng của A.

**Câu 3:** Trong hệ mật kháo công khai, để bảo mật truyền dữ liệu gửi từ A đến B cần:

- Sử dụng khóa công khai B

**Câu 4:** Khóa chính (master key) thường dung trong:

- Phân phối khóa phiên.

**Câu 5:** Hệ mật RSA là:

- Phương pháp mật mã khối.

- Sử dụng bài toán khó phân tích số.

**Câu 6:** Hãy tính d trong quá trình sinh khóa RSA với p = 53, q = 83, chọn e = 17:

- 1505

**Câu 7:** Trong quá trình sinh khóa RSA, tính khó trong dự đoán khóa riêng phụ thuộc vào:

- Độ lớn của các số nguyên tố p và q.

**Câu 8:** Tác dụng của các số N1, N2 trong sơ đồ phân phối khóa đối xứng giữa hai bên A và B là:

- N1 dùng để xác thực phiên làm việc N2 dùng để xác thực hai bên.

- N1 dùng để chống Phát lại (Replay).

- Khóa phiên từ KDC tới B do A gửi.

**Câu 9:** Cơ chế cân bằng tải lượng giao dịch trong sơ đồ phân phối khóa đối xứng để:

- Đảm bảo hiệu năng hoạt động của hệ thống.

- Để chống tấn công phân tích và định vị.

**Câu 10:** Quá trình xác thực trong sơ đồ phân phối khóa đối xứng tập trung nằm ở các pha:

- Pha xác thực lẫn nhau hai bên qua giao thức challeng/response, pha xác thực các bên với trung tâm KDC.

**Câu 11:** Chứng thư số dùng để:

- Chống giả mạo khóa công khai.

- Giảm tải cho trung tâm quản lý giao dịch.

**Câu 12:** Danh sách chứng thư số bị thu hồi CRL:

- Chứa chứng thư số bị thu hồi trước hạn.

**Câu 13:** Bên cấp phát chứng thư số bảo vệ danh sách CRL bằng:

- Chống giả mạo và sửa đổi danh sách bằng chữ ký số.

**Câu 14:** Trên chứng thư số, việc chống giả mạo khóa công khai được xác định qua:

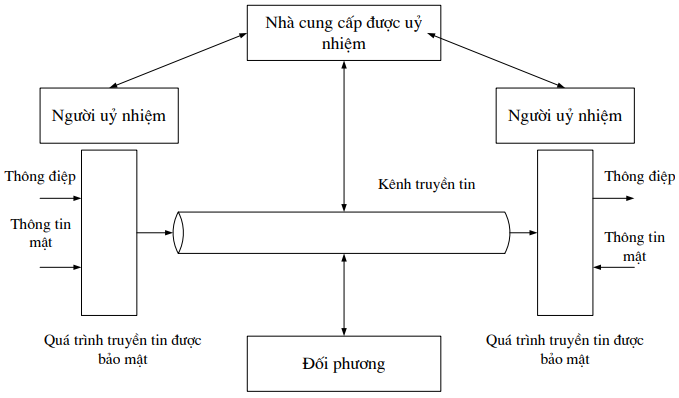
- Chữ ký số của bên cấp phát chứng thư số.

- Khóa riêng của bên cấp phát chứng thư số.

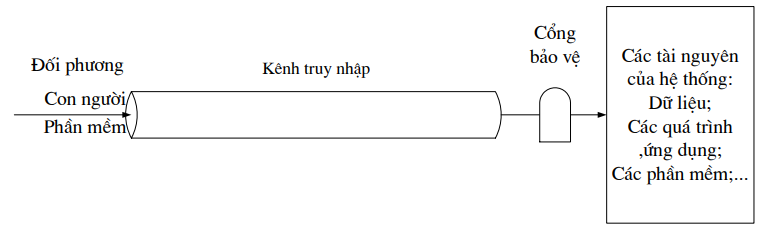
**\*) Một số mô hình:**

**Chương 1: Giới thiệu Nhập môn**

**Mô hình truyền tin an toàn**

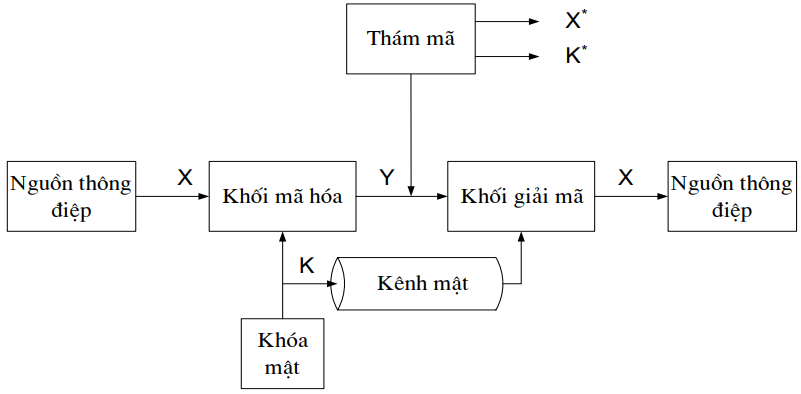


**Mô hình an toàn truy nhập hệ thống mạng**

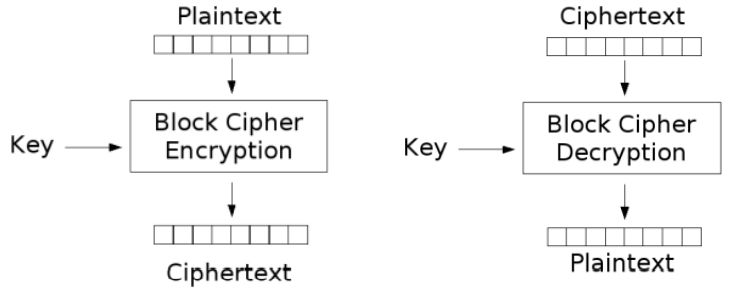


**Chương 2: Mã hóa đối xứng**

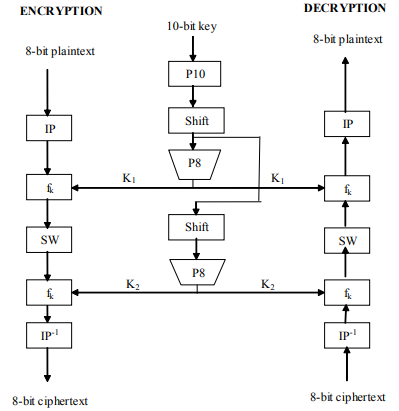
**Mô hình hệ thống mã hóa đối xứng**



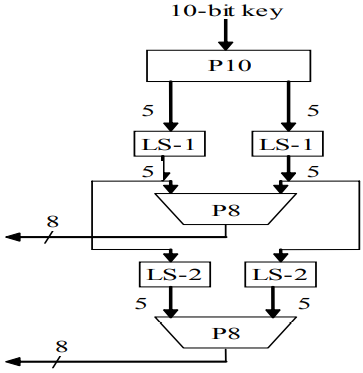
**Sơ đồ mã hóa và giải mã khối**



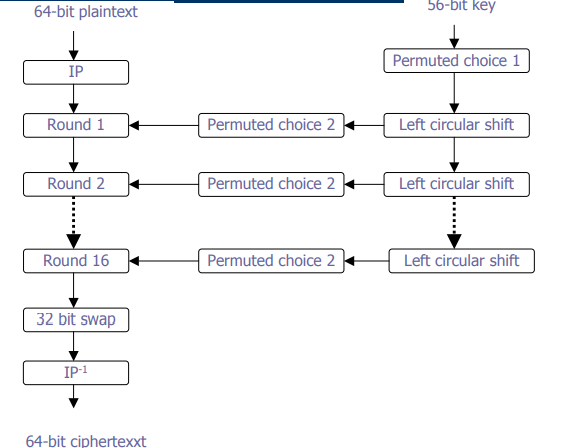
**Sơ đồ mã hóa và giải mã S-DES**



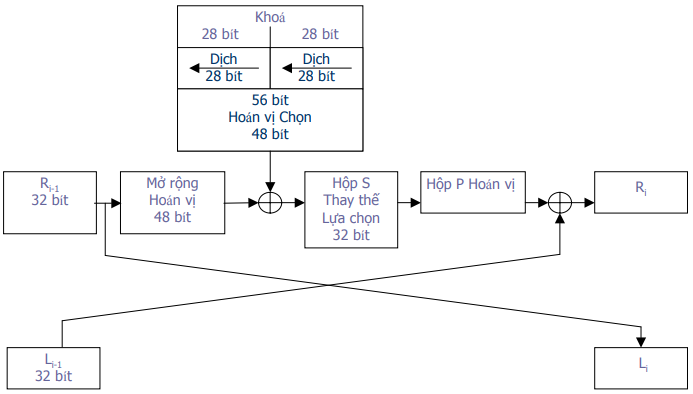
**Sơ đồ tạo khóa của thuật toán S-DES**



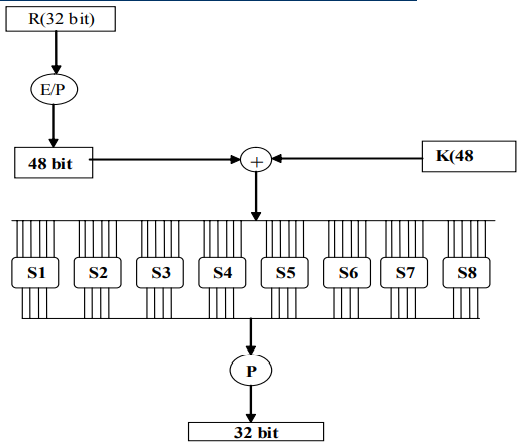
**Mô tả giải thuật chung của DES**



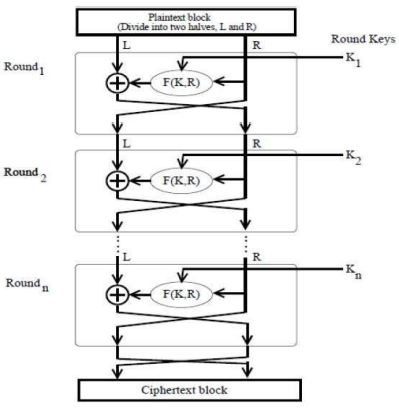
**Chi tiết một vòng lặp**



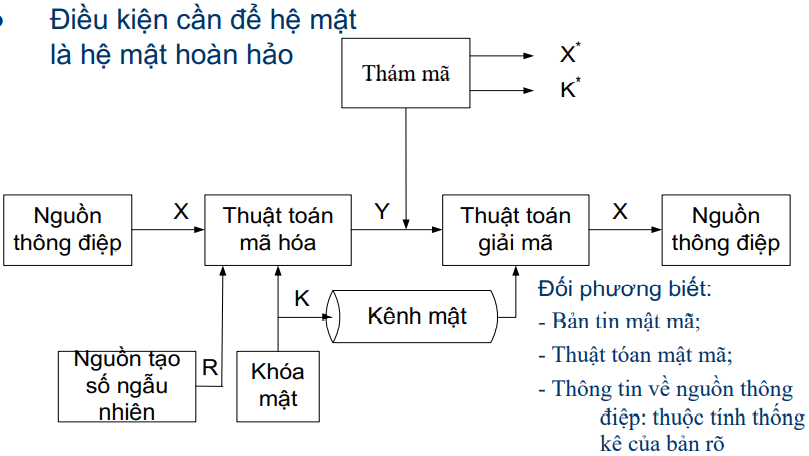
**Các hộp S-box**



**Mã khối lặp**

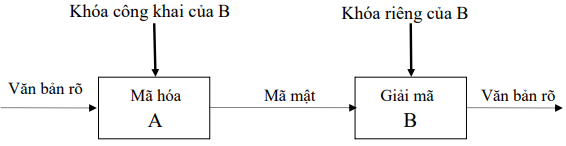


**Hệ mật hoàn hảo**

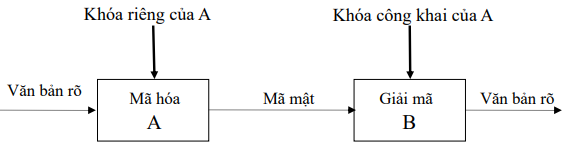


**Chương 3: Mã hóa công khai**

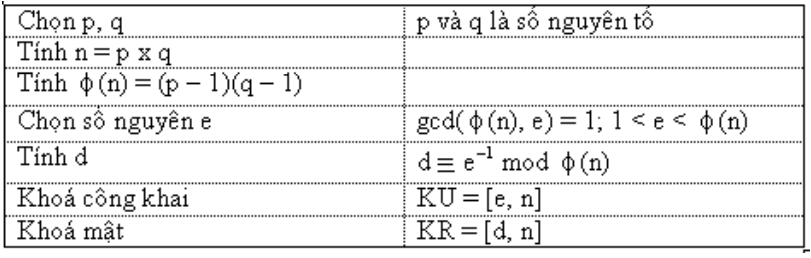
**Mô hình “Đảm bảo tính mật”**



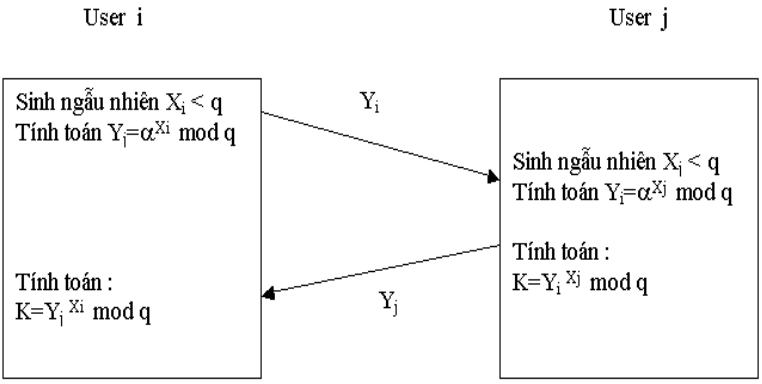
**Mô hình “Đảm bảo tính xác thực”**



**Sơ đồ tạo khóa RSA**



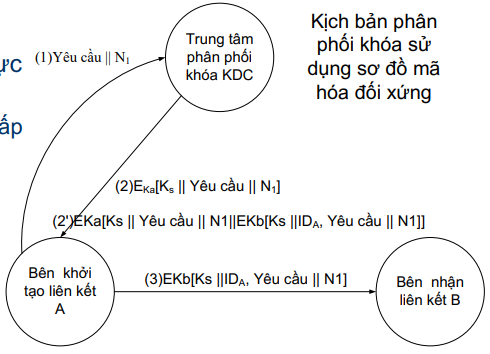
**Sơ đồ thuật toán Diffie-Hellman**



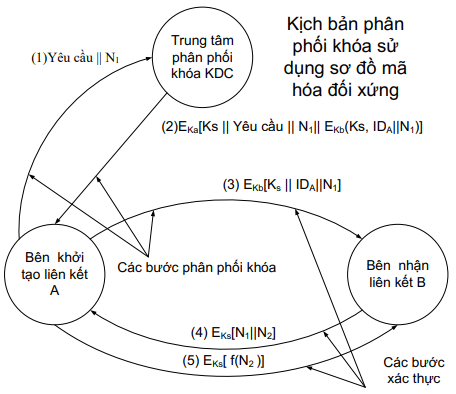
**Chương 4: Tin cậy 2 bên**

**\*) Phân phối khóa tập trung**

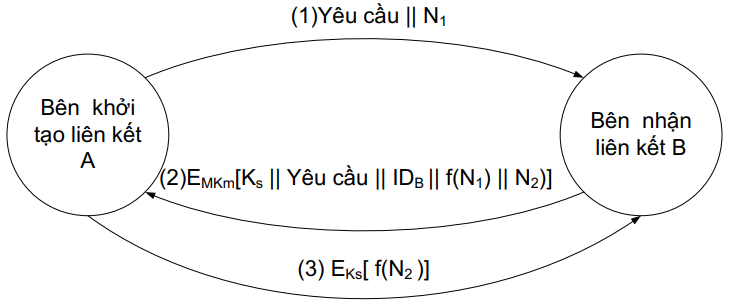
**Yêu cầu:**



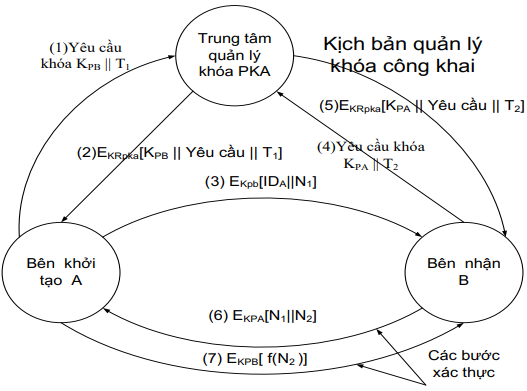
**Vấn đề xác thực:**



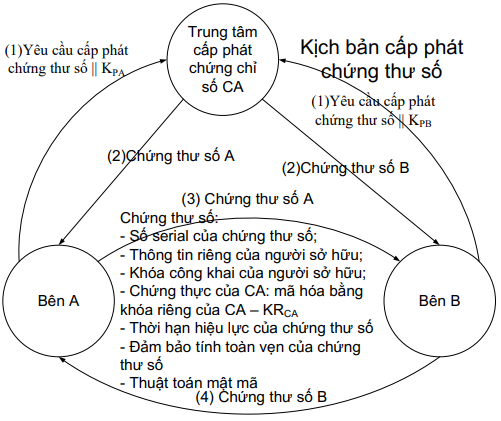
**\*) Phân phối khóa không tập trung**



**\*) Ủy quyền khóa công khai**

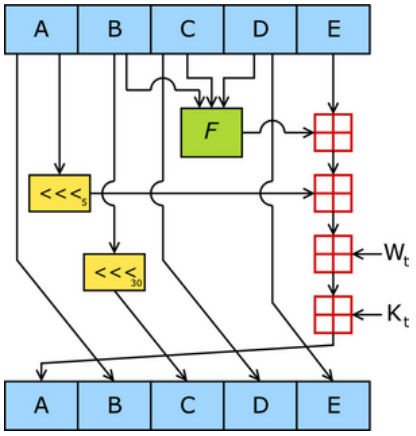


**\*) Chứng chỉ khóa công khai**



**Chương 5: Bài toán xác thực**

**Sơ đồ hoạt động SHA-1**



**Phần II: Tự luận**