ĐẠI NAM
UNIVERSITY

NHẬP MÔN AN TOÀN, BẢO MẬT THÔNG TIN

Giảng viên: Nguyễn Văn Nhân
Email: nhannv@dainam.edu.vn
Điện thoại: 0346542854

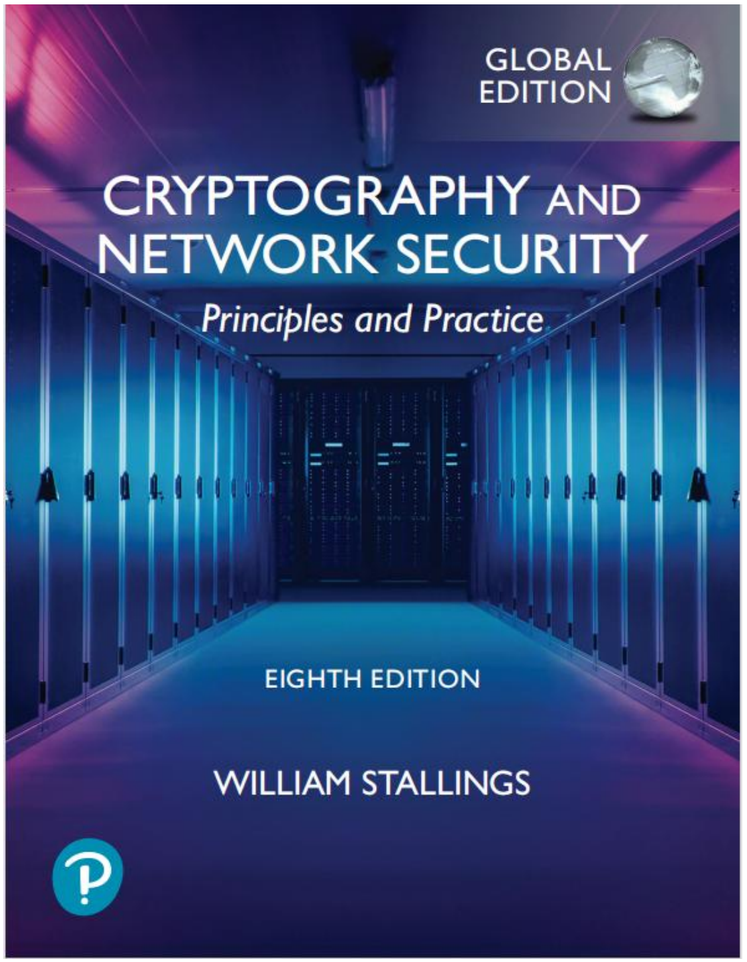
THÔNG TIN MÔN HỌC

1. Số tín chỉ: 03 (45 tiết)

2. Cơ cấu điểm: 40% (QT-KT) + 60 % (BTL)

3. Đánh giá kết thúc: Bài tập lớn

4. Tài liệu: Tiếng Anh + Tiếng Việt



THÔNG TIN MÔN HỌC

Tham gia nhóm Zalo: ATBMTT 17-09

VỊ TRÍ VIỆC LÀM

Kỹ Sư Mạng Và Bảo Mật (Network & Security)

Công Ty Cổ Phần Thương Mại Và Dịch Vụ Công Nghệ GTSC Việt Nam

$ 25-40 triệu | Hà Nội | 31/03/2025

IT Phần Mềm | Network

Nộp đơn

Tuyển 02 Nam Kỹ Thuật Điện, Biết Cài Mạng Lắp Camera

CÔNG TY TNHH CÔNG NGHỆ ĐIỆN TỬ THANH SƠN

$ 12-12 triệu | TPHCM | 31/03/2025

Kỹ Thuật Điện Tử | LAN

Nộp đơn

Nhân Viên Security SME

TMA Technology Group

$ 16-25 triệu | TPHCM | 30/03/2025

.NET | IT Phần Mềm

Nộp đơn

Security Engineer

Apero Technologies Group

$ 25-40 triệu | Hà Nội | 23/03/2025

.NET | Firewall

Nộp đơn

Junior Security Engineer - Tại Hà Nội - Thu Nhập Hấp Dẫn

Công Ty TNHH Avepoint Việt Nam

$ 10-15 triệu | Hà Nội | 30/06/2025

IT Phần Mềm | Java

Nộp đơn

MỤC TIÊU KIẾN THỨC VÀ KỸ NĂNG

1. **Hiểu thách thức và luật an ninh mạng:** Nắm các vấn đề mất an toàn, tấn công mạng, chính sách bảo mật, quản trị nguy cơ và các khía cạnh pháp lý liên quan.
2. **Nắm vững thuật toán bảo mật:** Hiểu và áp dụng mã hóa/giải mã (DES, AES, RSA, Diffie-Hellman), hàm băm (MD5, SHA), và chữ ký số RSA.
3. **Phát triển kỹ năng ứng dụng:** Nhận diện, phân tích tấn công mạng, đề xuất giải pháp, và áp dụng thuật toán mã hóa, khóa công khai, chữ ký số trong giao dịch.

ĐẠI NAM
UNIVERSITY

Bài 1

CƠ SỞ AN TOÀN, BẢO MẬT THÔNG TIN

Giảng viên: Nguyễn Văn Nhân
Email: nhannv@dainam.edu.vn
Điện thoại: 0346542854

NỘI DUNG

1. Giới thiệu chung

2. Tổng quan về an toàn, bảo mật thông tin

3. Mật mã học

GIỚI THIỆU

❖ Tìm hiểu về một số vụ tấn công mạng nổi tiếng toàn cầu

=> Tầm quan trọng của bảo mật thông tin.

GIỚI THIỆU

Hacker là kẻ xấu?

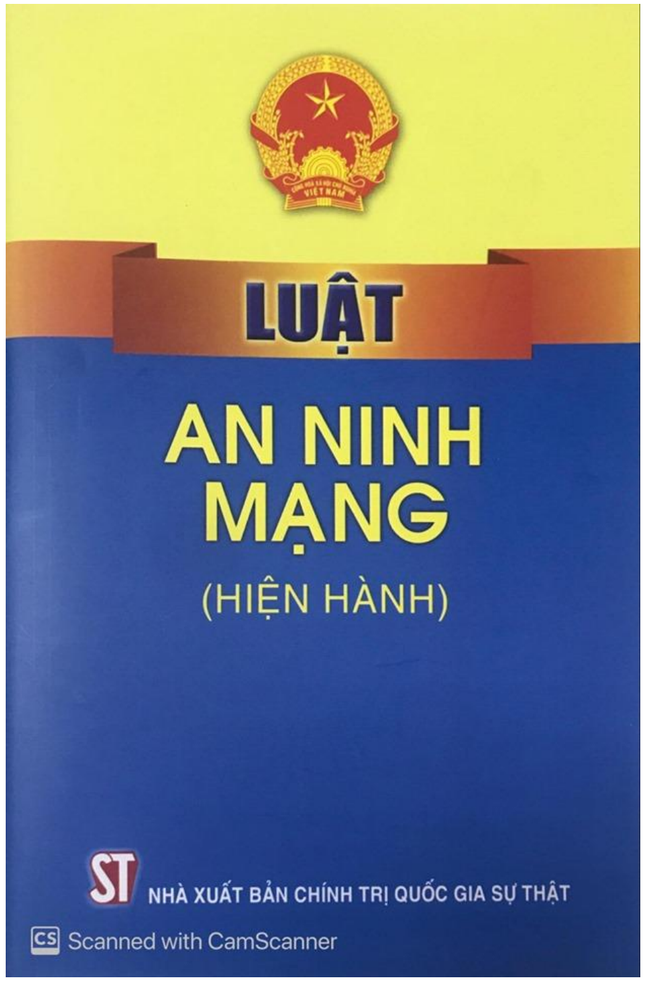
GIỚI THIỆU

Cyber Security?

Information Security?

GIỚI THIỆU

Luật an ninh mạng?



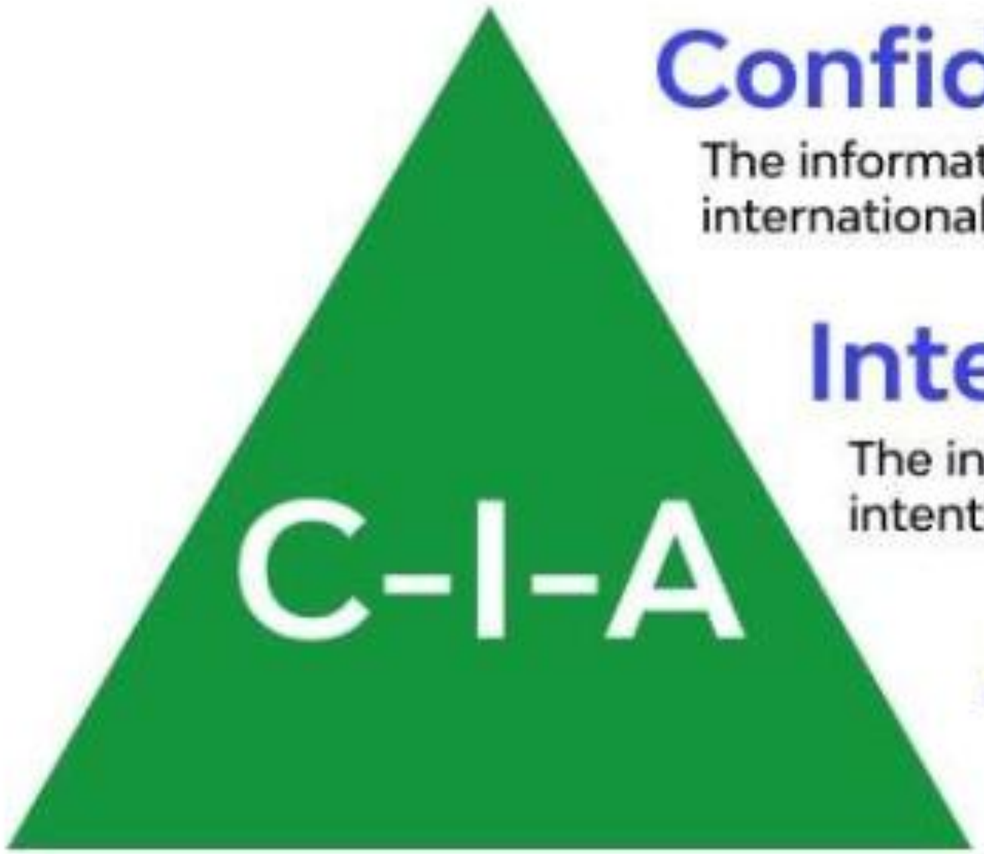
https://vanban.chinhphu.vn/?pageid=27160&docid=206114

TỔNG QUAN VỀ AN TOÀN, BẢO MẬT THÔNG TIN

Khái niệm về an toàn, bảo mật thông tin

- Bảo vệ thông tin và hệ thống thông tin nói chung khỏi các truy cập trái phép, sử dụng, làm lộ, chỉnh sửa, làm hỏng, ghi chép không được phép…

Tam giác C.I.A



Confidentiality

The information is safe from accidental or international disclosure

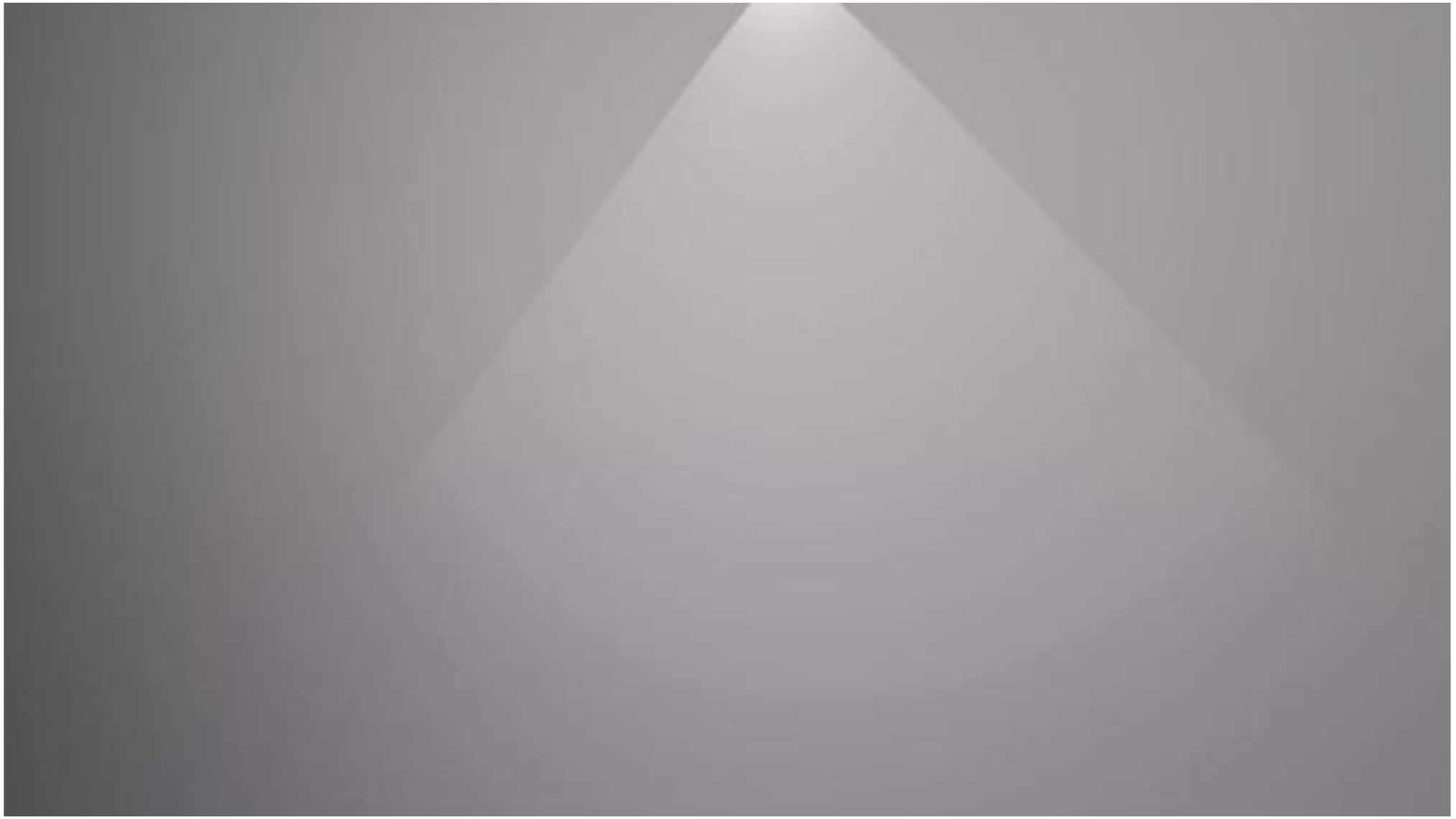
Integrity

The information is safe from accidental or intentional modification or alteration

Availability

The information is available to authorized users when needed.

TỔNG QUAN



TỔNG QUAN

- ✓ **Luôn tồn tại nhiều mối đe dọa trực tuyến**, bao gồm lừa đảo ("scam scam scam scam scam"), mã độc ("creepy malware"), tấn công ("hack hack hack hack hack"), và nguy cơ mất dữ liệu cá nhân ("cookie going to crash crash crash crash cash") cũng như dữ liệu hệ thống ("hard drive's going to crash crash crash crash crash")
- ✓ **Việc chủ động bảo vệ bản thân trên mạng là rất quan trọng**. Điều này bao gồm việc "lock it down", sao lưu dữ liệu ("back back. Back it up"), và cảnh giác với các liên kết đáng ngờ ("I'm not going to click")
- ✓ **Cần liên tục học hỏi về các mối đe dọa trực tuyến** để có thể bảo vệ mình một cách tốt nhất ("keep surfing. Can't stop. Won't stop learning. The threats from everywhere on the web")
- ✓ **Email lừa đảo ("fishing mails") là một mối đe dọa phổ biến** mà người dùng cần phải cẩn trọng

Các hình thức làm mất an toàn thông tin

- Chủ động:

  Tấn công, lấy cắp thông tin, Xâm nhập, phá hoại

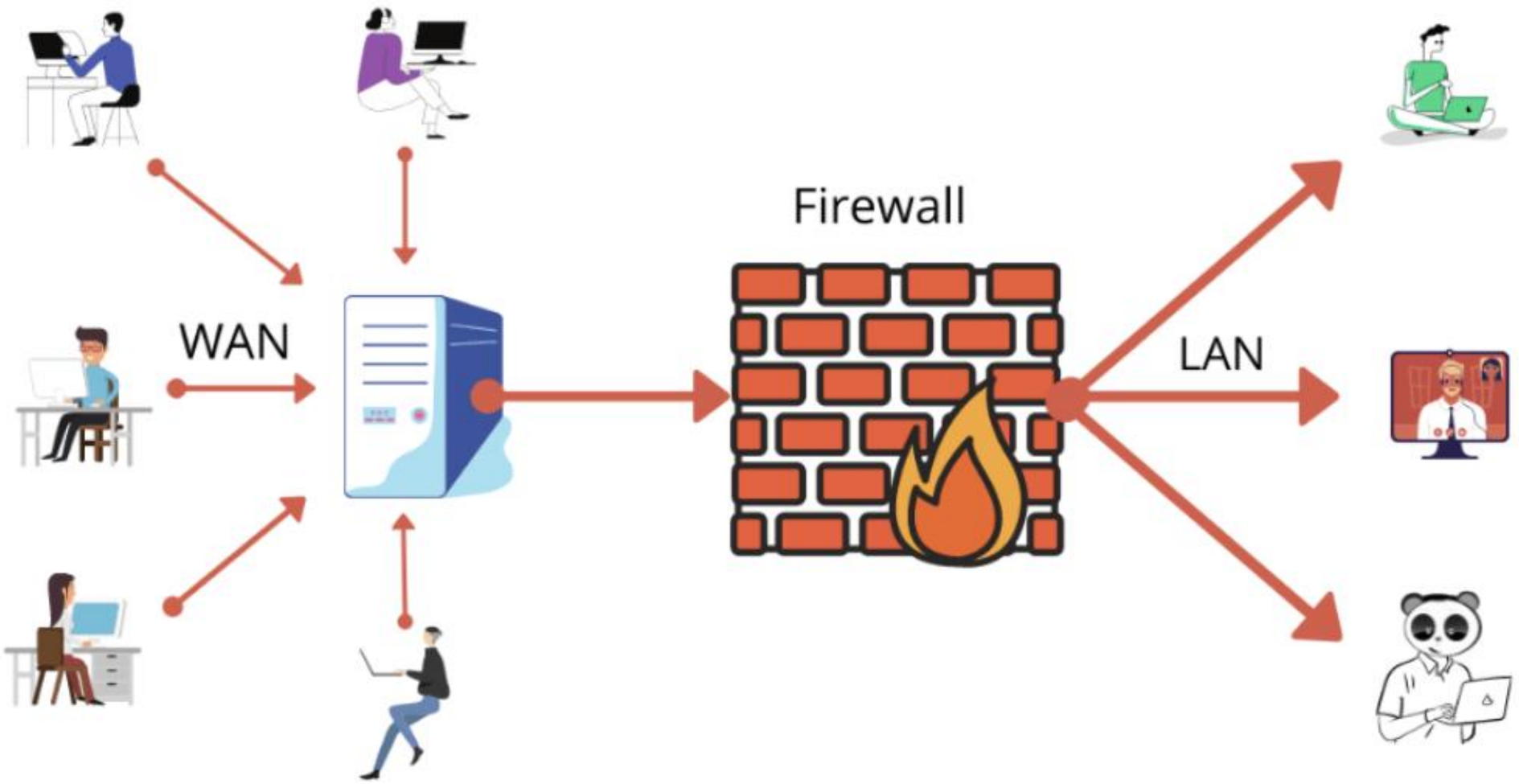
- Thụ động:

  Thiết kế, lập trình, quản trị

Các biện pháp an toàn, bảo mật thông tin

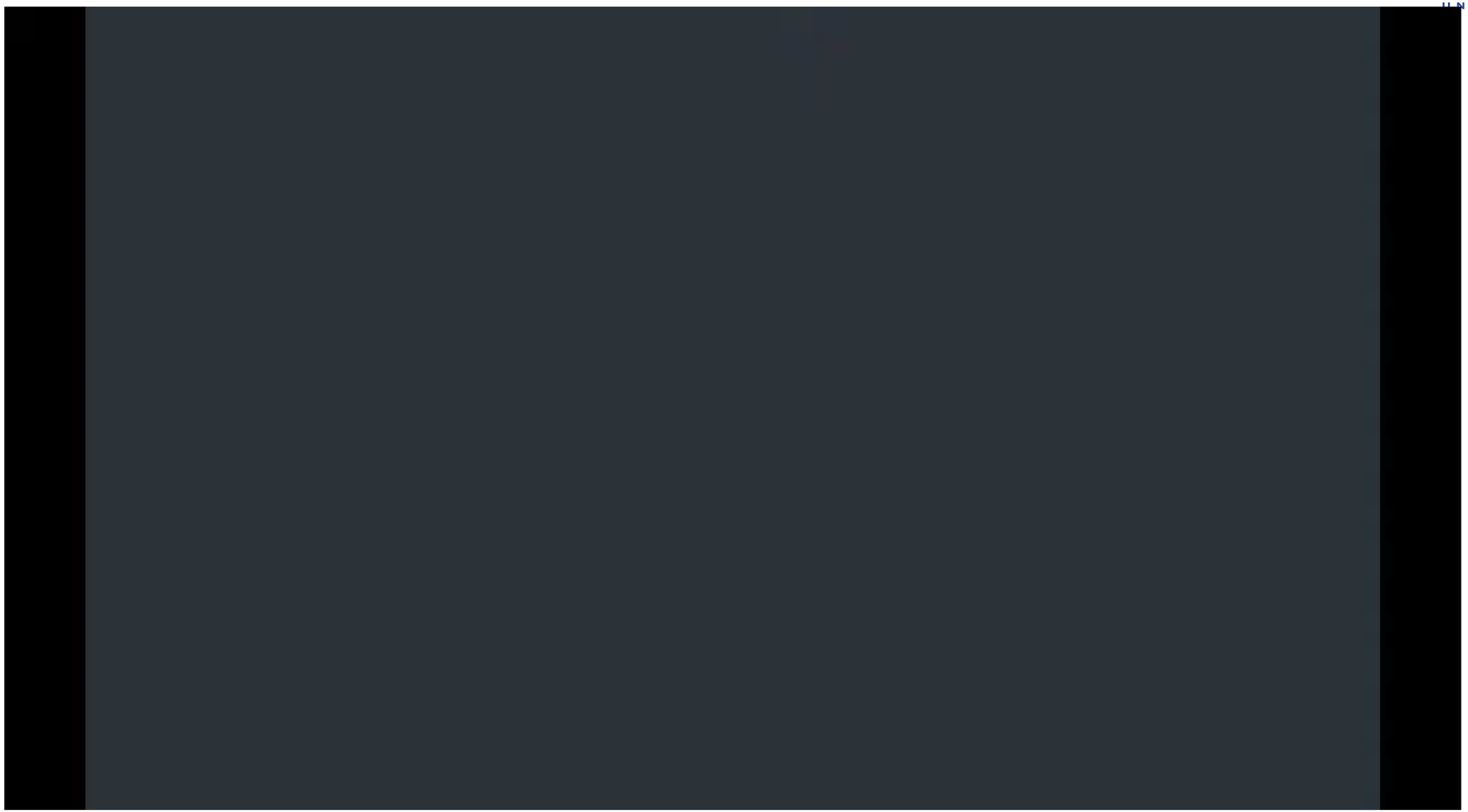
- Vật lý
- Giao thức
- Dữ liệu, phần mềm
- Chính sách, phương thức, luật pháp

TỔNG QUAN



MẬT MÃ HỌC

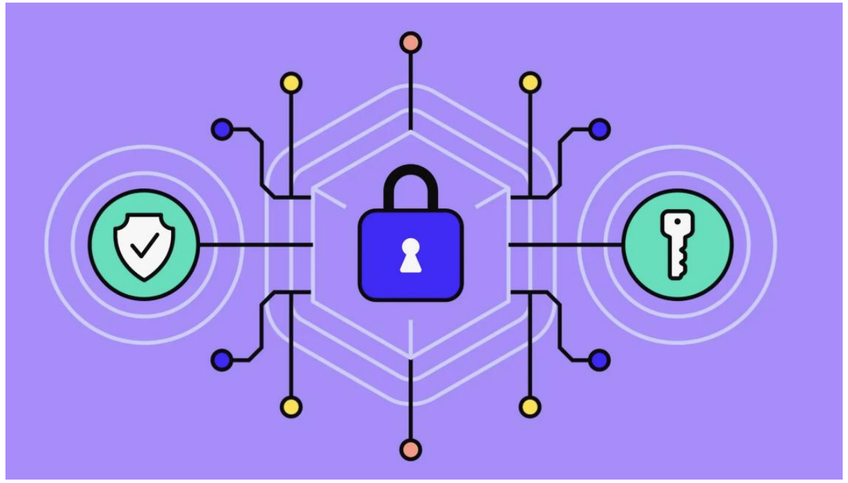
MẬT MÃ HỌC



Lịch sử về mật mã học

Khái niệm mật mã học

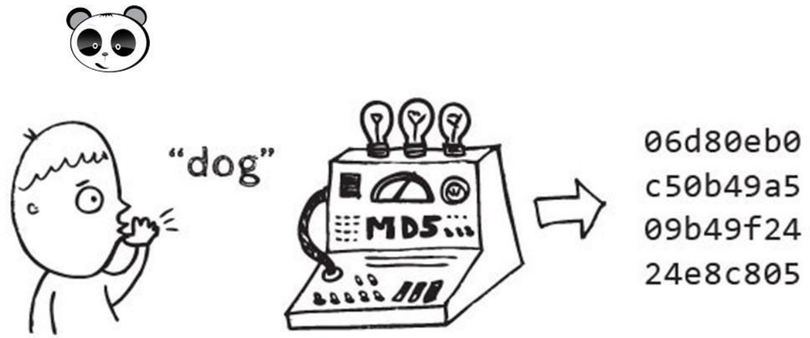
- Mật mã học (Cryptography): Là ngành khoa học nghiên cứu về việc đảm bảo an toàn thông tin. Mật mã học gắn liền với quá trình mã hóa nghĩa là chuyển đổi thông tin từ dạng "có thể hiểu được" thành dạng "không thể hiểu được" và ngược lại là quá trình giải mã



https://viblo.asia/p/nhung-khai-niem-co-ban-trong-mat-ma-hoc-RnB5p7MrlPG

Khái niệm mật mã học

❖ Cryptography is a branch of mathematics that deal with the transformation of data. Cryptography algorithms are used in many ways in information security and network security. Cryptography is an essential component in the secure storage and transmission of data, and in the secure interaction between parties.



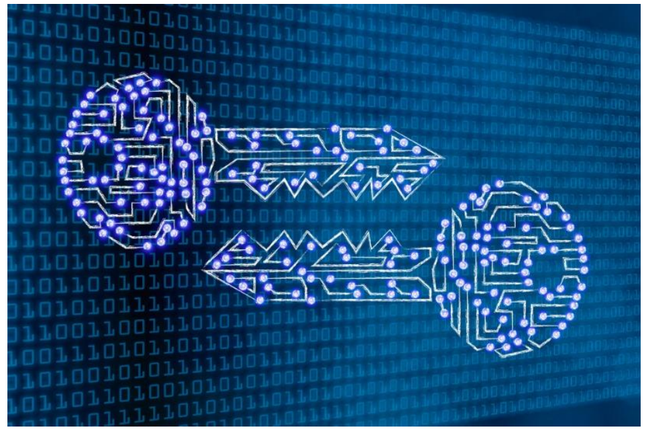
Khái niệm mật mã học

❖ Thám mã (Cryptanalysis): Nghiên cứu cách phá các hệ mật nhằm phục hồi bản rõ ban đầu từ bản mã, nghiên cứu các nguyên lí và phương pháp giải mã mà không biết khóa.

- Tìm khóa vét cạn
- Phân tích thống kê
- Phân tích toán

MẬT MÃ HỌC

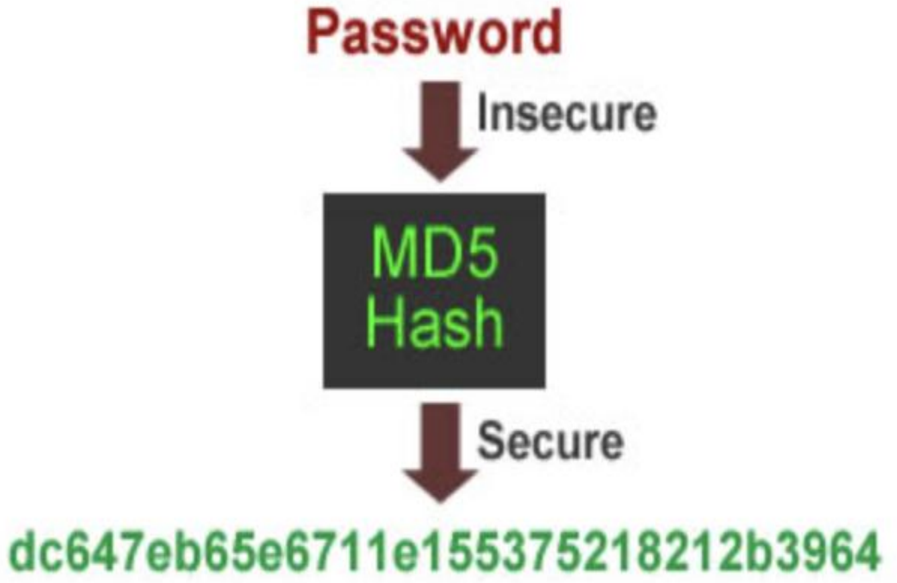
Khái niệm mật mã học



- Bản rõ (Plaintext): Dạng ban đầu của thông báo
- Bản mã (Ciphertext): Dạng mã của bản rõ ban đầu
- Khóa (Key): thông tin tham số dùng để mã hóa
- Mã hóa (Encryption): Quá trình biến đổi thông tin từ dạng bản rõ sang bản mã bằng khóa hoặc không cần khóa
- Giải mã (Decryption): Quá trình ngược lại biến đổi thông tin từ dạng bản mã sang bản rõ

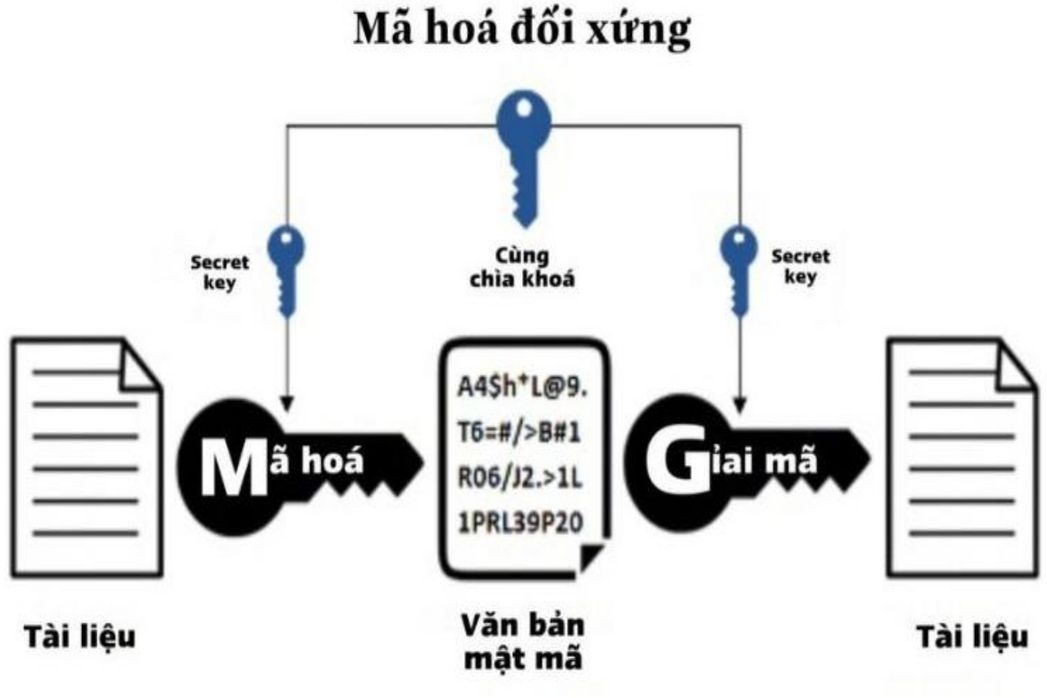
Mã hoá một chiều (Keyless Algorithms)

- 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.



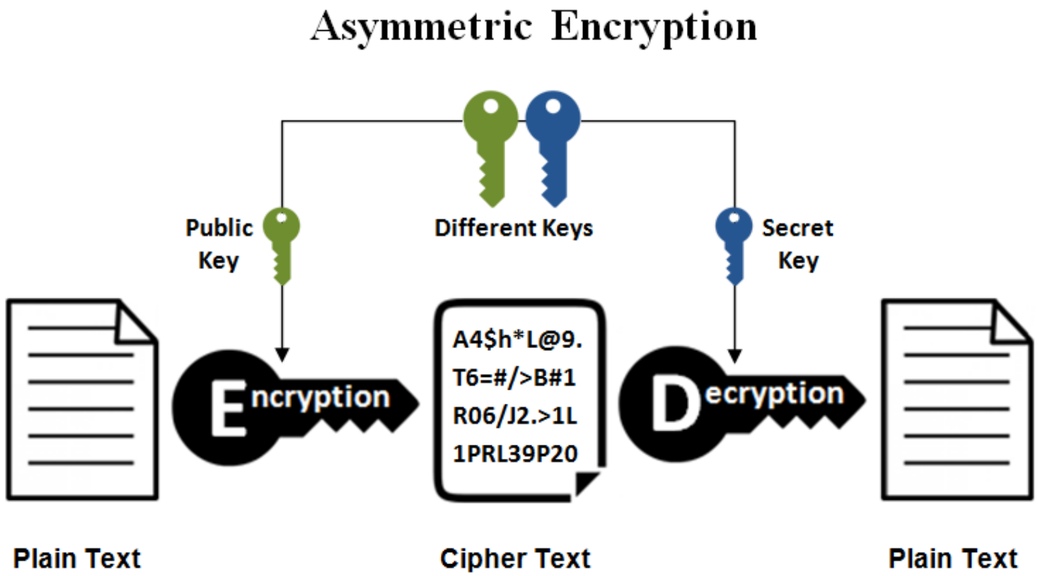
Thuật toán mã hoá đối xứng (Single-Key Algorithms)

- Mã hóa đối xứng còn có một số tên gọi khác như Secret Key Cryptography (hay Private Key Cryptography), sử dụng cùng một khóa cho cả hai quá trình mã hóa và giải mã.
- Thuật toán: DES, AES



Thuật toán mã hoá bất đối xứng (Two-Key Algorithms)

- Hay còn được gọi với một cái tên khác là mã hóa khóa công khai (Public Key Cryptography), nó được thiết kế sao cho khóa sử dụng trong quá trình mã hóa khác biệt với khóa được sử dụng trong quá trình giải mã.



TỔNG KẾT

- Tổng quan về an toàn, bảo mật thông tin
- Mật mã học

ĐẠI NAM
UNIVERSITY