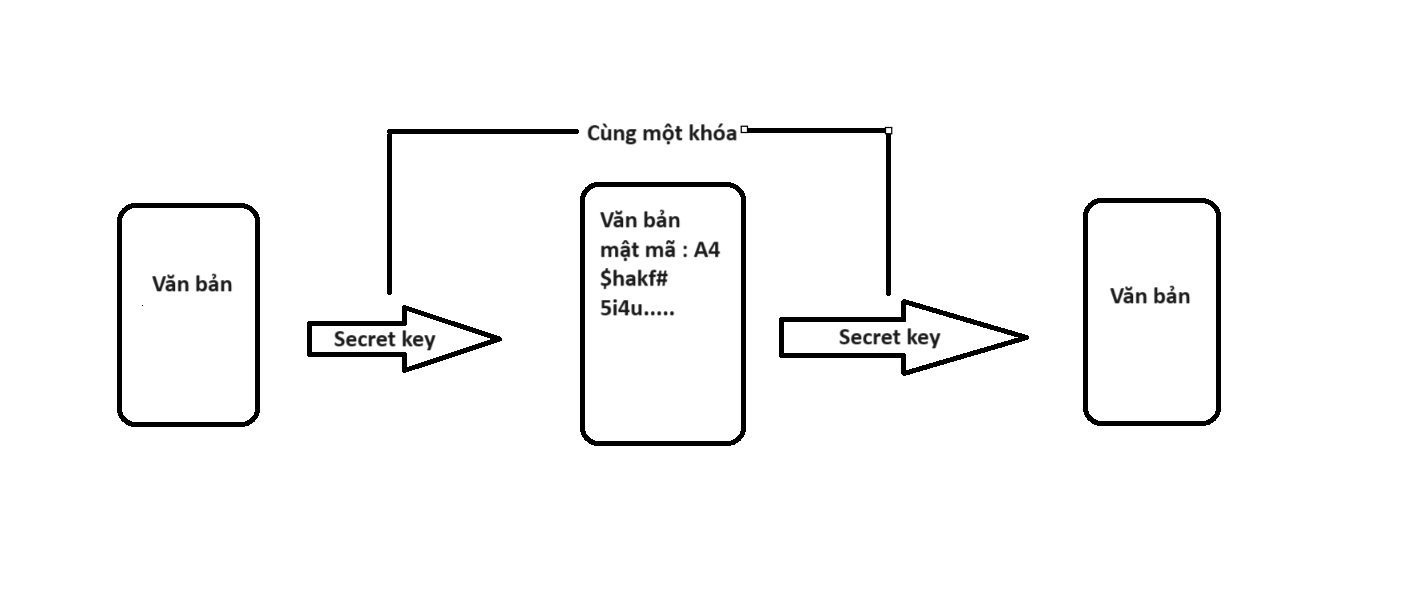
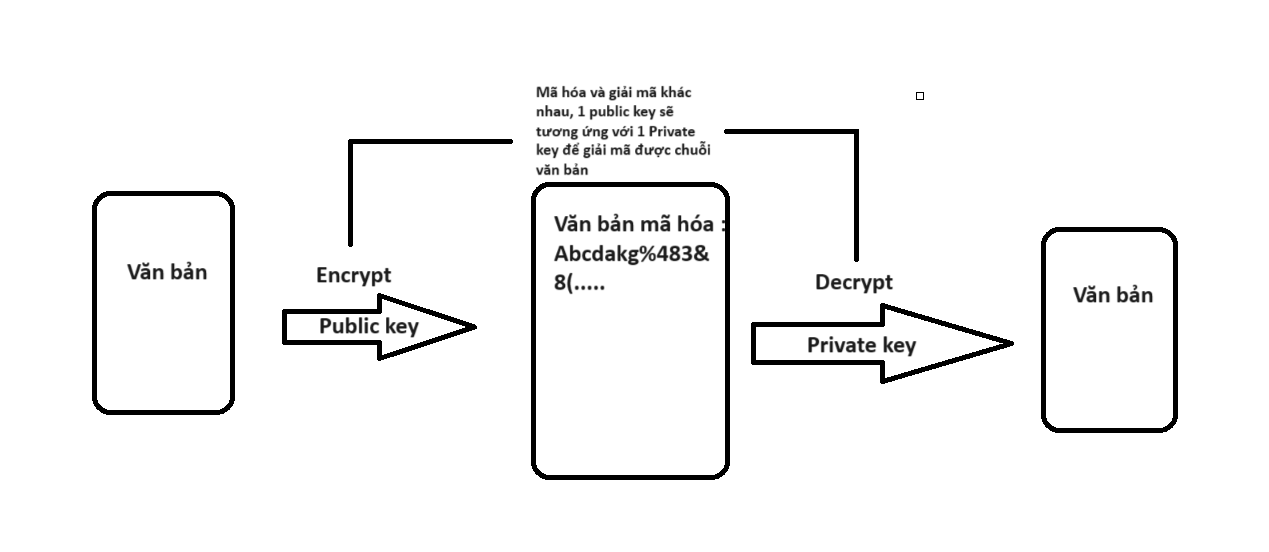
**Question 1 (5 points). About asymmetric symmetric encryption**

1. Khái niệm

* **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

1. Sở đồ
2. Mã hóa đối xứng:



1. Mã hóa bất đối xứng
2. So sánh

* Mã hóa đối xứng :
* Do thuật toán mã hóa đối xứng ít phức tạp hơn và có thể thực thi nhanh hơn, đây là kỹ thuật được đặc biệt ưa thích trong các hoạt động truyền tải dữ liệu hàng loạt.
* Văn bản gốc được mã hóa bằng một key trước khi gửi đi, và chính key này cũng sẽ được người nhận sử dụng để giải mã dữ liệu.
* Một số thuật toán mã hóa đối xứng được sử dụng phổ biến nhất bao gồm AES-128, AES-192 và AES-256.
* Mã hóa bất đối xứng:
  + Mã hóa bất đối xứng được cho là an toàn hơn mã hóa đối xứng vì nó sử dụng 2 key riêng biệt cho 2 quy trình mã hóa và giải mã.
  + Public key được sử dụng để mã hóa sẽ được công khai, nhưng private key để giải mã là hoàn toàn bí mật.
  + Phương pháp mã hóa này được sử dụng trong các giao tiếp hàng ngày qua internet.
  + Khi một tin nhắn được mã hóa bằng public key, nó chỉ có thể được giải mã bằng private key. Tuy nhiên, khi một tin nhắn được mã hóa bằng private key, nó có thể được giải mã bằng public key.
  + Chứng chỉ kỹ thuật số trong mô hình máy khách-máy chủ có thể được sử dụng để tìm thấy các public key.
  + Điểm hạn chế của mã hóa bất đối xứng là mất nhiều thời gian thực hiện hơn so với mã hóa đối xứng.
  + Các kỹ thuật mã hóa bất đối xứng phổ biến bao gồm RSA, DSA và PKCS.

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

1. Concept.
   * 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 and how to prevent it

SQL injection:

* + SQL Injection xảy ra khi ứng dụng web không kiểm tra hoặc xử lý đầu vào của người dùng đúng cách trước khi thực hiện truy vấn SQL. Khi một người dùng nhập dữ liệu động (như một trường tìm kiếm hoặc biểu mẫu đăng nhập), kẻ tấn công có thể chèn mã SQL độc hại để lừa ứng dụng thực hiện truy vấn không mong muốn.
  + VD: SELECT \* FROM users WHERE username='admin' AND password='' OR '1'='1'

Phòng trống :

* + Không tin tưởng input của người dùng
  + Xác nhận chuỗi các input ở phía máy chủ
  + Sử dụng câu lệnh tham số ví dụ như call Procedure