MẬT MÃ DES VÀ NHỮNG CẢI TIẾN

Cao Thị Thanh Xuân[1]

Tóm tắt: *DES (Data Encryption Standard) là một trong những thuật toán mã hóa đối xứng đầu tiên được sử dụng rộng rãi trong các ứng dụng bảo mật. DES sử dụng khóa đối xứng có độ dài 56 bit và mã hóa các khối dữ liệu có độ dài 64 bit. DES có ưu điểm về tốc độ xử lý nhanh và tính đối xứng, nhưng cũng có nhược điểm về độ dài khóa quá ngắn và khả năng bị tấn công bởi các kỹ thuật tấn công hiện đại. Nghiên cứu cho thấy rằng DES đã được sử dụng rộng rãi trong các ứng dụng bảo mật, tuy nhiên khả năng bị tấn công bởi các kỹ thuật tấn công hiện đại đã khiến cho thuật toán này trở nên lỗi thời và không còn đảm bảo tính bảo mật cao trong các ứng dụng hiện đại. Để cải thiện tính bảo mật của DES, các thuật toán mã hóa khác như Triple DES, Blowfish và AES đã được phát triển. Trong đó, AES là một trong những thuật toán mã hóa đối xứng đang được sử dụng rộng rãi nhất hiện nay.*

Từ khóa: *Mật mã DES, Triple Des, Blowfish, AES*

1. MỞ ĐẦU

Data Encryption Standard (DES) là một trong những thuật toán mã hóa đầu tiên được sử dụng rộng rãi trên thế giới. Thuật toán này được phát triển bởi Viện Tiêu chuẩn và Công nghệ Hoa Kỳ (National Institute of Standards and Technology - NIST) và được chính thức công bố vào năm 1977 [4,8,12]. DES ban đầu được phát triển để bảo vệ thông tin quân sự của Hoa Kỳ trong thời kỳ Chiến tranh Lạnh. Tuy nhiên, vì sự an toàn và tính ổn định của thuật toán, nó đã được sử dụng rộng rãi trong các ứng dụng bảo mật thông tin của doanh nghiệp và tổ chức trên toàn thế giới. DES sử dụng phương pháp mã hóa khối với khối dữ liệu đầu vào có kích thước 64 bit hoặc hơn. Thuật toán sử dụng một khối chuyển vị và một số phương pháp khác nhau để mã hóa dữ liệu và giải mã. Tuy mạnh mẽ và có khá nhiều ưu điểm, DES cũng đã bị các cuộc tấn công mã hóa thành công vào cuối những năm 1990. Vì vậy, NIST đã quyết định thay thế DES bằng thuật toán mã hóa mới hơn, Advanced Encryption Standard (AES) vào năm 2001. Tuy nhiên, DES vẫn được sử dụng trong một số trường hợp, nhưng nó đã được cải tiến để giảm thiểu những lỗ hổng bảo mật của nó.

2. NỘI DUNG NGHIÊN CỨU

2.1. Mật mã DES

a) Cấu trúc của thuật toán DES được thiết kế để mã hóa một khối dữ liệu đầu vào có kích thước 64 bit, bao gồm 56 bit được sử dụng cho khóa và 8 bit được sử dụng để kiểm soát và kiểm tra [1,6]. Cấu trúc chính của DES gồm các phép biến đổi khối dữ liệu (data

[1] Trường Đại học Kinh tế Kỹ thuật Công Nghiệp

blocks) theo các vòng lặp được lặp lại 16 lần, mỗi lần với một khóa con (subkey) được tạo ra từ khóa chính ban đầu. Các bước chính của DES bao gồm:

Bước 1: Chia khóa 64-bit thành hai nửa, mỗi nửa có 28 bit và dịch chuyển chúng sang trái hoặc phải để tạo ra 16 khóa con khác nhau.

Bước 2: Khối dữ liệu 64-bit được chuyển qua một hộp chuyển vị (initial permutation), nơi các bit trong khối được sắp xếp lại theo một thứ tự cụ thể.

Bước 3: Khối dữ liệu đã được chuyển vị sau đó được chia thành hai nửa có độ dài 32 bit. Mỗi nửa sau đó được thực hiện các phép biến đổi bên trong 16 vòng lặp. Các phép biến đổi này bao gồm một phép hoán vị, một phép mở rộng khối (expansion), một phép XOR với khóa con, một phép thay thế (substitution), và một phép hoán vị cuối cùng.

Bước 4: Cuối cùng, hai nửa khối đã được biến đổi được trao đổi và kết hợp thành một khối mới. Khối này được chuyển qua một hộp chuyển vị cuối cùng (final permutation) để tạo ra khối dữ liệu được mã hóa. Với cấu trúc này, DES có thể mã hóa và giải mã các khối dữ liệu 64 bit với độ an toàn tương đối.

Ví dụ: Để minh họa cách DES hoạt động, ta có thể sử dụng ví dụ sau:

Giả sử Alice muốn gửi một thông điệp bí mật đến Bob. Để bảo vệ thông điệp, Alice sử dụng DES để mã hóa nó trước khi gửi đi. Chúng ta chia thành các bước như sau:

Bước 1: Chuẩn bị khóa

Để sử dụng DES, Alice và Bob đồng ý trước một khóa bí mật. Khóa này sẽ được sử dụng để mã hóa và giải mã thông điệp. Ví dụ, Alice và Bob có thể sử dụng khóa "mysecretkey" để mã hóa thông điệp.

Bước 2: Mã hóa thông điệp

Sau khi chuẩn bị khóa, Alice sử dụng DES để mã hóa thông điệp của mình. Ví dụ, nếu Alice muốn gửi thông điệp "Hello, Bob!", cô ấy sẽ sử dụng khóa "mysecretkey" và DES để mã hóa thông điệp này. Kết quả sẽ là một chuỗi ký tự không đọc được.

Bước 3: Gửi thông điệp

Sau khi đã mã hóa thông điệp, Alice gửi nó cho Bob thông qua kênh truyền an toàn như email hoặc tin nhắn.

Bước 4: Giải mã thông điệp

Khi Bob nhận được thông điệp, anh ấy sử dụng khóa "mysecretkey" và DES để giải mã thông điệp. Khi đã giải mã, thông điệp sẽ trở lại dạng ban đầu "Hello, Bob!".

Như vậy, thông điệp đã được bảo vệ và chỉ có thể được giải mã bởi người nhận đúng khóa bí mật.

b) Một số ưu điểm của DES:

- Tính bảo mật cao: DES sử dụng khối dữ liệu 64 bit và khóa 56 bit, giúp tăng tính bảo mật cao đối với các cuộc tấn công từ các trường trung gian. Ví dụ: Một ngân hàng sử

dụng DES để mã hóa thông tin khách hàng, giúp ngăn chặn những cuộc tấn công từ phía hacker.

- Tính linh hoạt: DES có thể được sử dụng với các chế độ mã hóa khác nhau, bao gồm chế độ mã hóa điện tử mã hóa (ECB), chế độ mã hóa dãy (CBC) và chế độ mã hóa đối xứng (OFB). Điều này giúp cho DES trở thành một thuật toán linh hoạt và có thể sử dụng được với nhiều mục đích khác nhau. Ví dụ: DES có thể được sử dụng để mã hóa thông tin trong các ứng dụng máy tính cá nhân, các mạng LAN và WAN, các giao dịch tài chính, và các ứng dụng di động.

- Hiệu suất tốt: DES có tốc độ mã hóa và giải mã nhanh, vì vậy nó thường được sử dụng trong các hệ thống yêu cầu hiệu suất cao. Ví dụ: DES được sử dụng để mã hóa thông tin trong các ứng dụng lưu trữ đám mây và trong các hệ thống thương mại điện tử để đảm bảo tốc độ truyền dữ liệu cao.

- Dễ dàng triển khai: DES có cấu trúc đơn giản, giúp cho việc triển khai và sử dụng nó dễ dàng hơn các thuật toán mã hóa phức tạp khác. Ví dụ: DES được sử dụng trong các hệ thống tài liệu và hệ thống chia sẻ tài liệu để đảm bảo tính bảo mật cao và dễ dàng triển khai. Tính sử dụng rộng rãi của DES cũng là một ưu điểm nổi bật của nó. DES là một trong những thuật toán mã hóa phổ biến nhất và được sử dụng trong rất nhiều ngành gồm tài chính, y tế, công nghệ thông tin, ngân hàng, và nhiều ngành công nghiệp khác.

c) Một số nhược điểm của DES

- Khóa quá ngắn: DES sử dụng khóa 56 bit, đây là một độ dài khóa khá ngắn, và trong những năm gần đây, các cuộc tấn công brute force và từ điển đã trở nên hiệu quả hơn. Vì vậy, khóa của DES dễ dàng bị tấn công.

- Thiết kế đã cũ: Thuật toán DES được thiết kế và công bố vào năm 1977, và trong nhiều năm qua, đã có nhiều cuộc tấn công khác nhau đã được tìm thấy. Vì vậy, nó không còn được coi là an toàn và được khuyến cáo không nên sử dụng nữa.

- Không có tính toán định tuyến: DES không có tính toán định tuyến, điều này có nghĩa là các bit đầu vào và đầu ra của mỗi khối dữ liệu được xác định cùng một cách. Điều này dễ dàng cho kẻ tấn công quan sát và tiên đoán các khối dữ liệu mã hóa.

- Dễ dàng bị tấn công bằng cách thay đổi dữ liệu: DES có thể bị tấn công bằng cách thay đổi dữ liệu đầu vào một cách nghiêm trọng, điều này dẫn đến các cuộc tấn công được gọi là "tấn công plaintext đã biết" và "tấn công khối được chọn".

- Không phù hợp với các ứng dụng đòi hỏi mật mã cường độ cao: Trong các ứng dụng đòi hỏi mật mã cường độ cao, DES không còn được sử dụng nữa, thay vào đó, các thuật toán mã hóa khác như AES (Advanced Encryption Standard) đã được sử dụng thay thế.

2.2. Một số cải tiến của mã DES

Sau khi nhận ra những hạn chế của DES, nhiều cải tiến đã được đưa ra để nâng cao tính an toàn và hiệu quả của thuật toán. Dưới đây là một số cải tiến của DES:

a,Triple DES (3DES):

Triple DES [7] là một phiên bản nâng cao của DES, sử dụng ba vòng lặp mã hóa để tăng độ dài khóa lên 168 bit, từ đó tăng cường tính bảo mật. Triple DES được sử dụng trong các ứng dụng nhiều lớp, ví dụ như trong các hệ thống thanh toán điện tử, mạng máy tính và các hệ thống quản lý danh tính. Tuy nhiên, 3DES có tốc độ chậm hơn DES gốc.

Với Triple DES, mỗi khối dữ liệu được mã hóa ba lần, sử dụng hai khóa DES khác nhau. Một khóa DES được sử dụng để mã hóa dữ liệu, còn khóa DES khác được sử dụng để giải mã dữ liệu. Triple DES được coi là một trong những thuật toán mã hóa phổ biến nhất hiện nay.

Ưu điểm của Triple DES bao gồm:

Tính bảo mật cao hơn: Triple DES có độ dài khóa lên đến 168 bit, làm tăng đáng kể khả năng bảo mật so với DES.

Tương thích ngược với DES: Triple DES có thể tương thích với các hệ thống sử dụng DES.

Dễ triển khai: Triple DES được triển khai rộng rãi trên các nền tảng phần cứng và phần mềm khác nhau.

Tuy nhiên, Triple DES cũng có nhược điểm, bao gồm tốc độ xử lý chậm hơn so với những thuật toán mã hóa đối xứng hiện đại hơn, và khó khăn trong việc triển khai trên các hệ thống nhỏ.

b) DESX:

DESX kết hợp việc mã hóa và băm dữ liệu để tăng cường tính bảo mật. DESX sử dụng một khóa DES để mã hóa dữ liệu và một hàm băm để làm cho dữ liệu trở nên khó đoán [7]. DESX được sử dụng trong các ứng dụng bảo mật cho các hệ thống điện toán đám mây và lưu trữ dữ liệu trực tuyến. Ví dụ, Dropbox đã sử dụng DESX trong quá trình mã hóa và bảo vệ các tập tin được lưu trữ trên hệ thống của họ. Các thuật toán mã hóa này đã được sử dụng rộng rãi và có thể đáp ứng nhu cầu bảo mật của các ứng dụng khác nhau trong nhiều lĩnh vực khác nhau. DESX là một thuật toán mã hóa đối xứng, nó được phát triển từ DES (Data Encryption Standard) và sử dụng hai lần DES để mã hóa dữ liệu. DESX được sử dụng để cải thiện tính bảo mật của DES bằng cách thêm một bước mã hóa khóa, giúp làm giảm khả năng tấn công bằng brute force.

Các đặc điểm của DESX bao gồm:

Khóa dài hơn: DESX sử dụng khóa dài hơn 56 bit của DES, thông thường là 120 bit hoặc 128 bit, giúp tăng tính bảo mật.

Cấu trúc đơn giản: DESX có cấu trúc đơn giản, do đó việc triển khai và sử dụng nó đối với các ứng dụng bảo mật khác nhau rất dễ dàng.

Khả năng chống lại các cuộc tấn công: DESX có khả năng chống lại các cuộc tấn công brute force và tấn công theo mật khẩu.

Tính linh hoạt: DESX có thể được sử dụng trong nhiều ứng dụng bảo mật, bao gồm cả các ứng dụng bảo mật mạng và lưu trữ dữ liệu trực tuyến.

Tuy nhiên, nhược điểm của DESX là nó không nhanh bằng những thuật toán mã hóa hiện đại hơn, và khó khăn để mở rộng đến các khóa dài hơn. Ngoài ra, nếu các tấn công khác nhau được sử dụng, DESX cũng có thể trở nên dễ bị tấn công.

Mặc dù DESX không còn được sử dụng rộng rãi như các thuật toán mã hóa hiện đại hơn, nhưng nó vẫn được sử dụng trong một số ứng dụng, bao gồm cả Dropbox và Microsoft Windows.

c) Blowfish:

Blowfish là một thuật toán mã hóa đối xứng nhanh và an toàn hơn DES [5]. Blowfish sử dụng khóa dài hơn, từ 32 đến 448 bit, và có tốc độ xử lý nhanh hơn DES. Blowfish được sử dụng rộng rãi trong các ứng dụng web và phần mềm. Ví dụ, Blowfish được sử dụng trong mã hóa các thông tin cá nhân trên các trang web đăng ký trực tuyến. Blowfish là một thuật toán mã hóa đối xứng được tạo ra bởi Bruce Schneier vào năm 1993. Blowfish sử dụng khóa có độ dài lên đến 448 bit, vượt xa độ dài khóa của DES. Blowfish được sử dụng rộng rãi trong các ứng dụng bảo mật, bao gồm cả phần mềm mã hóa email và ứng dụng web.

Các đặc điểm của Blowfish bao gồm:

Độ dài khóa lớn: Blowfish sử dụng khóa có độ dài lên đến 448 bit, cung cấp độ bảo mật cao.

Tốc độ xử lý nhanh: Blowfish được thiết kế để xử lý nhanh, thường nhanh hơn các thuật toán mã hóa khác như DES.

Tính linh hoạt: Blowfish có thể được triển khai trên nhiều nền tảng phần cứng và phần mềm khác nhau.

Nhược điểm của Blowfish là nó không được sử dụng trong các tiêu chuẩn bảo mật quốc tế và có thể bị tấn công bằng một số kỹ thuật tấn công khác nhau. Triple DES (3DES) là một thuật toán mã hóa đối xứng phát triển từ DES, sử dụng ba vòng DES để tăng cường tính bảo mật.

d) AES (Advanced Encryption Standard):

AES là một thuật toán mã hóa đối xứng được sử dụng rộng rãi và được coi là một trong những thuật toán mã hóa mạnh nhất hiện nay [11]. AES sử dụng khóa dài 128, 192 hoặc 256 bit và có tốc độ xử lý nhanh hơn DES. AES được sử dụng trong nhiều ứng dụng bảo mật như mã hóa email, bảo mật dữ liệu đám mây, bảo mật ứng dụng di động, và cả trong lĩnh vực tài chính như giao dịch ngân hàng trực tuyến.

e) Serpent:

Serpent là một thuật toán mã hóa đối xứng mạnh mẽ, sử dụng khóa dài 128, 192 hoặc 256 bit và có tốc độ xử lý tương đương với AES [1,9]. Serpent được thiết kế để chống lại

các cuộc tấn công mã hóa khác nhau, bao gồm cả tấn công bằng lực brute force. Serpent được sử dụng trong nhiều hệ thống bảo mật mạng, bao gồm các hệ thống chuyển mạch, tường lửa, và phân tích mạng. Serpent là một thuật toán mã hóa đối xứng được đề xuất bởi Ross Anderson, Eli Biham và Lars Knudsen vào năm 1998. Serpent được thiết kế để đạt được tính bảo mật cao hơn so với DES và AES. Thuật toán này sử dụng khối dữ liệu 128-bit và có khóa có độ dài 128-bit, 192-bit hoặc 256-bit. Serpent được chọn để làm phần của các tiêu chuẩn bảo mật của Anh và được sử dụng trong nhiều ứng dụng bảo mật mạng. Nó được coi là một trong những thuật toán mã hóa đối xứng an toàn nhất hiện nay.

Một số đặc điểm của Serpent bao gồm:

Cấu trúc rõ ràng và đơn giản: Serpent có cấu trúc rõ ràng và đơn giản, dễ dàng để hiểu và kiểm tra tính đúng đắn của nó.

Chi phí tính toán cao: Serpent yêu cầu nhiều chi phí tính toán hơn so với DES và AES, điều này làm cho nó chậm hơn trong một số ứng dụng.

Khả năng chống lại các cuộc tấn công khác nhau: Serpent có khả năng chống lại các cuộc tấn công như tấn công phân tích đường đi khối, tấn công ngược, tấn công phân tích khóa,...

Serpent là một lựa chọn tốt cho các ứng dụng yêu cầu tính bảo mật cao và an toàn. Tuy nhiên, do tính chậm và chi phí tính toán cao của nó, Serpent không phù hợp cho các ứng dụng yêu cầu tốc độ cao như ứng dụng trò chơi hoặc các ứng dụng nhanh nhạy khác. Những cải tiến này đã giúp cải thiện tính an toàn và hiệu quả của thuật toán mã hóa đối xứng và thay thế cho DES trong nhiều trường hợp sử dụng.

3. KẾT LUẬN

Tóm lại, bài báo đã đưa ra cấu trúc của DES (Data Encryption Standard), đồng thời cung cấp ưu và nhược điểm của DES. Trong bài báo này, chúng tôi cũng giới thiệu một số cải tiến cho DES như Triple DES, Blowfish và AES để khắc phục các nhược điểm của DES. Trong những nghiên cứu tiếp theo, chúng tôi có thể nghiên cứu sâu và chi tiết hơn về các thuật toán và những ứng dụng bảo mật quan trọng khác phát triển từ Triple DES, Blowfish và AES.

TÀI LIỆU THAM KHẢO

1. R. Anderson, E. Biham, L. Knudsen, *Serpent: A Proposal for the Advanced Encryption Standard,*1998.
2. M. Bellare, A. Desai, E. Petrank, *Security of Symmetric Encryption against Mass Surveillance*, CRYPTO 2014, Part I, LNCS 8616, pp.31-50, 2014.
3. E. Biham , A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

4. R.E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, 1983.
5. S. Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd ed., John Wiley & Sons, 1996.
6. P. Christof, J. Pelzl, B. Preneel, *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, 2010.
7. P. Garrett, *Triple-DES and DES-X. Lecture notes*, University of Minnesota, 2002.
8. J.L. Massey, *Block Ciphers and Cryptanalysis*, Springer-Verlag, 1994.
9. F. Pub, *Data Encryption Standard (DES),* National Institute of Standards and Technology (NIST), 1999.
10. V. Rijmen, J. Daemen, *AES Proposal: Rijndael*, NIST, 1998.
11. S. Simon, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Fourth Estate, 2000.
12. B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, 1995.
13. S. William*, Cryptography and Network Security: Principles and Practice*, 7th ed., Pearson Education, 2017.

DES CODE AND IMPROVEMENTS

Cao Thi Thanh Xuan

Abstract: *DES (Data Encryption Standard) is one of the first widely used symmetric-key encryption algorithms in cybersecurity applications. DES uses a 56-bit symmetric key to encrypt 64-bit blocks of data. DES has the advantages of fast processing speed and symmetry, but also the disadvantages of too short key length and the possibility of being attacked by modern attack techniques. Research shows that DES has been widely used in security applications, but the ability to be attacked by modern attack techniques has made this algorithm obsolete and no longer secure. High security in modern applications. To improve the security of DES, other encryption algorithms such as Triple DES, Blowfish and AES have been developed. Among them, AES is one of the most widely used symmetric encryption algorithms today.*

Keywords: *DES, Triple Des, Blowfish, AES*

(Ngày Tòa soạn nhận được bài: 02-10-2023; ngày phản biện đánh giá: 24-10-2023; ngày chấp nhận đăng: 08-11-2023)