TEST-Vũ Xuân Dự

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#.

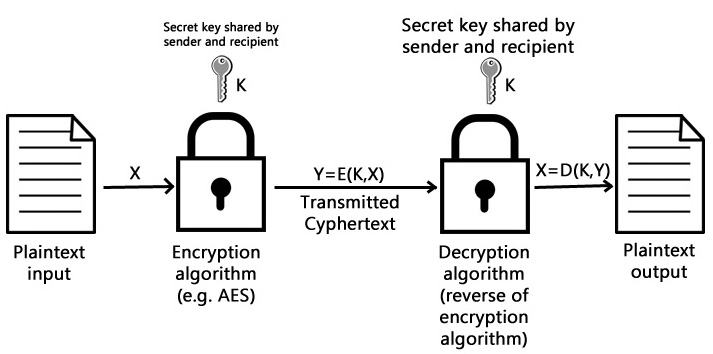
Bài làm

1.1. Khái niệm.

-Mã hóa đối xứng: Mã hóa đối xứng là một phương pháp trong lĩnh vực an ninh thông tin để bảo vệ dữ liệu bằng cách sử dụng một khóa (hoặc mật khẩu) để mã hóa và giải mã thông tin.

-Mã hóa bất đối xứng: Mã hóa bất đối xứng (asymmetric encryption), còn được gọi là mã hóa công khai, là một phương pháp mã hóa thông tin trong lĩnh vực an ninh thông tin, nơi có hai loại khóa được sử dụng: một khóa công khai (public key) và một khóa riêng tư (private key).

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



1.3. So sánh:

* Mã hóa đối xứng sử dụng cùng một khóa để mã hóa và giải mã, trong khi mã hóa bất đối xứng sử dụng cặp khóa: khóa công khai để mã hóa và khóa riêng tư để giải mã.
* Mã hóa đối xứng thường nhanh hơn vì không cần tính toán phức tạp như mã hóa bất đối xứng. Mã hóa bất đối xứng thường được sử dụng để giao tiếp an toàn, đảm bảo tính xác thực và chữ ký số.
* Mã hóa đối xứng thích hợp cho việc mã hóa dữ liệu lớn, trong khi mã hóa bất đối xứng thích hợp cho việc giao tiếp an toàn.

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

(Em làm trong file Question\_1-1.4)

Câu 2 (2 điểm). Lỗ hổng bảo mật

1. Khái niệm.

2. SQL Insert và cách phòng tránh.

Bài làm

1. Khái niệm: Lỗ hổng bảo mật (security vulnerability) là một điểm yếu hoặc sai sót trong hệ thống, ứng dụng, hoặc quy trình, có thể bị tấn công hoặc lợi dụng để đe dọa tính bảo mật và tính toàn vẹn của thông tin hoặc hệ thống.
2. SQL Injection và cách phòng tránh.

-Sử dụng Prepared Statements và Parameterized Queries:Sử dụng cách này, các tham số trong câu lệnh SQL được xác định trước và không bao giờ được kết hợp với dữ liệu người dùng trực tiếp. Điều này ngăn ngừa kẻ tấn công thêm mã SQL độc hại vào các trường dữ liệu.

-Input Validation: Kiểm tra và xác thực dữ liệu đầu vào từ người dùng trước khi nó được sử dụng trong câu lệnh SQL. Điều này bao gồm việc kiểm tra loại dữ liệu, giới hạn độ dài, và xóa hoặc mã hóa dữ liệu người dùng nếu cần.

-Security Testing: Thực hiện kiểm tra bảo mật định kỳ để phát hiện và giải quyết các lỗ hổng bảo mật trong ứng dụng và cơ sở dữ liệu.

-Hạn chế quyền truy cập của tài khoản cơ sở dữ liệu để đảm bảo rằng họ chỉ có quyền thực hiện các tác vụ cần thiết. Không nên sử dụng tài khoản có quyền quản trị (admin) cho các thao tác đơn giản.

-Regular Updates and Patch Management: Luôn duyệt các bản cập nhật và vá lỗ hổng của hệ thống quản lý cơ sở dữ liệu và ứng dụng web để đảm bảo rằng các lỗ hổng đã biết được khắc phục.

Câu 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

(Em làm trong file Question\_3.cs)