**CHƯƠNG 2. KẾT QUẢ NGHIÊN CỨU**

**2. 1. Nghiên cứu, tìm hiểu hệ mã hóa khóa bí mật**

**2.1.1 Khái niệm**

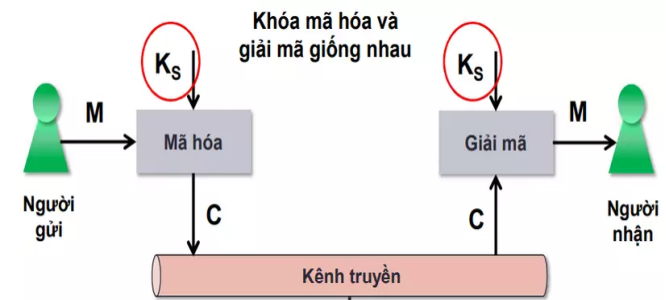
- Mã hóa khóa bí mật, còn gọi là mã hóa đối xứng hay mã hóa khóa riêng, là sử dụng một khóa cho cả quá trình mã hóa (được thực hiện bởi người gửi thông tin) và quá trình giải mã (được thực hiện bởi người nhận).

- Người gửi thông điệp sử dụng một khóa mật mã để mã hóa thông điệp và người nhận thông điệp cũng sử dụng một khóa như vậy để đọc mật mã hoặc giải mã thông điệp.

- Kĩ thuật mã hóa khóa bí mật này đã được IBM phát triển, áp dụng cho các cơ quan của Chính Phủ Mỹ năm 1977 được gọi là Tiêu chuẩn mã hóa dữ liệu (DES- data encryption standard).

- Quá trình mã hóa khóa bí mật được thực hiện như sau:

Một khách hàng (Anne) muốn gửi tới người bán hàng (Bob) một đơn đặt hàng, nhưng chỉ muốn một mình Bob có thể đọc được. Anne mã hóa đơn đặt hàng (dưới dạng văn bản gốc) của mình bằng một mã khóa rồi gửi đơn đặt hàng đã mã hóa đó cho Bob. Tất nhiên, ngoài Bob và Anne ra, không ai có thể đọc được nội dung thông điệp lộn xộn đã mã hóa. Khi nhận được thông điệp mã hóa, Bob giải mã thông điệp này bằng khóa giải mã và đọc các thông tin của đơn đặt hàng. Điều đáng chú ý là trong kĩ thuật mã hóa khóa bí mật, khóa để mã hóa thông điệp và khóa để giải mã thông điệp không giống như nhau.

****

**2.1.2 Hạn chế của kỹ thuật**

- Kĩ thuật mã hóa khóa bí mật là một phương pháp mã hóa thông tin hữu dụng trong nhiều trường hợp. Tuy nhiên, nó cũng có những hạn chế. Các bên tham gia trong quá trình mã hóa cần phải tin tưởng nhau và phải chắc chắn rằng, bản sao của mã hóa đang được đối tác bảo vệ cẩn mật. Thêm vào đó, nếu người gửi và người nhận thông điệp ở hai nơi khác nhau.

- Họ phải đảm bảo rằng, khi họ gặp mặt hoặc sử dụng một phương tiện thông tin liên lạc chung (hệ thống điện thoại, dịch vụ bưu chính) để trao mã khóa cho nhau không bị người khác nghe trộm hay bị lộ mã khóa.

- Bởi vì nếu như vậy, những người này sau đó có thể sử dụng mã khoá để đọc lén các thông điệp mà các bên gửi cho nhau. Điều này làm xuất hiện những trở ngại lớn trong việc quản lí (tạo, phân phối và lưu giữ) các mã khóa. Do sử dụng chung một khoá, cả người gửi lẫn người nhận thông báo đều phải biết khoá. Việc mã hoá và giải mã thông báo sử dụng mã hoá đối xứng rất nhanh và hiệu quả.

- Tuy nhiên, khoá dễ bị lộ và quá trình phân phối khoá cho các thành viên rất khó khăn do không thích hợp trong các môi trường lớn, chẳng hạn như Internet. Vì phải có một khoá riêng cho mỗi cặp người sử dụng nên cần phải có số lượng lớn sự kết hợp các cặp khoá. Để cho 12 người có thể liên lạc an toàn với nhau đã cần tới 66 cặp khoá riêng. Tổng quát, với N máy khách cá nhân, cần N(N-1)/2 cặp khoá.

**2.2. Mã hóa dữ liệu và ứng dụng trong thực tế**

Mã hóa dữ liệu (Data Encryption) là quá trình chuyển đổi thông tin từ dạng rõ ràng (plaintext) thành dạng mã hóa (ciphertext) để bảo vệ dữ liệu khỏi các truy cập trái phép. Dữ liệu mã hóa chỉ có thể được giải mã và đọc được bởi những người có khóa giải mã thích hợp. Đây là nền tảng của an ninh thông tin trong thời đại kỹ thuật số, đảm bảo dữ liệu được an toàn trong quá trình lưu trữ và truyền tải.

**2.2.1. Mục đích của mã hóa dữ liệu**

Mã hóa không chỉ bảo vệ dữ liệu cá nhân mà còn bảo vệ các giao dịch nhạy cảm, dữ liệu doanh nghiệp và thông tin liên lạc trên toàn cầu. Mục tiêu chính của mã hóa dữ liệu bao gồm:

- Bảo mật thông tin: Ngăn chặn việc truy cập trái phép và bảo vệ dữ liệu khỏi các cuộc tấn công.

- Đảm bảo tính toàn vẹn: Bảo vệ dữ liệu khỏi sự giả mạo hoặc chỉnh sửa trái phép trong quá trình truyền tải hoặc lưu trữ.

- Bảo vệ quyền riêng tư: Giới hạn quyền truy cập vào dữ liệu chỉ cho những người có thẩm quyền.

- Tăng cường độ tin cậy: Xây dựng niềm tin của người dùng vào các hệ thống và dịch vụ kỹ thuật số nhờ vào việc bảo vệ thông tin cá nhân và giao dịch nhạy cảm.

**2.2.2. Quy trình Mã hóa Dữ liệu**

Mã hóa dữ liệu bao gồm hai giai đoạn chính: mã hóa và giải mã, với các bước chi tiết như sau:

a. Mã hóa (Encryption):

- Dữ liệu ban đầu được chuyển đổi thành dạng không thể đọc được thông qua một thuật toán mã hóa.

- Một khóa mã hóa được sử dụng để kiểm soát quá trình này, đảm bảo chỉ người sở hữu khóa mới có thể mã hóa hoặc giải mã dữ liệu.

b. Giải mã (Decryption):

- Dữ liệu mã hóa được chuyển đổi trở lại thành dữ liệu ban đầu bằng cách sử dụng thuật toán và khóa giải mã tương ứng.

Ví dụ, khi một tin nhắn được mã hóa, người gửi sử dụng khóa mã hóa để chuyển đổi tin nhắn thành mã và người nhận sử dụng khóa giải mã để đọc được nội dung ban đầu.

**2.2.3. Các Loại Mã hóa Dữ liệu**

Có hai loại mã hóa chính: mã hóa đối xứng và mã hóa bất đối xứng, mỗi loại có đặc điểm và ứng dụng khác nhau.

a. Mã hóa Đối xứng (Symmetric Encryption)

- Nguyên lý hoạt động: Cùng một khóa được sử dụng để mã hóa và giải mã dữ liệu.

- Ưu điểm:

- Hiệu suất cao: Tốc độ mã hóa nhanh, phù hợp cho khối lượng dữ liệu lớn.

- Đơn giản và dễ triển khai: Quá trình mã hóa không yêu cầu nhiều tài nguyên.

- Nhược điểm:

- Quản lý khóa phức tạp: Khi số lượng người dùng tăng, việc phân phối và bảo mật khóa trở nên khó khăn.

- Ứng dụng: Mã hóa đối xứng được sử dụng phổ biến trong các hệ thống lưu trữ dữ liệu, VPN, mã hóa ổ đĩa, và các giao thức bảo mật như SSL/TLS.

- Thuật toán tiêu biểu:

- AES (Advanced Encryption Standard)

- DES (Data Encryption Standard)

b. Mã hóa Bất đối xứng (Asymmetric Encryption)

- Nguyên lý hoạt động: Sử dụng hai khóa khác nhau nhưng liên kết chặt chẽ: khóa công khai (public key) để mã hóa và khóa bí mật (private key) để giải mã.

- Ưu điểm:

- An toàn hơn trong môi trường mở: Không cần chia sẻ khóa bí mật, giảm nguy cơ bị lộ khóa.

- Hỗ trợ chữ ký số và xác thực: Đảm bảo danh tính người gửi và bảo vệ tính toàn vẹn của dữ liệu.

- Nhược điểm:

- Tốc độ chậm hơn mã hóa đối xứng: Do các phép toán phức tạp hơn.

- Cần nhiều tài nguyên: Đòi hỏi sức mạnh xử lý cao hơn để mã hóa dữ liệu.

- Ứng dụng: Mã hóa bất đối xứng được sử dụng trong email bảo mật (PGP), giao dịch tài chính trực tuyến, chữ ký số, và hệ thống PKI (Public Key Infrastructure).

- Thuật toán tiêu biểu:

- RSA (Rivest-Shamir-Adleman)

- Elgamal

2.2.4. Ứng dụng thực tế của mã hóa dữ liệu

Mã hóa dữ liệu là nền tảng của an ninh mạng và được ứng dụng rộng rãi trong nhiều lĩnh vực:

* **Giao tiếp qua mạng**: Các giao thức như HTTPS, SSL/TLS đều dựa trên mã hóa để bảo vệ thông tin truyền tải giữa máy chủ và trình duyệt.
* **Ngân hàng và thương mại điện tử**: Bảo vệ thông tin tài chính, giao dịch ngân hàng trực tuyến và các thanh toán điện tử.
* **Lưu trữ đám mây**: Các dịch vụ như Google Drive, Dropbox mã hóa dữ liệu để bảo vệ thông tin khách hàng.
* **Chữ ký số và xác thực người dùng**: Bảo đảm rằng thông điệp hoặc tài liệu chưa bị thay đổi và xác thực danh tính người gửi.

**2.2.5. Ứng dụng của hệ mã AES**

Ứng dụng của thuật toán mã hóa AES:

AES (Advanced Encryption Standard) là một thuật toán mã hóa đối xứng rất phổ biến được sử dụng để bảo vệ dữ liệu trong nhiều ứng dụng khác nhau. AES được coi là một trong những chuẩn mã hóa mạnh mẽ và an toàn nhất hiện nay.

- Bảo mật giao tiếp mạng

• VPN (Virtual Private Network): AES được sử dụng rộng rãi trong các giao thức VPN như IPsec và SSL/TLS để mã hóa dữ liệu truyền qua mạng. Điều này giúp bảo vệ thông tin nhạy cảm khi nó được truyền qua các mạng công cộng như internet.

Ví dụ: Khi bạn sử dụng một VPN như ExpressVPN, CyberGhost, hoặc NordVPN, AES mã hóa dữ liệu giữa thiết bị của bạn và máy chủ VPN để đảm bảo không ai có thể nghe lén hoặc tấn công vào kết nối của bạn.

• HTTPS: AES là một phần trong quá trình mã hóa các kết nối HTTPS (HyperText Transfer Protocol Secure). Nó đảm bảo rằng dữ liệu giữa trình duyệt và máy chủ web được mã hóa an toàn, bảo vệ người dùng khỏi các cuộc tấn công như nghe lén (eavesdropping) và tấn công trung gian (man-in-the-middle attacks).

Ví dụ: Khi bạn truy cập một trang web bảo mật (có giao thức HTTPS), AES được sử dụng để mã hóa dữ liệu truyền giữa máy tính của bạn và máy chủ web, bảo vệ thông tin cá nhân như tên người dùng, mật khẩu và dữ liệu thẻ tín dụng.

- Bảo mật lưu trữ dữ liệu:

• Mã hóa ổ cứng (Full Disk Encryption): Các phần mềm bảo mật như BitLocker (Windows) và FileVault (macOS) sử dụng AES để mã hóa toàn bộ ổ cứng, bảo vệ dữ liệu khỏi việc bị truy cập trái phép khi thiết bị bị mất hoặc bị đánh cắp.

Ví dụ: Windows sử dụng BitLocker để mã hóa toàn bộ ổ đĩa, trong khi macOS sử dụng FileVault. Cả hai đều sử dụng AES để đảm bảo rằng chỉ người dùng đã xác thực mới có thể truy cập dữ liệu.

• Mã hóa tập tin và thư mục: AES được sử dụng trong các công cụ mã hóa như VeraCrypt để mã hóa các tập tin hoặc thư mục quan trọng, bảo vệ dữ liệu khỏi những người không có quyền truy cập.

Ví dụ: Phần mềm như VeraCrypt hoặc 7-Zip sử dụng AES để mã hóa các tệp tin hoặc thư mục riêng biệt, bảo vệ dữ liệu khỏi việc bị xem hoặc sao chép trái phép.

- Thanh toán điện tử và giao dịch trực tuyến

• Thẻ tín dụng và thẻ ghi nợ: AES được sử dụng trong các giao dịch thanh toán trực tuyến để mã hóa thông tin thẻ tín dụng, bảo vệ dữ liệu tài chính khỏi bị đánh cắp hoặc giả mạo.

Ví dụ: Khi bạn thanh toán qua PayPal, Amazon hoặc các cổng thanh toán trực tuyến khác, AES mã hóa các thông tin như số thẻ tín dụng và địa chỉ giao hàng để bảo vệ dữ liệu khỏi bị xâm phạm.

• Mã hóa giao dịch ngân hàng: Các ngân hàng và tổ chức tài chính sử dụng AES để bảo mật các giao dịch tài chính trực tuyến, bảo vệ thông tin tài khoản và số dư của khách hàng.

Ví dụ: Khi bạn thực hiện chuyển khoản trực tuyến hoặc kiểm tra tài khoản qua dịch vụ ngân hàng trực tuyến, AES được sử dụng để mã hóa thông tin và bảo vệ các giao dịch.

- Bảo mật thông tin trong các thiết bị di động

• Mã hóa dữ liệu trên điện thoại di động: Hệ điều hành di động như Android và iOS sử dụng AES để mã hóa dữ liệu trên thiết bị, bảo vệ thông tin cá nhân như tin nhắn, hình ảnh, video và dữ liệu ứng dụng.

Ví dụ: Trên hệ điều hành Android và iOS, AES được sử dụng để mã hóa các tệp tin, tin nhắn và ứng dụng, giúp bảo vệ dữ liệu cá nhân của người dùng.

• Ứng dụng ngân hàng di động: Các ứng dụng ngân hàng di động sử dụng AES để mã hóa các giao dịch tài chính và thông tin nhạy cảm khác, đảm bảo rằng dữ liệu không bị xâm phạm.

Ví dụ: Các ứng dụng như ngân hàng Vietcombank, Techcombank, hoặc Mobile Banking của các ngân hàng khác sử dụng AES để bảo vệ dữ liệu tài chính của người dùng trong suốt quá trình giao dịch.

- Bảo mật email và tin nhắn

• Mã hóa email: Các dịch vụ email như ProtonMail sử dụng AES để mã hóa nội dung email, bảo vệ thông tin trao đổi giữa các bên gửi và nhận.

Ví dụ: Các dịch vụ email bảo mật như ProtonMail sử dụng AES để mã hóa nội dung email và các tệp đính kèm, đảm bảo rằng chỉ người nhận hợp lệ mới có thể giải mã và đọc thông tin.

- Xác thực và bảo vệ khóa

• Xác thực người dùng: AES được sử dụng trong các hệ thống xác thực người dùng, đặc biệt trong quá trình xác thực hai yếu tố (2FA) và xác thực qua mã OTP (One-Time Password).

• Mã hóa khóa và thông tin xác thực: Trong các hệ thống bảo mật, AES có thể được sử dụng để mã hóa khóa bảo mật và thông tin xác thực (authentication tokens), bảo vệ chúng khỏi bị đánh cắp khi lưu trữ.

- Bảo mật dữ liệu trong các dịch vụ đám mây

• Dịch vụ đám mây (Cloud Storage Services): Các nhà cung cấp dịch vụ đám mây như Google Drive, Dropbox, và Amazon S3 sử dụng AES để mã hóa dữ liệu của người dùng khi lưu trữ trên các máy chủ của họ. Điều này đảm bảo rằng dữ liệu không thể bị truy cập trái phép ngay cả khi máy chủ bị xâm nhập.

Ví dụ: Các dịch vụ lưu trữ đám mây như Google Drive, Dropbox, và Amazon S3 sử dụng AES để mã hóa dữ liệu của người dùng, bảo vệ tài liệu, hình ảnh và video khỏi việc bị lộ.

• Sao lưu và phục hồi dữ liệu: AES được sử dụng để mã hóa các bản sao lưu dữ liệu quan trọng trước khi chúng được lưu trữ hoặc đồng bộ trên đám mây.

Ví dụ: Dịch vụ sao lưu như Backblaze và Carbonite sử dụng AES để mã hóa dữ liệu sao lưu, bảo vệ các bản sao lưu khỏi việc bị truy cập trái phép.

- Mã hóa thông tin trong các thiết bị IoT

• Bảo mật giao tiếp giữa các thiết bị IoT: AES được sử dụng để mã hóa dữ liệu truyền giữa các thiết bị IoT và các máy chủ trung gian, bảo vệ các thông tin nhạy cảm như dữ liệu cảm biến, trạng thái thiết bị, v.v.

• Bảo mật cập nhật phần mềm: AES giúp bảo vệ các bản cập nhật phần mềm cho các thiết bị IoT khỏi việc bị can thiệp hoặc giả mạo trong quá trình truyền tải.

Ví dụ: Các thiết bị thông minh như camera an ninh, hệ thống nhà thông minh, hoặc thiết bị y tế đeo tay sử dụng AES để mã hóa dữ liệu truyền tải (như dữ liệu cảm biến) giữa các thiết bị và các hệ thống điều khiển, bảo vệ thông tin khỏi bị đánh cắp.

Như vậy, AES có vai trò quan trọng trong việc bảo vệ dữ liệu nhạy cảm trong nhiều lĩnh vực khác nhau, từ giao tiếp mạng, lưu trữ dữ liệu, thanh toán điện tử đến bảo mật trong các ứng dụng di động và thiết bị IoT. Nhờ vào khả năng mã hóa mạnh mẽ và tính hiệu quả, AES là một trong những thuật toán được ưa chuộng nhất để đảm bảo an toàn thông tin trong thế giới số ngày nay.