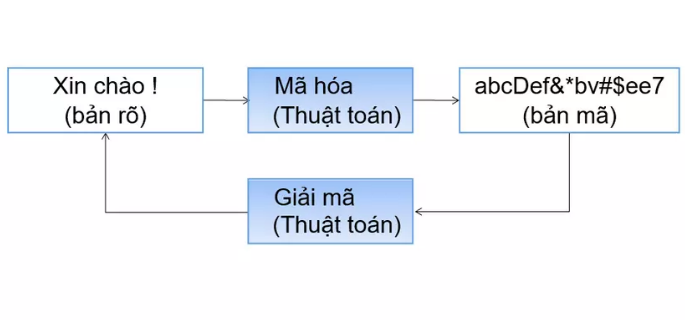
Câu 1:

1. Mã hóa đối xứng liên quan đến việc sử dụng một khóa duy nhất để mã hóa và giải mã dữ liệu, trong khi mã hóa bất đối xứng sử dụng hai khóa - một khóa chung và một khóa riêng - để mã hóa và giải mã dữ liệu . Mỗi loại mã hóa đều có điểm mạnh và điểm yếu riêng và việc lựa chọn giữa hai loại này tùy thuộc vào nhu cầu cụ thể của người dùng.
2. 
3. Có 2 loại mã hóa được triển khai phổ biến hiện nay là mã hóa đối xứng và bất đối xứng. Sự khác biệt cơ bản giữa 2 loại hình mã hóa này nằm ở chỗ mã hóa đối xứng sử dụng một key duy nhất cho cả hoạt động mã hóa và giải mã, trong khi mã hóa bất đối xứng sử dụng public key để mã hóa và private key để giải mã

Câu 2:

1. 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 dến kẻ tấn công mạng có thể truy cập trực tiếp dữ liệu mà bỏ qua quy trình thông thường.
2. SQL Injection là một trong những kiểu [hack](https://quantrimang.com/nhung-hieu-biet-co-ban-nhat-de-tro-thanh-hacker-phan-1-4650) web bằng cách inject các mã [SQL](https://quantrimang.com/sql) query/command vào input trước khi chuyển cho ứng dụng web xử lí, bạn có thể login mà không cần username và password, remote execution (thực thi từ xa), dump data và lấy root của [SQL server](https://quantrimang.com/SQL-server). Công cụ dùng để tấn công là một trình duyệt web bất kì, chẳng hạn như Internet Explorer, Netscape, Lynx, ….  
   Cách phòng tránh:  
   Các tổ chức có thể tập trung vào những bước sau đây để bảo vệ mình khỏi những cuộc tấn công SQL Injection:

* Không bao giờ được tin tưởng những input người dùng nhập vào: Dữ liệu luôn phải được xác thực trước khi sử dụng trong các câu lệnh SQL.
* Các thủ tục được lưu trữ: Những thủ tục này có thể trừu tượng hóa các lệnh SQL và xem xét toàn bộ input như các tham số. Nhờ đó, nó không thể gây ảnh hưởng đến cú pháp lệnh SQL.
* Các lệnh được chuẩn bị sẵn: Điều này bao gồm việc tạo truy vấn SQL như hành động đầu tiên và sau đó xử lý toàn bộ dữ liệu được gửi như những tham số.
* Những cụm từ thông dụng: Những cụm từ này được sử dụng để phát hiện mã độc và loại bỏ nó trước khi câu lệnh SQL được thực hiện.
* Thông báo lỗi đúng: Thông báo lỗi phải tuyệt đối tránh tiết lộ những thông tin/chi tiết nhạy cảm và vị trí xảy ra lỗi trên thông báo lỗi.
* Giới hạn quyền truy cập của người dùng đối với cơ sở dữ liệu: Chỉ những tài khoản có quyền truy cập theo yêu cầu mới được kết nối với cơ sở dữ liệu. Điều này có thể giúp giảm thiểu những lệnh SQL được thực thi tự động trên server.
* Hãy loại bỏ các kí tự meta như '"/\; và các kí tự extend như NULL, CR, LF, ... trong các string nhận được từ:
* input do người dùng đệ trình
* các tham số từ URL
* các giá trị từ cookie
* Đối với các giá trị numeric, hãy chuyển nó sang integer trước khi query SQL, hoặc dùng ISNUMERIC để chắc chắn nó là một số integer.
* Thay đổi "*Startup and run SQL Server*" dùng mức *low privilege user* trong tab SQL Server Security.
* Xóa các stored procedure trong database ***master*** mà không dùng như:
* xp\_cmdshell
* xp\_startmail
* xp\_sendmail
* sp\_makewebtask