# **CHƯƠNG 2: ỨNG DỤNG CỦA DES TRONG MÃ HÓA DỮ LIỆU**

## **2.1. Nghiên cứu, tìm hiểu về hệ mã hóa khóa bí mật**

#### ****2.1.1. Khái niệm mã hóa khóa bí mật (Symmetric Encryption)****

* **Mã hóa khóa bí mật**, còn gọi là **mã hóa đối xứng**, là một phương pháp mã hóa trong đó cả việc **mã hóa** và **giải mã** dữ liệu đều sử dụng cùng một khóa bí mật.
* Khóa này cần được giữ bí mật và chia sẻ an toàn giữa các bên tham gia trong quá trình truyền tải hoặc lưu trữ dữ liệu.

#### ****2.1.2. Đặc điểm của mã hóa khóa bí mật****

#### ****2.1.3. Nguyên tắc hoạt động của mã hóa khóa bí mật****

**Bước 1: Mã hóa dữ liệu**

* + Bên gửi sử dụng khóa bí mật để mã hóa dữ liệu plaintext (dữ liệu ban đầu) thành ciphertext (dữ liệu mã hóa).
  + Ciphertext này được gửi qua kênh truyền tải đến bên nhận.

**Bước 2: Giải mã dữ liệu**

* + Bên nhận sử dụng cùng một khóa bí mật để giải mã ciphertext, khôi phục dữ liệu về dạng plaintext gốc.

**Quy trình:**

* + Mã hóa và giải mã đều dựa trên các phép toán toán học hoặc logic cụ thể (ví dụ: thay thế và hoán vị).

#### ****2.1.4. Các thuật toán mã hóa khóa bí mật phổ biến****

**DES (Data Encryption Standard):**

#### ****2.1.5. Ứng dụng của mã hóa khóa bí mật****

**Bảo mật dữ liệu trong truyền tải:**

* + Được sử dụng trong các giao thức như SSL/TLS để mã hóa dữ liệu truyền qua mạng Internet.

**Mã hóa tệp tin và cơ sở dữ liệu:**

* + Thông tin nhạy cảm được mã hóa để đảm bảo rằng chỉ những người có khóa bí mật mới có thể truy cập.

**Mã hóa trong hệ thống nhúng và IoT:**

* + Các thiết bị nhỏ gọn thường sử dụng mã hóa đối xứng để giảm chi phí xử lý.

**Hệ thống tài chính:**

* + Bảo mật mã PIN, giao dịch ngân hàng, và các hệ thống ATM sử dụng mã hóa khóa bí mật để đảm bảo an toàn.

#### ****2.1.6. Ưu điểm và nhược điểm của mã hóa khóa bí mật****

**Ưu điểm:**

* **Hiệu suất cao:** Tốc độ mã hóa/giải mã nhanh, phù hợp với xử lý dữ liệu lớn.
* **Đơn giản:** Cơ chế dễ triển khai, không yêu cầu nhiều tài nguyên.

**Nhược điểm:**

* **Vấn đề phân phối khóa:** Khó khăn trong việc trao đổi và bảo mật khóa trong môi trường không tin cậy.
* **Không phù hợp cho nhiều người dùng:** Nếu có nhiều người tham gia, cần có một khóa riêng cho từng cặp, dẫn đến sự phức tạp trong quản lý khóa.

#### ****2.1.7. Các thách thức và giải pháp****

**Thách thức:**

* + **Phân phối khóa an toàn:** Làm thế nào để chia sẻ khóa bí mật mà không bị rò rỉ trong quá trình truyền tải.
  + **Tấn công brute-force:** Đảm bảo kích thước khóa đủ lớn để tránh bị bẻ khóa.

**Giải pháp:**

* + **Kết hợp với mã hóa khóa công khai:** Sử dụng các thuật toán khóa công khai (như RSA) để phân phối khóa bí mật an toàn.
  + **Sử dụng thuật toán hiện đại:** Thay thế các thuật toán yếu như DES bằng AES hoặc các tiêu chuẩn an toàn hơn.

## **2.2. Các ứng dụng của DES trong mã hóa dữ liệu**

### **2.2.1. Bảo mật thông tin trong truyền thông**

### **2.2.2. Mã hóa dữ liệu trong ngân hàng**

### **2.2.3. Ứng dụng trong hệ thống lưu trữ dữ liệu**

### **2.2.4. Ứng dụng trong các thiết bị phần cứng**

### **2.2.5. Ứng dụng trong phát triển hệ thống mã hóa**

### **2.2.6. Ứng dụng trong các hệ thống chính phủ**

**2.3. Nghiên cứu việc triển khai DES trong các hệ thống mã hóa**

#### ****2.3.1. Mô tả cấu trúc triển khai DES trong thực tế****

* **Chức năng chính:** DES (Data Encryption Standard) được sử dụng để mã hóa dữ liệu nhạy cảm trong các hệ thống. Trong hệ thống mã hóa cơ bản, DES sẽ thực hiện việc mã hóa thông tin từ dạng plaintext (dữ liệu thông thường) sang ciphertext (dữ liệu mã hóa) trước khi lưu trữ hoặc truyền tải.
* **Triển khai:**
  1. Hệ thống chỉ cần hai thành phần chính: một mô-đun mã hóa/giải mã DES và một kho khóa bí mật (Secret Key Storage).
  2. Được ứng dụng trong các kịch bản đơn giản như mã hóa dữ liệu trong các file lưu trữ hoặc truyền tải thông tin giữa hai bên trong một mạng cục bộ (LAN).

**2.3.1.2. Tích hợp DES vào các hệ thống lớn**

* **Trong cơ sở dữ liệu:**
  + DES được tích hợp để mã hóa các trường dữ liệu quan trọng (như mật khẩu, thông tin cá nhân). Ví dụ: CSDL sử dụng DES để mã hóa trước khi lưu trữ và giải mã khi truy vấn.
* **Trong hệ thống lưu trữ đám mây:**
  + DES được tích hợp để mã hóa dữ liệu trước khi tải lên đám mây, đảm bảo rằng dữ liệu ở trạng thái mã hóa trong toàn bộ vòng đời lưu trữ.
  + Quản lý khóa được xử lý bởi các dịch vụ bảo mật chuyên biệt (Key Management Services - KMS) để tránh việc rò rỉ khóa mã hóa.

#### ****2.3.2. Các thành phần chính trong hệ thống mã hóa sử dụng DES****

**2.3.2.1. Thành phần xử lý mã hóa/giải mã**

* **Vai trò:** Đảm nhận chức năng chuyển đổi dữ liệu giữa plaintext và ciphertext bằng thuật toán DES.
* **Cấu trúc:**
  + Gồm các mô-đun:
    - Mã hóa DES (Encryption Module): Sử dụng khóa bí mật để chuyển đổi plaintext thành ciphertext.
    - Giải mã DES (Decryption Module): Sử dụng cùng khóa bí mật để chuyển đổi ciphertext trở lại plaintext.
  + Áp dụng các bước chính trong DES: Permutation, Substitution, và Key Schedule (tạo khóa con cho từng vòng).

**2.3.2.2. Thành phần quản lý và phân phối khóa**

#### ****2.3.3. Cách thức hoạt động****

**2.3.3.1. Quy trình chuyển đổi plaintext sang ciphertext bằng DES**

* **Các bước cơ bản:**
  1. **Chia nhỏ dữ liệu:** Chia dữ liệu đầu vào thành các khối 64-bit.
  2. **Mã hóa từng khối:** Áp dụng thuật toán DES (16 vòng mã hóa với hoán vị và thay thế) lên từng khối.
  3. **Ghép nối khối mã hóa:** Tạo ra ciphertext hoàn chỉnh.
* **Giải mã:** Thực hiện quy trình ngược lại để lấy lại plaintext từ ciphertext.

**2.3.3.2. Cơ chế đảm bảo tính toàn vẹn và an toàn**

* **Checksum hoặc MAC (Message Authentication Code):** Kết hợp DES với các kỹ thuật như HMAC để đảm bảo tính toàn vẹn của dữ liệu.
* **Bảo vệ trong truyền tải:**
  + Sử dụng các giao thức như SSL/TLS để mã hóa kênh truyền tải.
  + Dữ liệu được mã hóa bằng DES sẽ được truyền qua kênh mã hóa này để tăng mức độ bảo mật.

#### ****2.3.4. Ứng dụng cụ thể****

**2.3.4.1. Hệ thống bảo mật sử dụng DES trong giao dịch tài chính**

**– Lý do sử dụng DES trong ATM:**

1. DES được thiết kế để thực hiện trên phần cứng chuyên dụng (như các chip mã hóa trong ATM), giúp tăng tốc độ xử lý.
2. Tại thời điểm DES được phổ biến, đây là thuật toán phù hợp cho các hệ thống giao dịch tài chính với chi phí phần cứng thấp và độ phức tạp vừa phải.

#### ****2.3.4.2. Phân tích ưu điểm và nhược điểm khi sử dụng DES trong hệ thống****

**– Ưu điểm:**

**– Nhược điểm:**