Câu 1: Giới thiệu về mã hóa đối xứng và bất đối xứng

1.1 Khái niệm:

* Mã hóa đối xứng (Symmetric Encryption): là phương pháp mã hóa sử dụng cùng một khóa để mã hóa và giải mã dữ liệu. Trong mã hóa đối xứng, khóa được chia sẻ giữa người gửi và người nhận. Hai thuật toán chính trong mã hóa đối xứng là thuật toán mã hóa và thuật toán giải mã.
* Mã hóa bất đối xứng (Asymmetric Encryption): là phương pháp mã hóa sử dụng hai khóa khác nhau, gọi là khóa công khai (public key) và khóa bí mật (private key). Khóa công khai được chia sẻ với mọi người trong khi khóa bí mật chỉ được giữ bởi người nhận. Hai thuật toán chính trong mã hóa bất đối xứng là thuật toán mã hóa và thuật toán giải mã.

1.2 Sơ đồ mã hóa và giải mã:

+----------------+ +------------------------+

| | | |

| Dữ liệu gốc | | Dữ liệu mã hóa |

| | | |

+----------------+ +------------------------+

| |

| |

| |

| |

+-----------v-----------+ +----------------v----------------+

| | | |

| Mã hóa bất đối xứng | | Giải mã bất đối xứng |

| | | |

+-----------+-----------+ +----------------+---------------+

| |

| |

| |

| |

+-----------v-----------+ +----------------v----------------+

| | | |

| Khóa công khai | | Khóa bí mật |

| | | |

+-----------+-----------+ +----------------+---------------+

| |

| |

| |

| |

+-----------v-----------+ +----------------v----------------+

| | | |

| Thuật toán mã hóa | | Thuật toán giải mã |

| | | |

+-----------+-----------+ +----------------+---------------+

| |

| |

| |

| |

+-----------v-----------+ +----------------v----------------+

| | | |

| Dữ liệu mã hóa | | Dữ liệu giải mã |

| | | |

|  |  |  |
| --- | --- | --- |
| Mô hình mã hóa đối xứng |  |  |

1.3 So sánh:

* Mã hóa đối xứng:
  + Ưu điểm: Tốc độ mã hóa và giải mã nhanh, phù hợp cho việc xử lý dữ liệu lớn.
  + Nhược điểm: Yêu cầu chia sẻ khóa bí mật giữa người gửi và người nhận.
* Mã hóa bất đối xứng:
  + Ưu điểm: Không yêu cầu chia sẻ khóa bí mật, an toàn hơn trong việc truyền khóa. Có thể sử dụng cho chữ ký điện tử và giao tiếp an toàn qua mạng.
  + Nhược điểm: Tốc độ mã hóa và giải mã chậm hơn mã hóa đối xứng.

Câu 2 : Lỗ hổng bảo mật 1:

- Khái niệm của lỗ hổng bảo mật 1 thường liên quan đến một vấn đề nào đó trong hệ thống, phần mềm hoặc môi trường mà khi được khai thắc có thể cho phép kẻ tấn công thực hiện các hành động không được uỷ quyền hoặc gây hại đối với hệ thống, thông tin hoặc người dùng.

+ Lỗ hổng bảo mật trong phần mềm  
+ Lỗ hổng bảo mật trong mạng  
+ Lỗ hổng bảo mật trong quản lý dự liệu