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

**Question 1 (5 points).** About asymmetric symmetric encryption

1.1(1 point) Concept.

1.2(1 point) Draw an encoding and decoding diagram.

1.3(1 point) Compare.

1.4(2 points) Write a program to encrypt and decrypt using asymmetric by C# language.

**Question 2 (2 points)**. Security Vulnerability

1. Concept.

2. SQL Injection and how to prevent it.

**Question 3 3(3 points)**. Authentication

Using the password authentication method, let's know a program in C# language that encrypts

**(SHA-256)** a user's password string with the following information:

*Username*: Admin, *Password*: Awdx!@#$%xdwa

Bài làm:

**Question 1**

**\*Mã hoá đối xứng:**   
-Khái niệm:

Là những hệ mật được sử dụng chung 1 khóa trong quá trình mã hóa và mã hóa.

Một số thuật toán mã hóa đối xứng được sử dụng phổ biến nhất bao gồm AES-128, AES-192 và AES-256.

-Sơ đồ:



Cơ chế hoạt động

+Người gửi sử dụng khóa chung (Ks) để mã hóa thông tin rồi gửi cho người nhận.

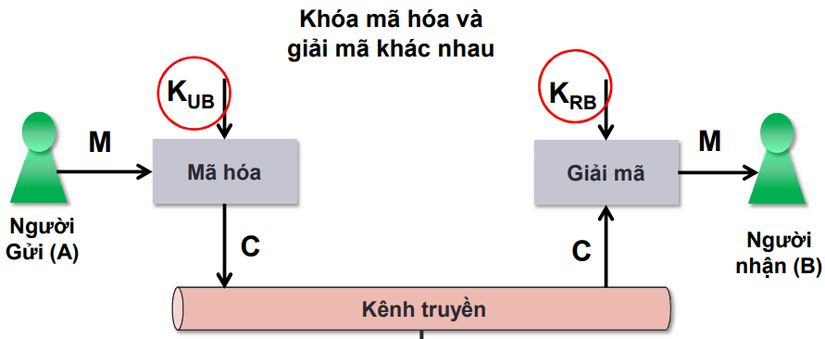
+Người nhận nhận được thông tin đó sẽ dùng chính khóa chung (Ks) để giải mã.

**\*Mã hoá bất đối xứng:**

-Khái niệm: là mã hoá mà thay vì người dùng dùng chung 1 khóa như ở hệ mật mã khóa đối xứng thì ở đây sẽ dùng 1 cặp khóa có tên là public key và private key.

Các kỹ thuật mã hóa bất đối xứng phổ biến bao gồm RSA, DSA và PKCS.

-Sơ đồ:



Cơ chế hoạt động

* Người gửi(A) gửi thông tin đã được mã hóa bằng khóa công khai (Kub) của người nhận(B) thông qua kênh truyền tin không bí mật
* Người nhận(B) nhận được thông tin đó sẽ giải mã bằng khóa riêng (Krb) của mình.
* Hacker cũng sẽ biết khóa công khai (Kub) của B tuy nhiên do không có khóa riêng (Krb) nên Hacker không thể xem được thông tin gửi

\*So sánh:

-Giống:

+Đều dùng để mã hoá

-Khác:

+Mã hóa bất đối xứng mất nhiều thời gian hơn để thực hiện do logic phức tạp liên quan. Vì lý do này, mã hóa đối xứng vẫn được ưu tiên sử dụng khi truyền dữ liệu hàng loạt.

+Mã hóa bất đối xứng an toàn hơn vì nó sử dụng các key khác nhau cho quá trình mã hóa và giải mã.

Câu2.  
-Lỗ hổng bảo mật (security vulnerability) là khuyết điểm trong quá trình lập trình hoặc việc cấu hình sai hệ thống mà qua đó tạo ra sơ hở dẫn đến kẻ tấn công mạng có thể truy cập trực tiếp dữ liệu mà bỏ qua quy trình thông thường.

Việc khai thác lỗ hổng bảo mật còn được gọi là Exploit sẽ giúp các Hacker tận dụng lỗ hổng bảo mật để đạt được lợi ích.

-SQL Injection: là một trong những cách tấn công mạng nhằm lấy dữ liệu qua SQL select

khi đăng nhập người dùng input user, password vào form đăng nhập, nếu coder kiểm tra bằng cách: select user from tblUser where user= inputUser AND password= inputPass thì hacker sẽ truy cập được vào tài khoản đó khi nhập pass= ' OR -- vì khi đó chuỗi select sẽ thành

select user from tblUser where user= inputUser AND password= inputPass OR 1=1

--> điều kiện luôn trả về giá trị TRUE.

bài học:

- khi check user, password không kiểm tra trực tiếp giá trị mà người dùng nhập vào

- sử dụng hash password

Câu 3.