INDUSTRIAL UNIVERSITY OF HOCHIMINH CITY

Chương 5:
MẬT MÃ HỌC

(CRYPTOGRAPHY)

Nội dung

1. Khái niệm cơ bản
2. Kỹ thuật mã hóa đối xứng
3. Kỹ thuật mã hóa bất đối xứng

1. Khái niệm cơ bản về mã hóa

Mật mã học (cryptography):	• Là ngành khoa học nghiên cứu các phương pháp toán học để mã hóa giữ bảo mật thông tin. Bao gồm mã hóa và giải mã.
Mã hóa (Encryption):	• Là quá trình chuyển bản rõ thành mã hóa. Nó giúp chúng ta che giấu, bảo mật thông tin trong khi lưu trữ cũng như truyền thông tin đi.
Giải mã (Decryption)	• Giải mã (decryption) là quá trình đưa bản mã về lại bản rõ ban đầu

1. Khái niệm cơ bản về mã hóa

Bản rõ (Plaintext):

- Là văn bản ban đầu được gọi là bản tin gốc. ở dạng rõ, có nghĩa có thể đọc hiểu và cần bảo vệ.

Bản mã (Ciphertext):

- Là văn bản sau khi mã hóa, ở dạng mờ, nghĩa là không thể đọc hiểu được.

Khóa (Key):

- Được sử dụng trong quá trình mã hóa và giải mã

Hệ thống mã hóa (cryptosystem)

- Cryptosystem = encryption + decryption algorithms

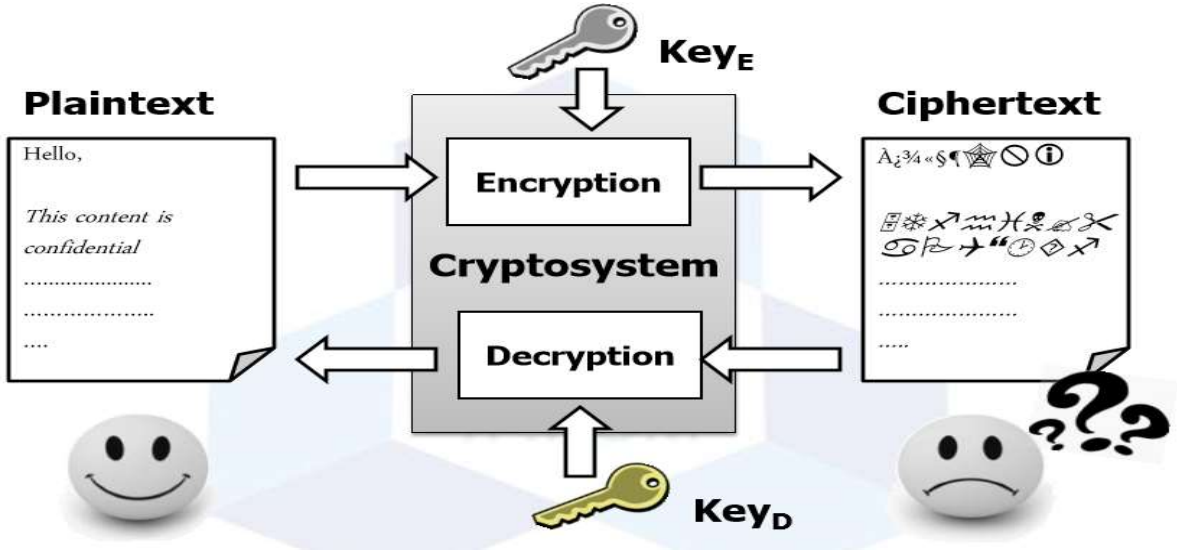
1. Khái niệm cơ bản về mã hóa

Chức năng cơ bản của hệ mã hóa

- **Tính bí mật**: nó đảm bảo tính bí mật của dữ liệu mà mình gửi đi và chỉ những người liên quan mới biết được nội dung.
- **Tính toàn vẹn**: đảm bảo dữ liệu không thể bị mất mát hoặc chỉnh sửa trong qua trình gửi và nhận mà không bị phát hiện.
- **Tính xác thực**: đảm bảo danh tính của thực thể được xác minh.
- **Tính không thể chối từ**: đảm bảo người gửi không thể chối cãi với thông tin mình gửi đi

1. Khái niệm cơ bản về mã hóa

Hệ thống mã hóa



1. Khái niệm cơ bản về mã hóa

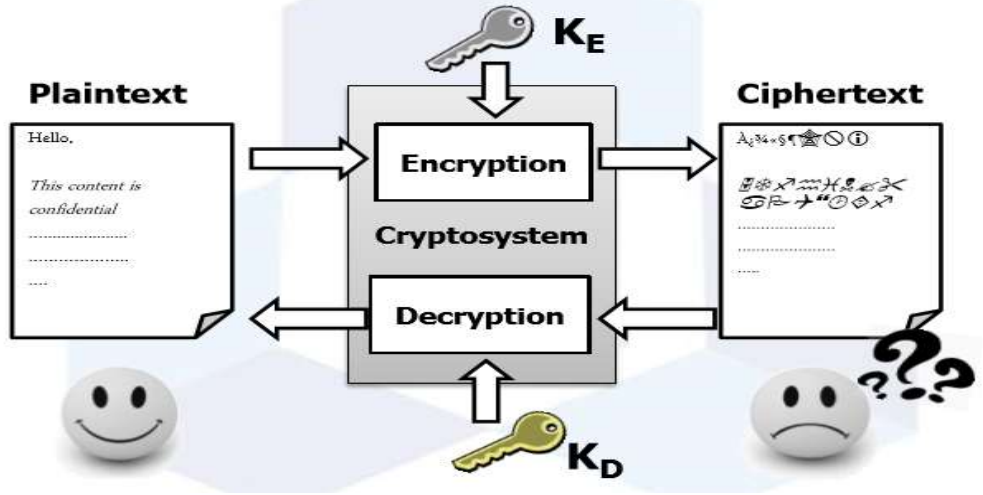
Hệ thống mã hóa

- **Hệ thống mã hóa đối xứng (Symmetric Cryptosystem)**
  - Sử dụng một khóa bí mật chia sẻ (sharedsecret-key) cho cả hai quá trình mã hóa và giải mã.
- **Hệ thống mã hóa bất đối xứng (Asymmetric Cryptosystem)**
  - Sử dụng một khóa công khai (public key) và một khóa riêng phần (private key) cho quá trình mã hóa và giải mã.
  - Hệ thống mã hóa bất đối xứng còn gọi hệ thống mã hóa khóa công khai (public-key cryptosystem)

1. Khái niệm cơ bản về mã hóa

Hệ thống mã hóa

- Mã hóa đối xứng: $K_E = K_D$
- Mã hóa bất đối xứng: $K_E \neq K_D$



1. Khái niệm cơ bản về mã hóa

Kỹ thuật cơ bản để chuyển bản rõ thành bản mã

(a) **Phép thế (substitution)**: dùng từng ký tự (hay từng nhóm ký tự) trong bản rõ được thay thế bằng một ký tự (hay một nhóm ký tự) khác để tạo ra bản mã. Bên nhận chỉ cần đảo ngược trình tự thay thế trên bản mã để có được bản rõ ban đầu.

(b) **Hoán vị (transposition)**: Các ký tự trong bản rõ được giữ nguyên, chúng chỉ được sắp xếp lại vị trí để tạo ra bản mã. Yêu cầu cơ bản là không có thông tin nào bị mất (có nghĩa là tất cả các thao thác có thể đảo ngược).

2. Kỹ thuật mã hóa đối xứng

- Mã hóa đối xứng sử dụng một khóa bí mật chia sẻ (sharedsecret-key) cho cả hai quá trình mã hóa và giải mã.
- Còn gọi **mã hóa một khóa** hoặc **mã hóa khóa bí mật**

2. Kỹ thuật mã hóa đối xứng

Hệ mã hóa gồm

- Bản rõ (M): bản tin được sinh ra bởi bên gửi
- Bản mã (C): bản tin che giấu thông tin của bản rõ, được gửi tới bên nhận qua một kênh truyền thông thường (không bảo mật)
- Khóa (Ks): nó là giá trị ngẫu nhiên và bí mật được chia sẽ giữa các bên trao đổi thông tin và được tạo ra từ:
  - Bên thứ 3 được tin cậy tạo và phân phối tới bên gửi và bên nhận
  - Hoặc, bên gửi tạo ra và chuyển cho bên nhận
- Mã hóa (encrypt-E): $C = E(K_S, M)$
- Giải mã (decrypt): $M = D(K_S, C) = D(K_S, E(K_S, M))$

2. Kỹ thuật mã hóa đối xứng

Cơ chế hoạt động

- Người gửi (sender) và người nhận (recipient) chia sẽ chung khóa K_s (chỉ có người gửi và người nhận biết K_s)
- Người gửi sẻ dùng thuật toán mã hóa để mã hóa thông điệp M thành bản mã C và gửi C cho người nhận, người nhận nhận được C sẽ dùng thuật toán giải mã để giải mã C thành M thì mới có thể đọc được
- Chỉ ai có khóa K_s thì mới thể giải C thành M

2. Kỹ thuật mã hóa đối xứng

Đặc điểm

- Khóa K_s dùng để mã hóa và giải mã → nếu bị lộ hoặc bị đánh cắp bởi người thứ 3 thì thông điệp M sẽ bị lộ thông tin, không còn bảo mật.
- Cần kênh truyền bảo mật để chia sẻ khóa bí mật giữa các bên → tốn chi phí
- Để đảm bảo liên lạc an toàn cho tất cả mọi người trong một nhóm gồm n người → cần tổng số lượng lớn khóa là n(n-1)/2, vấn đề quản lý và phân phối khóa
- Mã đối xứng dùng để bảo mật dữ liệu nhưng không thể dùng để xác thực hay chống thoái thác.

2. Kỹ thuật mã hóa đối xứng

Các kỹ thuật mã hóa đối xứng thông dụng:

- Mã cổ điển
- DES
- Triple DES
- AES

2. Kỹ thuật mã hóa đối xứng – mã DES

- **Data Encryption Standard (DES)**
- Phát hành 1977, chuẩn hóa 1979
- Mỗi thông điệp được chia thành những khối (block) 64 bits
- Kích thước khóa là 56 bít
- 1998, tổ chức Electronic Frontier Foundation (EFF) xây dựng được một thiết bị phá mã DES gồm nhiều máy tính chạy song song, trị giá khoảng 250.000$. Thời gian thử khóa là 3 ngày.
- Hiện nay mã DES vẫn còn được sử dụng trong thương mại, tuy nhiên người ta đã bắt đầu áp dụng những phương pháp mã hóa khác có chiều dài khóa lớn hơn (128 bít hay 256 bít) như TripleDES hoặc AES.

2. Kỹ thuật mã hóa đối xứng – Triple DES

- 1999, Triple DES được khuyến khích sử dụng thay cho DES
- Triple DES: thực hiện giải thuật DES ba lần.
- Mã hóa: $C=E(E(E(M, K_1),K_2),K_3)$
- Chiều dài khóa là 168 bít sẽ gây phức tạp hơn nhiều cho việc phá mã bằng phương pháp tấn công gặp-nhau-ở-giữa.
- Trong thực tế người ta chỉ dùng Triple DES với hai khóa *K*1, *K*2 mà vẫn đảm bảo độ an toàn cần thiết.

$$C=E(E(E(P, K_1),K_2),K_1)$$

2. Kỹ thuật mã hóa đối xứng – mã AES

- **Advanced Encryption Standard (AES)**
- Thập niên 90, nguy cơ của mã hóa DES là kích thước khóa ngắn, có thể bị phá mã trong tương lai gần, Cục tiêu chuẩn quốc gia Hoa Kỳ đã kêu gọi xây dựng một phương pháp mã hóa mới. Cuối cùng một thuật toán có tên là Rijndael (của Daemen và Rijmen) được chọn và đổi tên thành ***Andvanced Encryption Standard*** hay *AES*.
- Khóa có kích thước 256 bít là ***"an toàn mãi mãi"*** bất kể những tiến bộ trong ngành kỹ thuật máy tính.

3. Kỹ thuật mã hóa bất đối xứng

Các vấn đề gặp phải của kỹ thuật mã hóa đối xứng?

- Quản lý và phân phối khóa phức tạp
  - Mỗi cặp người dùng phải có khóa riêng
  - N người dùng cần N * (N-1)/2 khóa

  → Việc quản lý khóa trở nên phức tạp khi số lượng người dùng tăng
- Không phù hợp cho chữ ký số do không đạt được
  - Tính xác thực
  - Tính chống khoái thác

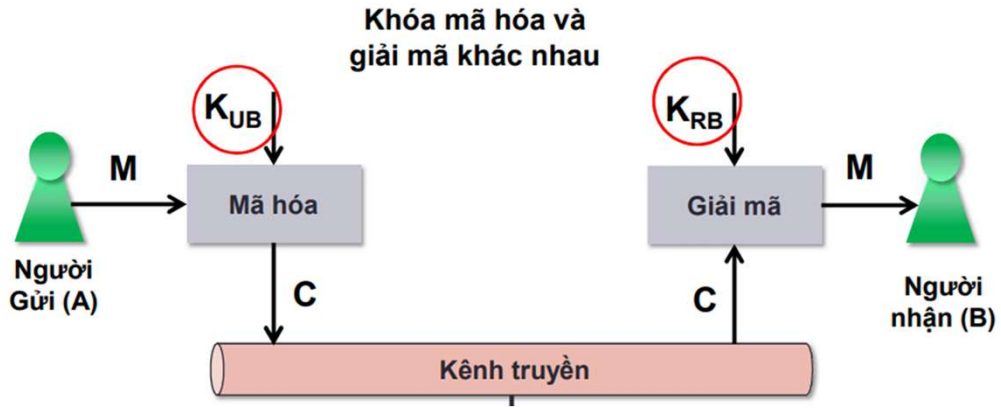
→ mã hóa bất đối xứng ra đời khắc phục 2 vấn đề này của đối xứng

3. Kỹ thuật mã hóa bất đối xứng

- Mỗi người dùng có 1 khóa riêng phần (Private key) và 1 khóa công khai (Public Key)
  - Khóa riêng phần bí mật
  - Khóa công khai có thể chia sẻ
- Quản lý khóa
  - N người dùng cần N khóa công khai được xác thực
  - Hạ tầng khóa công khai PKI

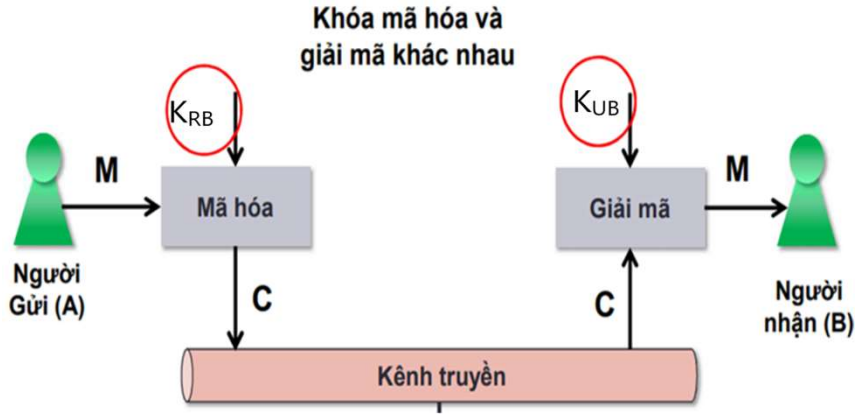
3. Kỹ thuật mã hóa bất đối xứng

- Mã hóa dùng khóa công khai KU
  - C = E(M, KU)
- Giải mã dùng khóa riêng KR
  - M = D(C, KR)



3. Kỹ thuật mã hóa bất đối xứng

- Mã hóa dùng khóa khóa riêng KR
  - C = E(M, KR)
- Giải mã dùng công khai KU
  - M = D(C, KU)



Mã hóa đối xứng vs. bất đối xứng

	Khóa bí mật	Khóa công khai
Số khóa	1	2
Bảo vệ khóa	Khóa được giữ bí mật	1 khóa bí mật 1 khóa công khai
Ứng dụng	Bí mật và toàn vẹn dữ liệu	Trao đổi khóa Xác thực
Tốc độ	Nhanh	Chậm

3. Kỹ thuật mã hóa bất đối xứng

- Lý thuyết nền tảng
  - Độ phức tạp
  - Số học đồng dư (Modular Arithmetic)
- Các hệ Mật mã khóa công khai
  - RSA
  - Đường cong êlip (Elliptic Curve)
  - Diffie-Hellman
  - ElGamal
  - DSS

3. Kỹ thuật mã hóa bất đối xứng

- Ứng dụng mã hóa công khai
- Có thể phân thành 3 loại:
  - **Mã hóa/giải mã (*Encryption/decryption*):** Sender mã hóa thông điệp bằng khóa public key của người nhận.
  - **Chữ ký số (*Digital signatures*)** – cung cấp chứng thực (authentication): Sender mã hóa thông điệp bằng khóa public key của người nhận. Chữ ký được lưu bằng một thuật toán áp đặt vào message hoặc gắn vào một khối nhỏ dữ liệu mà là một hàm của message
  - **Trao đổi khóa (*Key exchange*)**: Hai bên hợp tác để trao đổi **khóa phiên (session key)**

3. Kỹ thuật mã hóa bất đối xứng

- Một vài thuật toán thì phù hợp cho tất cả các ứng dụng, loại khác thì chỉ dành riêng cho một loại ứng dụng

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Elliptic Curve	Yes	Yes	Yes
Diffie-Hellman	No	No	Yes
DSS	No	Yes	No