MẬT MÃ ỨD TRONG ATTT

Bài 01: Nhắc lại kiến thức tổng quan về mật mã

1. Nội dung khóa học
2. Tổng quan về các thuật toán mật mã
3. Một số vấn đề khác trong mật mã
4. Bài tập lớn, tiểu luận

1. Nội dung khóa học
2. Tổng quan về các thuật toán mật mã
3. Một số vấn đề khác trong mật mã
4. Bài tập lớn, tiểu luận

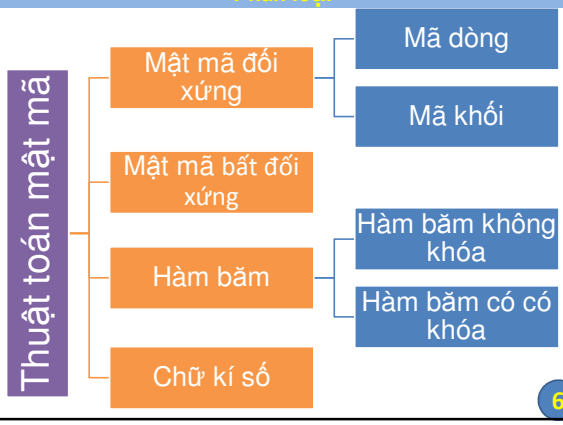
Nội dung khóa học

- ❑Nội dung
- ❑Tài liệu tham khảo
  - Cơ sở lý thuyết mật mã (Hv KTMM), 2013
  - Mật mã ứng dụng trong ATTT (Hv KTMM), 2013
  - St Denis, Tom. Cryptography for developers. Elsevier, 2006.
  - Applied Cryptography (Bruce Schneier)
  - Handbook of Applied Cryptography (Menezes et al.)
  - Cryptography Engineering (Bruce Schneier)
  - D. Boneh and Victor Shoup. A Graduate Course in Applied Cryptography, 2015.
  - Saiful Azad, Al-Sakib Khan Pathan. Practical Cryptography: Algorithms and Implementations Using C++, 2015.

4

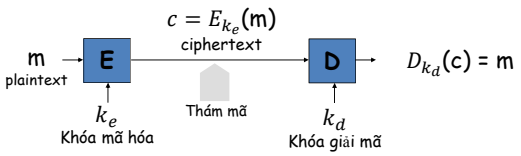
1. Nội dung khóa học
2. Tổng quan về các thuật toán mật mã
3. Một số vấn đề khác trong mật mã
4. Bài tập lớn, tiểu luận

Phân loại



6

Mật mã đối xứng

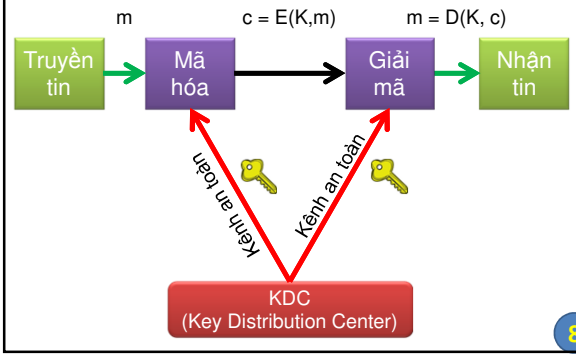


DES, 3DES
IDEA
AES
RC2,
RC4
SEAL

thông thường $k_e = k_d$

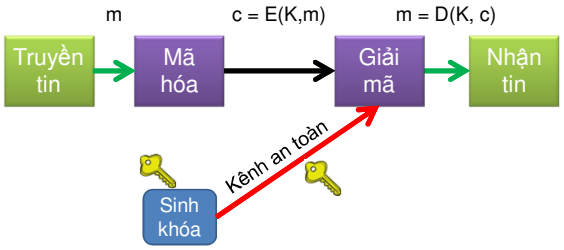
7

Mật mã đối xứng



8

Mật mã đối xứng



9

Tính chất của mật mã đối xứng

- Biết được khóa mã hóa sẽ dễ dàng suy ra khóa giải mã (Thông thường: Khóa mã hóa và khóa giải mã là như nhau), khóa được chia sẻ và giữ bí mật bởi hai bên.
- Với khóa K định trước thì quan hệ giữa bản rõ m và bản mã c là một tương ứng 1:1
- Số lượng khóa trong hệ thống n người dùng là n(n-1)/2
- Nói chung, khó chứng minh được độ an toàn về mặt lý thuyết → An toàn thực tế
- Các phép toán thường đơn giản nên cho tốc độ cao

10

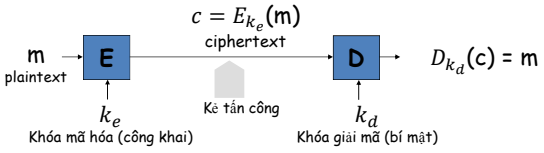
Ứng dụng của mật mã khóa đối xứng

Ứng dụng của mật mã khóa **đối xứng**

- Mã hóa dữ liệu khi lưu trữ
- Mã hóa dữ liệu trên đường truyền
- Xác thực
- Sử dụng như hàm băm có khóa

11

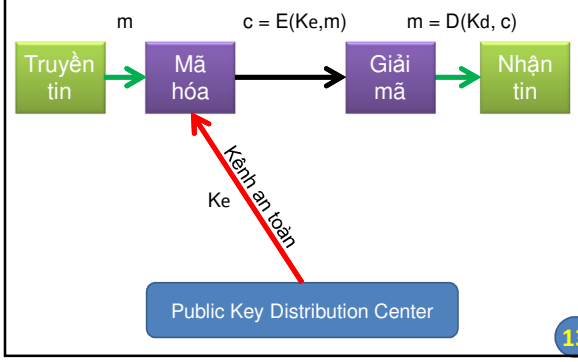
Mật mã khóa công khai



RSA
El-Gamal; DSA
ECDH, ECDSA

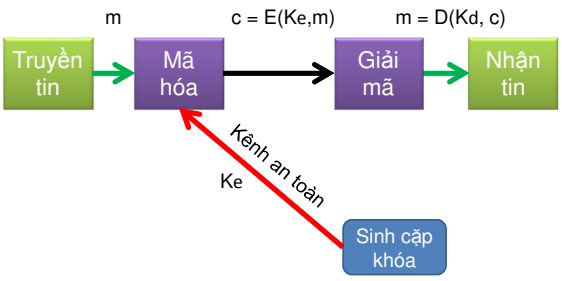
12

Mật mã khóa công khai



13

Mật mã khóa công khai



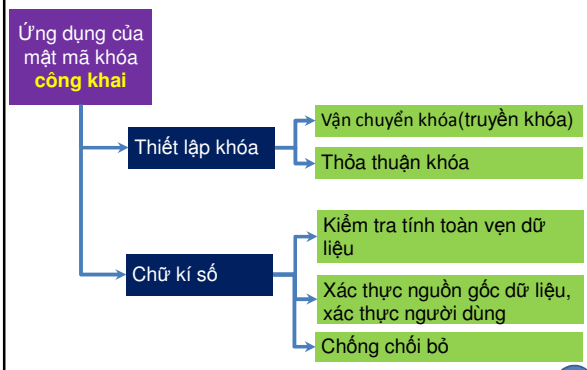
14

Tính chất của mã hóa khóa công khai

- Khóa mã hóa và khóa giải mã là khác nhau.
- Mỗi bên có khóa bí mật của riêng mình và khóa công khai tương ứng (Kd, Ke).
- Từ khóa công khai không thể tìm ra khóa bí mật
- Dữ liệu được mã hóa bằng khóa công khai, giải mã bằng khóa bí mật
- Mọi người đều có thể mã hóa nhưng chỉ một người có thể giải mã, chính người mã hóa cũng không thể giải mã
- Thường tính toán trên số lớn nên cho tốc độ thực thi thấp

15

Ứng dụng của mật mã khóa công khai



16

So sánh mật mã đối xứng và mật mã khóa công khai

Mật mã đối xứng	Mật mã khóa công khai
	IG n số ỏ
	toán nên
nên tốc độ CAO → có thể xử lý lượng LỚN dữ liệu	tốc độ THẤP → chỉ phù hợp với lượng NHỎ dữ liệu

Loại nào an toàn hơn?

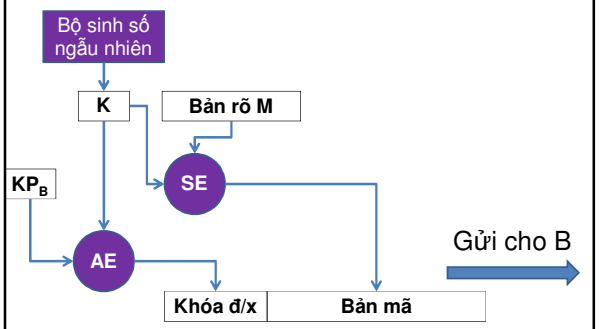
17

So sánh mật mã đối xứng và mật mã khóa công khai

Sử dụng mật mã đối xứng
hay
mật mã khóa công khai?

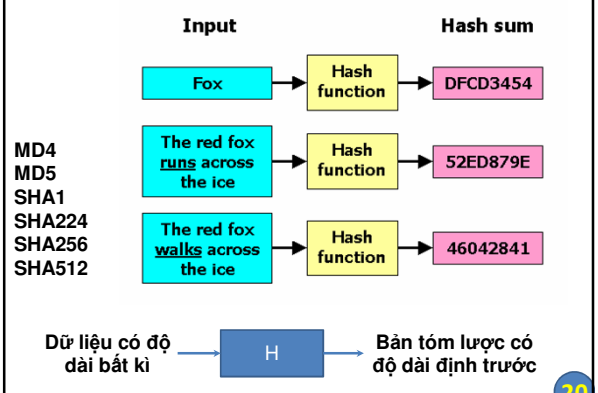
18

Sử dụng mật mã đối xứng và mật mã khóa công khai



19

Hàm băm



20

Tính chất của hàm băm

- Nén → quan hệ giữa thông điệp và bản tóm lược không phải là tương ứng 1:1
- Kháng tiền ảnh: từ H(x) không thể tìm được x
- Kháng tiền ảnh thứ hai: cho trước x, không thể tìm được x' sao cho H(x) = H(x')
- Kháng va chạm: không thể tìm được cặp (x, y) sao cho H(x) = H(y)

21

Ứng dụng của hàm băm

Ứng dụng của **hàm băm**

- Kiểm tra tính toàn vẹn dữ liệu
- Xác thực nguồn gốc dữ liệu
- Sử dụng trong các lược đồ xác thực người dùng

22

Chữ kí số

Chữ kí viết tay

- Đặc trưng cho người kí, mỗi người có một chữ kí đặc trưng, không thể được tạo ra bởi người khác
- Chữ kí gắn liền với một văn bản, không thể tách rời văn bản, thường giống nhau trên nhiều văn bản.
- Mọi người đều có khả năng kiểm tra chữ kí của một người bất kì

23

Chữ kí số

Chữ kí số

- Là thông điệp dữ liệu (dãy bít)
- Có các tính chất của chữ kí viết tay

24

Chữ kí số

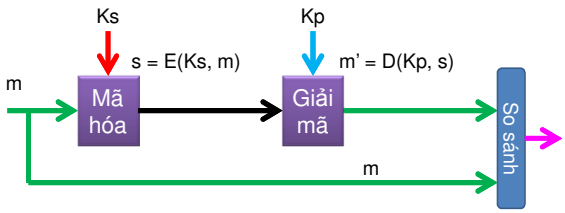
Chữ kí số

- Đặc trưng cho người kí → phụ thuộc vào yếu tố bí mật của riêng người kí
- Là phần tách rời với văn bản, hai văn bản khác nhau thì có chữ kí số khác nhau → chữ kí phụ thuộc vào chính văn bản
- Người bất kì có thể kiểm tra →có một đại lượng công khai tương ứng với yếu tố bí mật

→ ứng dụng mật mã khóa công khai

25

Chữ ký số



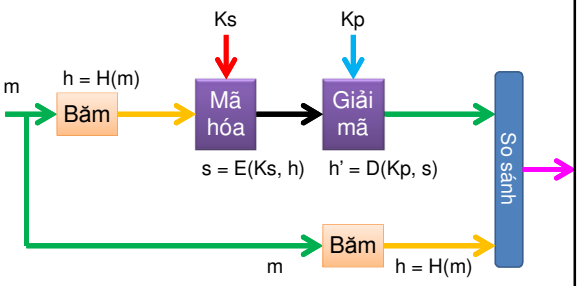
Lưu lượng tăng gấp đôi

Kích thước của m thường vượt quá khả năng tính toán hiện nay

→ Lấy đại diện của m

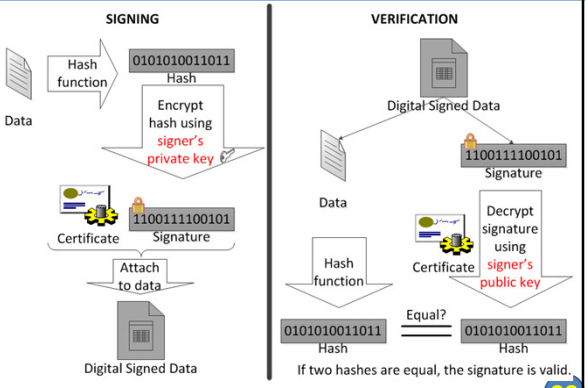
26

Chữ ký số



27

Chữ kí số



28

Một số ứng dụng thực tế của mật mã

Vai trò của mật mã trong ATTT

29

Vai trò của mật mã trong ATTT

Đảm bảo tính bí mật

Đảm bảo tính toàn vẹn

Đảm bảo tính xác thực

Đảm bảo tính chống chối bỏ

30

Một số ứng dụng thực tế của mật mã

Mã hóa file, ổ đĩa

- Office, PDF, Archive...
- NTFS
- BitLocker, TrueCrypt,...

Mã hóa dữ liệu trên đường truyền

- VPN, IPsec, SSL/TLS, SSH...
- S/MIME

Chứng thực điện tử

- Xác thực người dùng bằng eToken
- Chữ kí số: Khai báo thuế qua mạng, Code Signing, Chống chối bỏ trong các hệ thống quản lý công việc điện tử

.....

- .....

31

Một số ứng dụng thực tế của mật mã

Bạn biết ứng dụng nào nữa?

32

1. Nội dung khóa học
2. Tổng quan về các thuật toán mật mã
3. **Một số vấn đề khác trong mật mã**
4. Bài tập lớn, tiểu luận

Một số vấn đề khác trong mật mã

- Thiết kế các hệ mật an toàn
- Các phương pháp thám mã
- Cài đặt các hệ mật an toàn
  - Cài đặt hiệu quả bằng phần mềm
  - Cài đặt hiệu quả bằng phần cứng
  - Lược đồ mật mã chống lại tấn công lên thuật toán
  - Lược đồ mật mã chống lại tấn công kênh kề
- Sinh khóa tốt
  - Sinh số ngẫu nhiên
  - Sinh số giả ngẫu nhiên
  - Sinh số nguyên tố
- Trao đổi khóa an toàn
- Nghiệp vụ mật mã
- Ứng dụng mật mã
- Luật pháp, chính sách, tiêu chuẩn về mật mã

34

1. Nội dung khóa học
2. Tổng quan về các thuật toán mật mã
3. Một số vấn đề khác trong mật mã
4. **Bài tập lớn**