TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI

**KHOA CÔNG NGHỆ THÔNG TIN**

------🙙🕮🙛-------



**BÁO CÁO THỰC NGHIỆM**

Học phần: An ninh mạng

**Chủ đề**: **Chuẩn DES và ứng dụng trong mã hóa dữ liệu (Sử dụng ngôn ngữ C#,Java)**

Giáo viên hướng dẫn: TS. Phạm Văn Hiệp

Mã lớp học phần: 2024IT6070001

Nhóm sinh viên thực hiện: Nhóm 4

1. Trần Trọng Hiếu Mã SV: 2022602004

2. Lê Đức Chương Mã SV: 2022602955

3. Nguyễn Viết Minh Hoàng Mã SV: 2022600282

4. Trần Xuân Hoàn Mã SV: 2022601562

5. Lê Văn Giang Mã SV: 2021606816

Hà Nội - Năm 2024

**MỤC LỤC**

Danh mục các từ viết tắt…

Danh mục hình ảnh…

Danh mục bảng biểu…

…Các chương, các đề mục trong báo cáo…

# **LỜI NÓI ĐẦU**

Trong thời đại công nghệ số, dữ liệu không chỉ đơn thuần là thông tin, mà còn là tài sản vô giá của cá nhân, tổ chức và quốc gia. Chính vì vậy, việc bảo vệ dữ liệu trước các nguy cơ như truy cập trái phép, đánh cắp, và giả mạo ngày càng trở nên quan trọng. Một trong những giải pháp hữu hiệu và phổ biến nhất để đảm bảo tính bảo mật cho dữ liệu chính là áp dụng các thuật toán mã hóa.

Thuật toán mã hóa DES (Data Encryption Standard), mặc dù đã xuất hiện từ lâu, vẫn giữ vai trò quan trọng trong lịch sử phát triển các công nghệ mã hóa hiện đại. DES không chỉ là nền tảng cho nhiều thuật toán mã hóa phức tạp hơn mà còn là công cụ học thuật quan trọng để sinh viên nghiên cứu về nguyên lý hoạt động của các hệ thống bảo mật thông tin.

Nhận thức được tầm quan trọng của chủ đề này, nhóm chúng em đã lựa chọn thực hiện bài tập lớn môn An ninh mạng với chủ đề: “Chuẩn DES và ứng dụng trong mã hóa dữ liệu”. Mục tiêu của bài tập lớn không chỉ dừng lại ở việc tìm hiểu lý thuyết mà còn tập trung vào triển khai thực tiễn thuật toán DES bằng hai ngôn ngữ lập trình phổ biến là C# và Java, nhằm xây dựng nền tảng kiến thức vững chắc cũng như rèn luyện kỹ năng lập trình.

Bài báo cáo là kết quả của quá trình nghiên cứu, phân tích tài liệu, và triển khai thực tiễn trong suốt thời gian thực hiện bài tập lớn. Trong quá trình thực hiện, chúng em đã cố gắng học hỏi, nỗ lực hoàn thành bài tập với sự nghiêm túc cao nhất. Tuy nhiên, do hạn chế về thời gian và kinh nghiệm, chắc chắn bài làm sẽ không tránh khỏi những thiếu sót.

Chúng em xin chân thành cảm ơn sự hướng dẫn tận tình của giáo viên bộ môn An ninh mạng, và sự hỗ trợ của các tài liệu tham khảo trong quá trình nghiên cứu.

Hy vọng rằng bài báo cáo này không chỉ đáp ứng yêu cầu của môn học mà còn góp phần nâng cao kiến thức của chúng em về lĩnh vực an ninh mạng, từ đó ứng dụng hiệu quả vào công việc thực tế trong tương lai.

# **CHƯƠNG 1: TỔNG QUAN**

## **1.1. Tổng quan về An ninh mạng**

### **1.1.1. Khái niệm về an ninh mạng**

An ninh mạng, hay còn gọi là bảo mật mạng (Cybersecurity), là tập hợp các phương pháp, công nghệ và quy trình được thiết kế nhằm bảo vệ hệ thống mạng, thiết bị, và dữ liệu khỏi các cuộc tấn công, truy cập trái phép, hoặc phá hoại. Trong thời đại công nghệ 4.0, khi thông tin được số hóa và lưu trữ trực tuyến, an ninh mạng đóng vai trò quan trọng trong việc đảm bảo sự an toàn và ổn định của các tổ chức, doanh nghiệp, cũng như cá nhân.

An ninh mạng không chỉ bảo vệ dữ liệu khỏi các mối đe dọa mà còn đảm bảo các nguyên tắc cơ bản:

* Tính bí mật (Confidentiality): Chỉ những đối tượng được cấp quyền mới có thể truy cập thông tin.
* Tính toàn vẹn (Integrity): Dữ liệu không bị sửa đổi hoặc phá hoại bởi những tác nhân trái phép.
* Tính sẵn sàng (Availability): Hệ thống và dữ liệu luôn sẵn sàng để truy cập khi cần thiết.

### **1.1.2. Vai trò của an ninh mạng**

An ninh mạng có vai trò thiết yếu trong tất cả các lĩnh vực, đặc biệt là trong:

* Chính phủ và quốc phòng: Bảo vệ các thông tin mật, ngăn chặn các cuộc tấn công mạng có mục tiêu chính trị.
* Doanh nghiệp: Đảm bảo thông tin khách hàng, dữ liệu nội bộ không bị rò rỉ, giữ vững uy tín và tính cạnh tranh.
* Người dùng cá nhân: Bảo vệ thông tin cá nhân, tài khoản ngân hàng, và tránh các hành vi lừa đảo trực tuyến.

Trong bối cảnh các cuộc tấn công mạng ngày càng gia tăng về số lượng và mức độ tinh vi, an ninh mạng không chỉ là vấn đề kỹ thuật mà còn là yếu tố sống còn để phát triển kinh tế và bảo vệ quyền lợi người dùng.

### **1.1.3. Các mối đe dọa an ninh mạng phổ biến**

Hiện nay, có nhiều loại mối đe dọa an ninh mạng, từ các cuộc tấn công nhỏ lẻ đến các chiến dịch tấn công quy mô lớn:

* Malware (Phần mềm độc hại): Bao gồm virus, ransomware, spyware, và trojan, thường được sử dụng để chiếm quyền kiểm soát hoặc làm hỏng hệ thống.
* Phishing (Tấn công lừa đảo): Lợi dụng sự tin tưởng của người dùng để thu thập thông tin nhạy cảm như tài khoản ngân hàng hoặc mật khẩu.
* DDoS (Tấn công từ chối dịch vụ): Làm gián đoạn hoạt động của hệ thống bằng cách gửi lượng lớn yêu cầu khiến hệ thống bị quá tải.
* APT (Mối đe dọa kéo dài và tinh vi): Các cuộc tấn công nhắm đến mục tiêu cụ thể, thường nhằm đánh cắp dữ liệu quan trọng hoặc phá hoại hệ thống.
* Tấn công vào chuỗi cung ứng: Nhắm vào các nhà cung cấp hoặc đối tác của mục tiêu để xâm nhập hệ thống.

### **1.1.4. Các phương pháp bảo vệ an ninh mạng**

Để đối phó với các mối đe dọa trên, nhiều giải pháp và công nghệ đã được triển khai:

* Tường lửa (Firewall): Ngăn chặn lưu lượng truy cập trái phép vào hệ thống mạng.
* Mã hóa dữ liệu: Sử dụng các thuật toán như DES, AES, RSA để đảm bảo thông tin được bảo vệ trong quá trình truyền tải.
* Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS): Giám sát hoạt động mạng để phát hiện và ngăn chặn các mối đe dọa.
* Xác thực hai yếu tố (2FA): Tăng cường bảo mật bằng cách yêu cầu người dùng xác minh danh tính qua nhiều bước.
* Cập nhật hệ thống thường xuyên: Vá lỗi và cập nhật phiên bản mới để loại bỏ lỗ hổng bảo mật.

### **1.1.5. Xu hướng và thách thức trong an ninh mạng**

Sự phát triển của công nghệ kéo theo nhiều thách thức mới trong lĩnh vực an ninh mạng, bao gồm:

* Trí tuệ nhân tạo (AI): Cả hai bên (tấn công và phòng thủ) đều đang sử dụng AI để tăng cường hiệu quả.
* Internet of Things (IoT): Số lượng thiết bị kết nối ngày càng nhiều khiến phạm vi bị tấn công ngày càng rộng.
* Tấn công không gian mạng (Cyberwarfare): Các quốc gia sử dụng chiến tranh mạng như một công cụ chiến lược.
* Thiếu nhân lực an ninh mạng: Sự thiếu hụt chuyên gia khiến việc bảo vệ mạng trở nên khó khăn hơn.

### **1.1.6. Kết luận**

An ninh mạng là một lĩnh vực không ngừng phát triển và đòi hỏi sự đầu tư lớn về cả nguồn lực con người lẫn công nghệ. Việc nâng cao nhận thức và trang bị kiến thức về an ninh mạng không chỉ giúp bảo vệ hệ thống khỏi các mối đe dọa mà còn đảm bảo sự phát triển bền vững trong môi trường số hóa ngày nay.

## **1.2. Tổng quan về thuật toán DES**

### **1.2.1. Giới thiệu chung về thuật toán DES**

DES (Data Encryption Standard) là chuẩn mã hóa dữ liệu đầu tiên trên thế giới, do Cơ quan an ninh Quốc gia Hoa Kỳ (NSA) đề xuất trên cơ sở cải tiến thuật toán Lucifer do hãng IBM công bố năm 1964. DES đã được sử dụng rộng rãi ở Hoa Kỳ và nhiều quốc gia khác trong các thập kỷ 70, 80, 90 cho đến khi được thay thế bởi Tiêu chuẩn mã hóa dữ liệu tiên tiến AES (Advanced Encryption Standard) vào năm 2002.

A diagram of a computer flowchart

Description automatically generated

*Hình 1:*

Đầu vào của DES là khối 64 bit, đầu ra cũng là khối 64 bit. Khóa mã hóa có độ dài 56 bit, nhưng thực chất ban đầu là 64 bit, được lấy đi các bit ở vị trí chia hết cho 8 dùng để kiểm tra tính chẵn lẻ.

### **1.2.2. Thuật toán**

DES là thuật toán mã hóa theo khối, nó xử lý từng khối thông tin của bản rõ có độ dài xác định là 64 bit. Trước khi đi vào 16 chu trình chính, khối dữ liệu cần bảo mật sẽ được tách ra thành từng khối 64 bit, và từng khối 64 bit này sẽ lần lượt được đưa vào 16 vòng mã hóa DES để thực hiện. **Input:** Bản rõ M = m1m2…m64 là một khối 64 bit, khóa 64 bit K = k1k2…k64. **Output:** Bản mã 64 bit C = c1c2… c64

+ Bước 1: Sinh khóa con: Sử dụng thuật toán sinh khóa con từ khóa K ta sẽ được 16 khóa con K1, K2, … K16

+ Bước 2: Sử dụng phép hoán vị khởi đầu IP (Initial Permutation) để hoán vị các bit của M, kết quả nhận được chia thành 2 nửa là L0 = m63m62…m32, R0 = m31m30…m0.

+ Bước 3: Với i chạy từ i = 1 đến 16 thực hiện: Tính các Li và Ri theo công thức: Li = Ri-1 Ri = Li-1 XOR f(Ri-1, Ki) trong đó f(Ri-1, Ki) = R(S(E(Ri-1) XOR Ki)). Việc tính f(Ri-1, Ki) sẽ được trình bày chi tiết ở phần sau.

+ Bước 4: Đổi vị trí khối L16, R16 ta được khối R16L16 = b1b2…b64.

+ Bước 5: Sử dụng phép hoán vị kết thúc FP(Final Permutation – nghịch đảo với hoán vị khởi đầu IP) ta thu được bản mã cần tìm : C = IP-1(b1b2…b64)

A diagram of a computer

Description automatically generated

*Hình 2:*

### **1.2.3. Quá trình sinh khóa con**

16 vòng lặp của DES chạy cùng thuật toán như nhau nhưng với 16 khóa con khác nhau. Các khóa con đều được sinh ra từ khóa chính của DES bằng thuật toán sinh khóa con.

A diagram of a computer flowchart

Description automatically generated

*Hình 3:*

Khóa ban đầu là 1 xâu có độ dài 64 bit, bit thứ 8 của mỗi byte sẽ được lấy ra để kiểm tra phát hiện lỗi, tạo ra chuỗi 56 bit. Sau khi bỏ các bit kiểm tra ta sẽ hoán vị chuỗi 56 bit này. Hai bước trên được thực hiện thông qua hoán vị ma trận PC-1 (Permuted choice 1).

A number grid with black numbers

Description automatically generated

*Hình 4:*

Tiếp theo ta kết quả sau khi PC-1 thành 2 phần : C0 : 28 bit đầu. D0 : 28 bit cuối. Mỗi phần sẽ được xử lý 1 cách độc lập. Ci = LSi(Ci-1) Di = LSi(Ci-1) với 1 ≤ i ≤ 16. LSi là biểu diễn phép dịch bit vòng (cyclic shift) sang trái 1 hoặc 2 vị trí tùy thuộc vào i.

*Bảng 1.2.*

| **Vòng lặp** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Số lần dịch trái | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

Cuối cùng sử dụng hoán vị cố định PC-2 (Permuted choice 2) để hoán vị chuỗi CiDi 56 bit tạo thành khóa Ki với 48 bit.

A number grid with numbers

Description automatically generated

*Hình 5:*

# **TÀI LIỆU THAM KHẢO**

(Sắp xếp theo ngôn ngữ: Việt, Anh, Pháp, Đức, Nga…)

[1]. Nguyễn Xuân Dũng, Bảo mật thông tin – Mô Hình và ứng dụng, NXB thống kê, 2009.

[2]. Bùi Doãn Khanh, Nguyễn Đình Thúc, Mã hóa thông tin – Lý thuyết và ứng dụng, NXB Lao động xã hội, 2011.

[3]. William Stallings**,** Cryptography and Network Security Principles and Practices**,** Fourth Edition, Prentice Hall, 2005.

…

[n]. <http://www.hhs.com>

(thời gian truy cập: 15h00, ngày 27/10/2024)

**Phụ lục 1: Chương trình Java**

**Phụ lục 2: Chương trình C#**