Câu hỏi thi SEM 3 – NSC (An ninh mạng và Mật mã)

Câu 1 (5 điểm). Giới thiệu về mã hóa đối xứng bất đối xứng

1.1(1 điểm) Khái niệm.

1.2(1 điểm) Vẽ sơ đồ mã hóa và giải mã.

1.3(1 điểm) So sánh.

1.4(2 điểm) Viết chương trình mã hóa và giải mã bất đối xứng bằng ngôn ngữ C#.

Câu 2 (2 điểm). Lỗ hổng bảo mật

1. Khái niệm.

2. SQL Insert và cách phòng tránh.

Câu 3 3(3 điểm). Xác thực

Sử dụng phương pháp xác thực mật khẩu, hãy tìm hiểu một chương trình bằng ngôn ngữ C# mã hóa

(SHA-256) chuỗi mật khẩu của người dùng với thông tin sau:

Tên người dùng: Quản trị viên, Mật khẩu: Awdx!@#$%xdwa

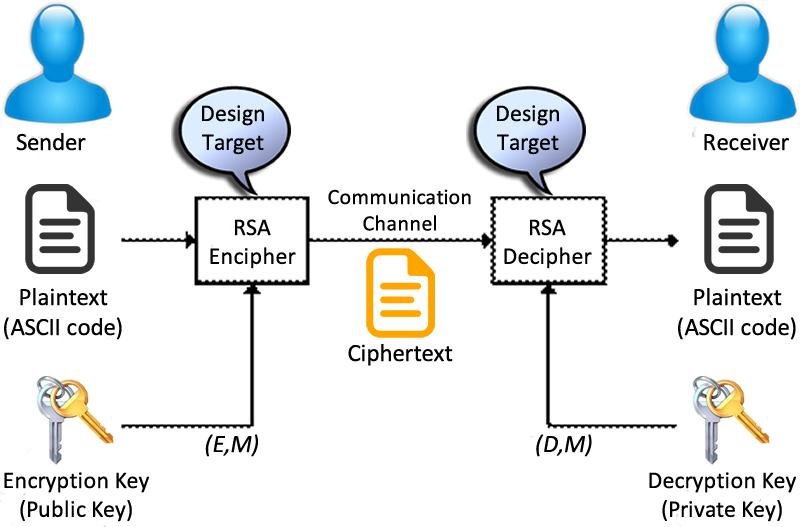
Câu 1

a)

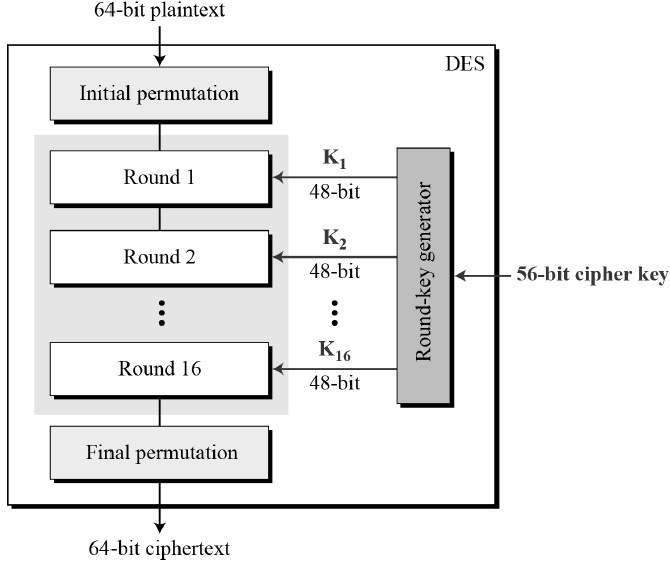
Mã hoá đối xứng (hay còn gọi là mã hoá bí mật): Nói đơn giản là người ta dùng cùng một chìa khoá để khoá và mở thông tin cần được giữ bí mật. Và cả hai bên gửi và nhận thông tin đều phải có chìa khoá này.

Mã hoá bất đối xứng (hay còn gọi là mã hoá công khai): Có thể hiểu là người ta dùng hai chìa khoá khác nhau để khoá và mở khoá thông tin bí mật. public key sẽ được công khai, và được gửi đi đến đối tượng cần mã hoá thông tin, còn private key được giữ bí mật, và nó đóng vai trò như chìa khoá vạn năng có thể mở được tất cả thông tin được khoá bằng public key.

b)



Ví dụ mô hình mã hóa bất đối xứng RSA



VÍ dụ mô hình mã hóa đối xứng DES

c) So sánh

- Mã hóa đối xứng dùng 1 key để mã hóa cũng như giải mã, còn mã hóa bất đối xứng dùng dùng 2 key khác nhau là public key và private key đễ mã hóa cũng như giải mã

- mã hóa đối xứng đơn giản ít phức tạp nhưng cũng dễ bị bẻ khóa nên không nên dùng trong các thông tin quan trọng

- mã hóa bất đối xứng phức tạp hơn, dịch mã lâu hơn mã hóa đối xứng nhưng an toàn hơn mã hóa đối xứng

2.

a)Lỗ hỏng bảo mật là điểm yếu trong hệ thống bảo mật trên ứng dụng,phần mềm, thiết bị,..

có thể gây rò gỉ thông tin cá nhân, dữ liệu quan trọng , độ an toàn của hệ thống

b)

SQL Insert ???

-SQL Injection là kĩ thuật insert sql gây phá hủy cơ sở dữ liệu của người dùng bằng cách đặt mã độc vào câu lệnh sql thông qua đầu vào của web

- cách phòng chống:

+ Tham số hóa truy vấn’

+ Xác thực dữ liệu đầu vào của người dùng

+ Ẩn thông tin của các thông báo

+ Hạn chế quyền

+ Backup dữ liệu thường xuyên