**SEM 3 – NSC ( Network Security and Cryptography) Exam Questions**

Họ và tên: Nguyễn Mạnh Hiếu

Lớp: T2207E

Bài1: Giới thiệu về mã hoá đối xứng

+) Khái niệm mã hoá bất đối xứng:

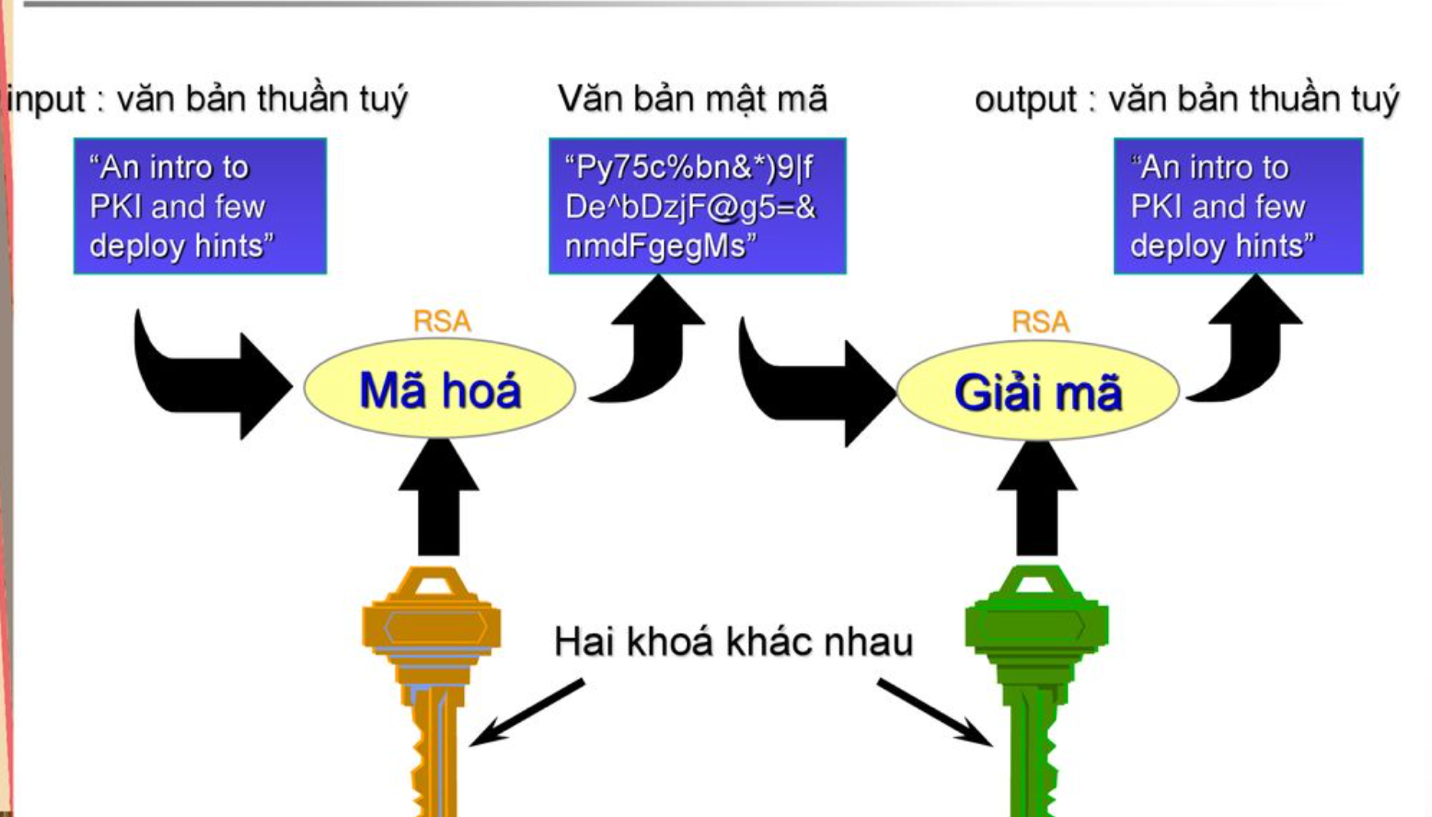
Mã hoá không đối xứng sử dụng một cặp khoá bao gồm khoá công khai (public key) Mã hóa không đối xứng sử dụng một cặp khóa bao gồm khóa công khai (public key) và khóa riêng tư (private key). Khóa công khai được chia sẻ công khai và được sử dụng để mã hóa dữ liệu, trong khi khóa riêng tư được bảo mật và chỉ được sử dụng để giải mã thông tin đã được mã hóa bằng khóa công khai tương ứng.

+) khái niệm mã hoá đối xứng:

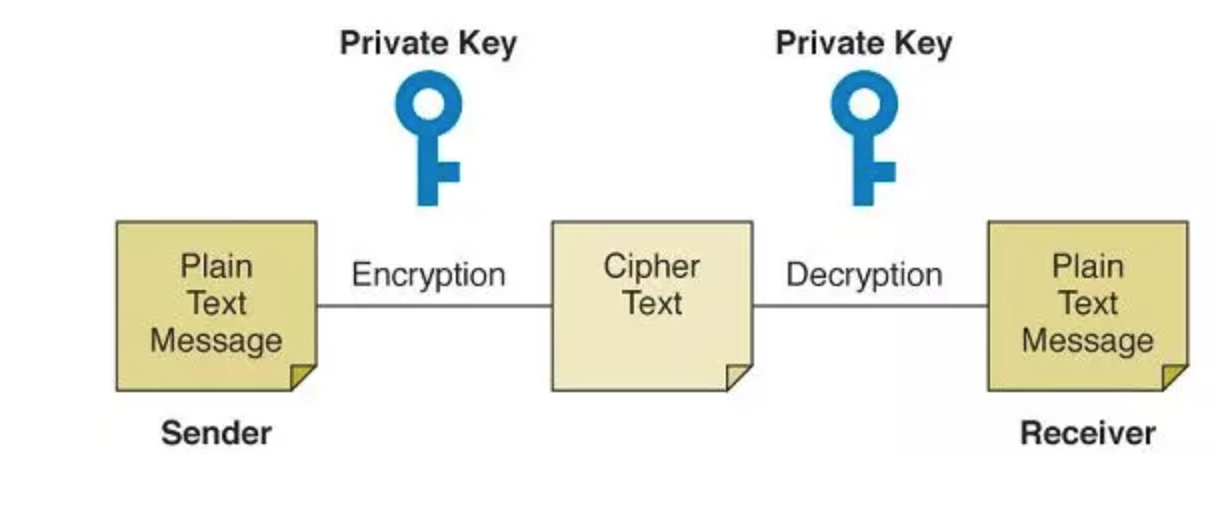
-) Mã hoá đối xứng sử dụng cùng một khóa để mã hóa và giải mã dữ liệu.

-) Khóa được sử dụng trong quá trình mã hóa và giải mã là giống nhau, nghĩa là cả hai bên liên quan đều biết và sử dụng cùng một khóa.

+) Hình vẽ mã hoá bất đối xứng:



+) hình vẽ mã hoá đối xứng



+) so sánh mã hoá bất đối xứng và đối xứng

-) Mã hóa đối xứng (symmetric encryption) sử dụng cùng một khóa để mã hóa và giải mã dữ liệu, trong khi mã hóa không đối xứng sử dụng một cặp khóa khác nhau.

-) Mã hóa đối xứng đơn giản hơn và nhanh hơn mã hóa không đối xứng, nhưng yêu cầu việc chia sẻ khóa bí mật giữa hai bên liên quan.

-) Mã hóa không đối xứng giúp giải quyết vấn đề chia sẻ khóa bí mật và cung cấp tính toàn vẹn dữ liệu và xác thực nguồn gốc thông qua việc sử dụng khóa riêng tư để giải mã.

Bài 2: Lỗ hổng bảo mật

1. Khái niệm

+) Lỗ hổng bảo mật là một điểm yếu hoặc một lỗ hổng trong hệ thống, ứng dụng hoặc quá trình mà tấn công viên có thể khai thác để xâm nhập, truy cập trái phép hoặc gây hại đến hệ thống hoặc dữ liệu. Lỗ hổng bảo mật có thể gây ra những hậu quả nghiêm trọng, như việc lộ thông tin nhạy cảm, mất dữ liệu, hoặc bị kiểm soát hoàn toàn bởi tấn công viên.

1. SQL Insert và cách phòng tránh

+) SQL Injection là một lỗ hổng bảo mật phổ biến trong các ứng dụng web sử dụng cơ sở dữ liệu. Kỹ thuật này cho phép tấn công viên chèn các câu lệnh SQL độc hại vào các trường dữ liệu đầu vào của ứng dụng, từ đó thực hiện các hành động không được ủy quyền như truy vấn, sửa đổi hoặc xóa dữ liệu trong cơ sở dữ liệu.

+) cách phòng tránh:

1. Sử dụng câu lệnh khuyến nghị: Sử dụng các câu lệnh khuyến nghị (prepared statements) hoặc truy vấn tham số hóa (parameterized queries) để tạo các truy vấn SQL. Điều này sẽ giúp tách biệt dữ liệu đầu vào và câu lệnh SQL, ngăn chặn tấn công viên chèn mã độc vào câu lệnh SQL.
2. Kiểm tra và xử lý dữ liệu đầu vào: Kiểm tra và xử lý kỹ lưỡng dữ liệu đầu vào từ người dùng để loại bỏ các ký tự đặc biệt hoặc thực hiện các phép escape để tránh việc chèn câu lệnh SQL độc hại.
3. Cập nhật và bảo mật hệ thống: Đảm bảo cập nhật và bảo mật hệ điều hành, cơ sở dữ liệu và phần mềm hệ thống để ngăn chặn các lỗ hổng bảo mật đã biết và tận dụng được.
4. Sử dụng công cụ bảo mật: Sử dụng các công cụ bảo mật, như Firewall ứng dụng web và Hệ thống phát hiện xâm nhập (Intrusion Detection System), để giám sát và ngăn chặn các hoạt động tấn công SQL Injection.