***Mục lục:***

***I/Tổng quan về Cryptography***

*1/ Cryptography là gì?*

*2/ Mục tiêu của Cryptography*

*3/Phân loại mã hóa*

***II/Một số kiến thức cơ bản và các thuật toán mã hóa tiêu biểu***

*1/ Một số kiến thức cơ bản*

*2/ Một số thuật toán mã hóa tiêu biểu*

***Mở đầu:***

*Trong thời đại công nghệ số phát triển mạnh mẽ như hiện nay, thông tin trở thành một tài sản quý giá và cần được bảo vệ một cách nghiêm ngặt. Hàng loạt các giao dịch tài chính, dữ liệu cá nhân, và thông tin nhạy cảm được truyền tải qua các hệ thống mạng mỗi ngày, kéo theo đó là nguy cơ bị đánh cắp, giả mạo hoặc phá hoại. Trước thực trạng đó, Cryptography (mật mã học) đã và đang đóng vai trò quan trọng trong việc đảm bảo tính bảo mật, toàn vẹn và xác thực của thông tin.*

Từ những phương pháp mã hóa đơn giản thời cổ đại như Caesar cipher đến các thuật toán mã hóa hiện đại phức tạp như SHA-3 hay RSA, Cryptography không ngừng phát triển để thích ứng với các thách thức an ninh mạng ngày càng tinh vi. Với mục tiêu tìm hiểu nền tảng lý thuyết của mật mã học và khám phá một số thuật toán mã hóa tiêu biểu, tiểu luận này sẽ cung cấp cái nhìn tổng quan về lĩnh vực này, đồng thời giới thiệu 1 số thuật toán mã hóa nổi tiếng

***I. Tổng quan về Cryptography (mật mã học)***

***1. Cryptography là gì?***

C**ryptography** (mật mã học) là lĩnh vực nghiên cứu các kỹ thuật bảo mật thông tin, đảm bảo rằng dữ liệu chỉ có thể được đọc và hiểu bởi những người được phép. Đây là một nhánh quan trọng của an toàn thông tin và an ninh mạng.

### **Một cách đơn giản:**

Cryptography = Nghệ thuật **mã hóa** và **giải mã** thông tin.

**Mật mã học** là lĩnh vực liên quan đến các kỹ thuật ngôn ngữ và toán học để đảm bảo [an toàn thông tin](https://vi.wikipedia.org/wiki/An_toàn_thông_tin), cụ thể là trong [thông tin liên lạc](https://vi.wikipedia.org/wiki/Thông_tin_liên_lạc). Trong lịch sử, mật mã học gắn liền với quá trình [*mã hóa*](https://vi.wikipedia.org/wiki/Mã_hóa) (encryption) và giải mã (decryption).

***### Chèn hình 1###***

Một số thuật ngữ quan trọng:

* Decryption (mã hóa): là quá trình chuyển đổi thông tin (dữ liệu gốc) thành một dạng khó hiểu (dữ liệu mã hóa) để ngăn người không có quyền truy cập đọc được nội dung.
* Encryption (giải mã): Giải mã là quá trình biến dữ liệu đã mã hóa trở lại thành dữ liệu gốc, sao cho người được phép có thể đọc và hiểu thông tin ban đầu.
* [Plaintext](https://en.wikipedia.org/wiki/Plaintext) (Bản rõ): là thông tin ban đầu chưa được che giấu. Nó có thể ở dạng văn bản, hình ảnh, video hoặc bất kỳ định dạng khác. Plaintext có thể dễ dàng đọc và hiểu bởi bất kỳ ai có quyền truy cập vào nó nên nó cần được che dấu và bảo vệ.
* [Ciphertext](https://en.wikipedia.org/wiki/Ciphertext) (Bản mã): Là kết quả của quá trình mã hoá plaintext, là dạng dữ liệu đã được che giấu. Ciphertext là vô nghĩa với các bên khác, ngoại trừ các bên trao đổi thông tin với nhau.
* [Key](https://en.wikipedia.org/wiki/Key_(cryptography)) (Khoá): Còn gọi là cryptographic key (khoá mật mã), là một mẩu thông tin dưới dạng chuỗi số hoặc chữ cái, được sử dụng trong quá trình mã hoá và giải mã. Key là thành phần tối quan trọng, cần được giữ kín. Nếu key bị lộ, bất kỳ ai có được key cũng có thể biết được nội dung của plaintext.
* [Cipher](https://en.wikipedia.org/wiki/Cipher): Là thuật toán dùng để má hoá và giải mã dữ liệu.
* Decipher (Phá mã): Là thuật toán dùng để tấn công vào ciphertext với mục tiêu tiếp cận đến plaintext mà không cần tới key.

**2/ Mục tiêu của Cryptography**

Về cơ bản, mục tiêu chính ủa Cryptography là bảo đảm 4 yếu tố cho dữ liệu, bao gồm:

Confidentiality (Tính bảo mật)**,** Integrity (Tính toàn vẹn), Authentication (Tính xác thực), Non-repudiation (Tính chống chối bỏ)

***### Chèn hình 2 ###***

2.1 Confidentiality (Tính bảo mật)

Tính bí mật đảm bảo rằng thông tin chỉ có thể được truy cập bởi những người, thực thể hoặc hệ thống có quyền hợp lệ. Những người không được phép sẽ không thể hiểu được dữ liệu đó.

2.2 Integrity (Tính toàn vẹn)

Tính toàn vẹn đảm bảo rằng dữ liệu không bị thay đổi, chỉnh sửa hoặc giả mạo trong quá trình lưu trữ hoặc truyền tải. Dù chỉ một thay đổi nhỏ trong dữ liệu cũng phải được phát hiện.

2.3 Authentication (Tính xác thực)

Tính xác thực đảm bảo rằng thông tin nhận được là từ đúng người hoặc đúng nguồn gửi, không bị giả mạo danh tính. Nó cũng xác nhận rằng thông điệp không bị can thiệp bởi bên thứ ba.

2.4 Non-repudiation

Tính không chối bỏ đảm bảo rằng một cá nhân hoặc hệ thống không thể phủ nhận hành động mà họ đã thực hiện — chẳng hạn như đã gửi một tin nhắn, ký một tài liệu, hay thực hiện một giao dịch.

**Ví dụ:**

* Khi bạn ký một hợp đồng điện tử bằng chữ ký số, bạn không thể chối bỏ sau đó rằng bạn đã không ký nó — vì hệ thống có thể chứng minh được hành động đó là của bạn.
* ...

Kỹ thuật sử dụng:

* Chữ ký số kết hợp với timestamp (dấu thời gian)
* Ghi log có chứng thực
* Blockchain cũng là một công nghệ giúp đảm bảo tính không chối bỏ, nhờ khả năng ghi nhận mọi hành động vào sổ cái bất biến.

**3/ Phân loại mã hóa**

**3.1 Mã hóa đối xứng (symmetric encryption)**

Hay còn gọi là mã hóa khóa bí mật (Secret Key Encryption) là một phương pháp mã hóa trong đó cùng một khóa được sử dụng cả để mã hóa và giải mã dữ liệu. Đây là một trong những kỹ thuật mã hóa lâu đời và phổ biến nhất.

***### chèn hình 3.webapp ###***

***3.2 Mã hóa bất đối xứng (Asymmetric encryption)***

Hay còn gọi là mã hóa khóa công khai (Public Key Encryption) là một phương pháp mã hóa sử dụng hai khóa khác nhau: một khóa công khai (public key) để mã hóa và một khóa bí mật (private key) **để giải mã**. Đây là cơ sở của nhiều hệ thống bảo mật hiện đại như HTTPS, chữ ký số,…

***###Chèn hình 4.png###***

**3.3 Hàm băm mật mã (Cryptographic Hash Function)**

***###Chèn hình 5.png###***

Đôi khi ta chỉ cần mã hóa thông tin chứ không cần giải mã thông tin, khi đó ta sẽ dùng đến phương pháp mã hóa một chiều (Chỉ có thể mã hóa chứ không thể giải mã). Thông thường phương pháp mã hóa một chiều sử dụng một hàm băm (hash function) để biến một chuỗi thông tin thành một chuỗi hash có độ dài nhất định. Ta không có bất kì cách nào (rất khó) để khôi phục (hay giải mã) chuỗi hash về lại chuỗi thông tin ban đầu.

Hàm băm thường được dùng để kiểm tra tính toàn vẹn của dữ liệu.

**II/ Kiến thức cơ bản và một số thuật toán mã hóa tiêu biểu**

*1. Một số kiến thức cơ bản*

*1.1 Kí hiệu biểu diễn trong cryptography*

## a. Ký hiệu phổ biến

|  |  |
| --- | --- |
| Ký hiệu | Ý nghĩa |
| P | Plaintext – Văn bản gốc (chưa mã hóa) |
| C | Ciphertext – Văn bản đã mã hóa |
| K | Key – Khóa dùng để mã hóa hoặc giải mã |
| E\_K(P) | Encryption – Mã hóa P với khóa K, cho ra C |
| D\_K(C) | Decryption – Giải mã C với khóa K, lấy lại P |
| H(m) | Hash function – Băm thông điệp m thành giá trị băm |
| Sign\_sk(m) | Ký thông điệp m bằng khóa riêng sk |
| Verify\_pk(m, σ) | Xác minh chữ ký σ bằng khóa công khai pk |
| || | Phép nối (concatenation) giữa hai chuỗi |

## b. Ký hiệu khóa

|  |  |
| --- | --- |
| Ký hiệu | Ý nghĩa |
| K | Khóa chung (mã hóa đối xứng) |
| (pk, sk) | Cặp khóa công khai và khóa bí mật trong mã hóa bất đối xứng |
| K\_enc, K\_dec | Khóa dùng riêng cho mã hóa hoặc giải mã |

## c. Thuật ngữ kỹ thuật (thường viết tắt)

|  |  |
| --- | --- |
| Viết tắt | Ý nghĩa |
| PRG | Pseudo-Random Generator – Bộ sinh số giả ngẫu nhiên |
| PRF | Pseudo-Random Function – Hàm giả ngẫu nhiên |
| MAC | Message Authentication Code – Mã xác thực thông điệp |
| IV | Initialization Vector – Vector khởi tạo cho chế độ mã khối |
| OTP | One-Time Pad – Mã hóa pad một lần, tuyệt đối an toàn |

## *1.2 Một số kiến thức toán học cơ bản*

Trong suốt quá trình hình thành và phát triển, Cryptography đã liên tục áp dụng rất nhiều lĩnh vực toán học để xây dựng nên các phương pháp mã hóa ngày càng mạnh mẽ và an toàn hơn. Một số lĩnh vực toán học nổi bật được áp dụng gồm: Lý thuyết số, đại số tuyến tính, xác suất thống kê, lý thuyết thông tin, lý thuyết nhóm,… Ở đây chúng ta sẽ chỉ đề cập về một số kiến thức lý thuyết số cơ bản.

***\*Đồng dư thức:***

Cho a,b,n ∈ Z

Kí hiệu a ≡ b (mod n), có nghĩa là n|(a-b) hay (a-b)┇n

***\*Nghịch đảo Modulo:***

Cho số nguyên dương m và số tự nhiên a < m, nếu GCD(a, m) = 1 thì tồn tại X sao cho:

aX ≡ 1 (mod m)

\****Phi hàm Euler***: Phi hàm Euler của một số nguyên dương n là số lượng số nhỏ hơn và nguyên tố cùng nhau với n. Kí hiệu là Φ(n).

Ví dụ Φ(7) = 6, Φ(9) = 6,...

Dễ thấy nếu n là số nguyên tố thì Φ(n) = n-1.

***\*Định lí Euler:***

Cho a,n ∈ N\*, a và n nguyên tố cùng nhau

**aΦ(n) ≡ 1 (mod n)**

Dễ thấy nếu n nguyên tố, ta sẽ có:

**an-1≡ 1 (mod n)** (Định lí Fermat nhỏ)

***\*Định lí Wilson:***

Cho số nguyên n>1, n là số nguyên tố khi và chỉ khi:

(n-1)! **≡** n-1 (mod n)

***\*Định lí Phần dư Trung Hoa :***

Cho hệ phương trình đồng dư:  
  
x ≡ a₁ (mod m₁)  
x ≡ a₂ (mod m₂)  
...  
x ≡ ak (mod mk)  
  
Nếu các m₁, m₂, ..., m\_k đôi một nguyên tố cùng nhau, thì hệ có họ nghiệm duy nhất modulo M = m₁ \* m₂ \* ... \* m. Tức nghiệm sẽ có dạng x = x\* + kM (k ∈ Z)

2/ Một số thuật toán mã hóa tiêu biểu

2.1 Một số thuật toán mã hóa đối xứng tiêu biểu:

2.1.1 Mã hóa Caeser:

Mã hóa Caesar là một phương pháp mã hóa thay thế cổ điển và đơn giản. Mỗi ký tự trong bản rõ được thay thế bằng một ký tự khác nằm cách nó một số vị trí cố định trong bảng chữ cái.

***### Chèn hình 6.png***  Kèm caption “Minh họa với độ lệch k = 4” ***###***

Nếu quy ước kí tự A = 0, B = 1, C = 2,…, Z = 25

Ta có công thức tìm giá trị x\* tương ứng của kí tự sau khi mã hóa kí tự có giá trị x với khóa K:

x\* = E\_k​(x) = (x+k) % 26 (tạm xe

Từ đó dễ thấy công thức giải mã với khóa K:

x = D\_k(x\*) = (x\* + 26 – k) % 6