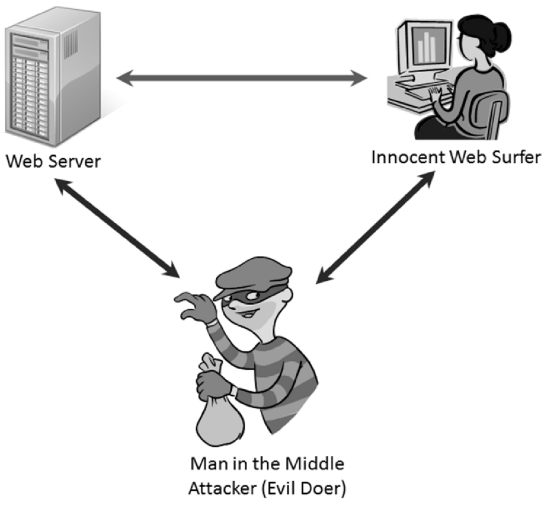
Chương 2

MÃ HOÁ VÀ CHỮ KÝ SỐ

TS. Phan Thượng Cang
CIT - CTU
2019

Thông tin trên đường truyền



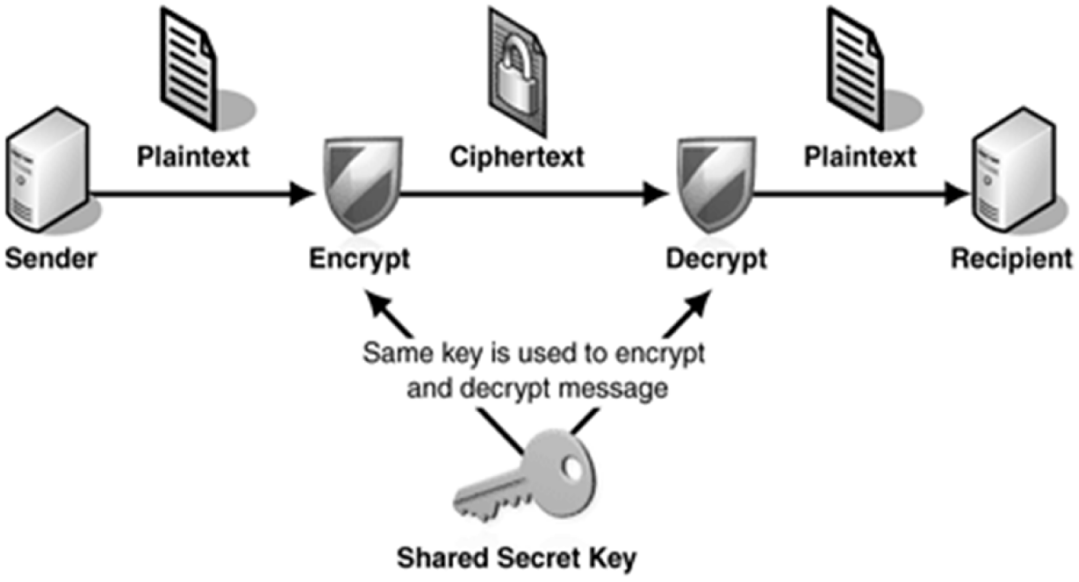
Các khái niệm mã hoá

- Văn bản gốc (plaintext) là văn bản ban đầu có nội dung có thể đọc được và cần được bảo vệ.
- Văn bản mã hóa (ciphertext) là văn bản sau khi mã hóa, nội dung không thể đọc được.
- Mã hóa (encryption) là quá trình chuyển văn bản gốc thành văn bản mã hóa. Giải mã (decryption) là quá trình đưa văn bản mã hóa về lại văn bản gốc ban đầu
- Hệ thống mã hóa (cryptosystem)

  Cryptosystem = encryption + decryption algorithms
- Khóa (key) được sử dụng trong quá trình mã hóa và giải mã

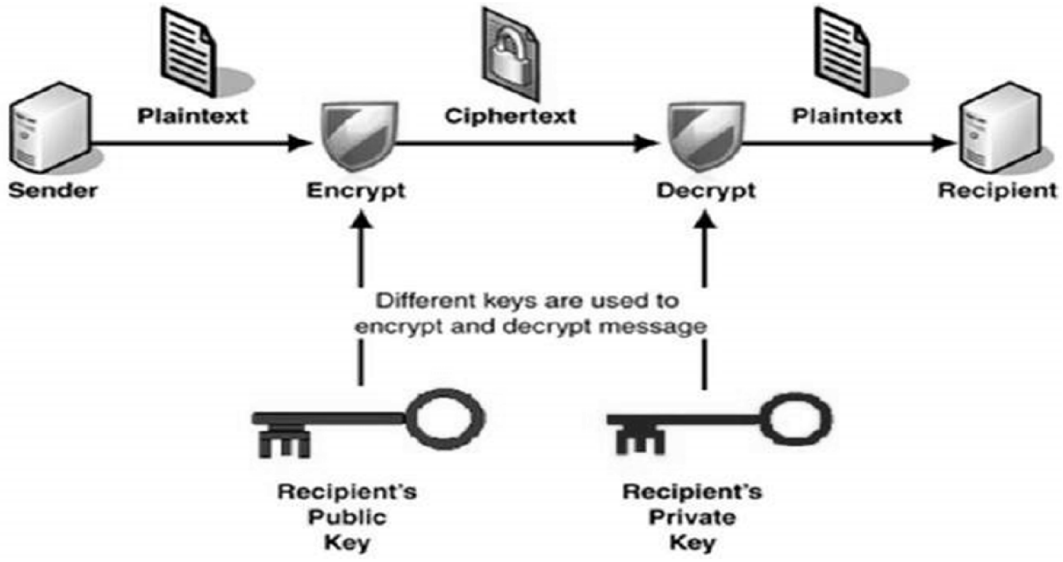
Mã hoá đối xứng

- Mã hóa đối xứng (symmetric cryptography) là mã hóa sử dụng một khóa bí mật chia sẻ (sharedsecret-key) cho cả hai quá trình mã hóa và giải mã. Các kỹ thuật mã hóa đối xứng thông dụng: DES(Data Encryption Standard), Triple DES, AES



Mã hoá bất đối xứng

- Mã hóa bất đối xứng (Asymmetric cryptography) là mã hóa sử dụng một khóa công khai (public key) và một khóa bí mật (private key) cho quá trình mã hóa và giải mã. Nó còn được gọi là hệ thống mã hóa khóa công khai (public-key cryptography). Kỹ thuật mã hóa bất đối xứng phổ biến: RSA



Ưu và nhược điểm các kỹ thuật mã hoá

- Kỹ thuật mã hóa đối xứng có tốc độ mã hóa và giải mã nhanh hơn so với mã hóa bất đối xứng. Nó phù hợp mã hóa dữ liệu nhỏ (Mã hóa khóa bí mật, mật khẩu, …)

- Kỹ thuật mã hóa bất đối xứng an toàn hơn so với mã hóa đối xứng. Nó phù hợp mã hóa dữ liệu lớn (Mã hóa dữ liệu)

- Thực tế, sử dụng kết hợp cả hai kỹ thuật

Kỹ thuật mã hoá bất đối xứng RSA (Ron Rivest, Adi Shamir và Len Adleman)

A - Quy trình tạo khóa công khai (public key) và khóa cá nhân (private key):

1.Chọn 2 số nguyên tố lớn ngẫu nhiên (trên 1024 bits), p và q.

2.Tính **n** = p * q . Hiện máy tính chưa thể tìm p,q lớn khi biết n.

3.Chọn **e** là một số nguyên tố, sao cho UCLN{ e, (p-1)*(q-1)} = 1 Điều này đảm bảo cho d ở bước 4 luôn tồn tại.

4.Tìm **d** sao cho d*e mod {(p-1)(q-1)} = 1.
Nghĩa là, d = (1+ k {(p-1)(q-1)})/e. Hoặc dùng Euclid mở rộng.

5.Cặp (e, n) chính là public key, (d, n) là private key. Ta không cần dùng tới 2 số p, q và có thể xóa bỏ chúng.

Kỹ thuật mã hoá bất đối xứng RSA

B - Quy trình mã hoá: $C = m^e \bmod n$

C - Quy trình giải mã: $m = c^d \bmod n$

Trong đó:
- m là thông điệp ban đầu
- e, n là public key
- c là dữ liệu đã được mã hoá
- d là private key thường là một số rất lớn, tích của 2 số nguyên tố, và được giữ an toàn tuyệt đối

Ví dụ 1 - RSA

$$C = m^e \bmod n$$
$$m = c^d \bmod n$$

p = 3, q = 11
$\Rightarrow$n = pq = 33
$\Rightarrow\varphi(n) = (p-1)(q-1) = 20$

- chọn e = 7 vì UCLN(7, 20) = 1, (chọn 0<e<20, e là số nguyên tố không chia hết 20)
- chọn d = 3 vì (dx7) mod 20 =1 => d = (1+k*20) /7 => d=3 (k=1)

Giả sử m = 6 (alt+6), mã hóa m và thu được:
c = 6 ^ 7 % 33 =30
Giải mã c để thu được m:
m = 30 ^ 3 % 33 = 6

Ví dụ 2 - RSA

$$C = m^e \bmod n$$
$$m = c^d \bmod n$$

p = 7, q = 19
$\Rightarrow$n = pq = 133
$\Rightarrow\varphi(n) = (p-1)(q-1) = 108$

chọn e = 5 vì UCLN(5, 108) = 1, (chọn e nguyên tố 1, 3, 5,..)

chọn d = 65 vì k=3, d = (1+k*108) /5 = 325/5 = 65

Giả sử m = 32 (dấu cách), mã hóa m và thu được:
c = 32 ^ 5 % 133 = 128

Giải mã c để thu được m:
m = 128 ^ 65 % 133 = 32

Ví dụ 3 - RSA

$$C = m^e \bmod n$$

$$m = c^d \bmod n$$

Ví dụ: p = 61 và q = 53
$n=p*q=61*53=3233$

Tính kết quả hàm số Euler (totient): $\Phi(n)=(p-1)(q-1)$
$\Phi(3233)=(61-1)*(53-1)=3120$

Chọn một số bất kỳ $1<e<3120$ và là số nguyên tố cùng nhau của 3120
=> Chọn e=17

Tính d là nghịch đảo modular của $e(\text{mod}\Phi(n))$:
$d*e \bmod \Phi(n)=d*17 \bmod 3120 =1$

Hoặc là dùng cách brute force để tính d (có thể được vì chúng ta chọn các số nhỏ), hoặc dùng thuật toán Euclid mở rộng, ta có d=2735

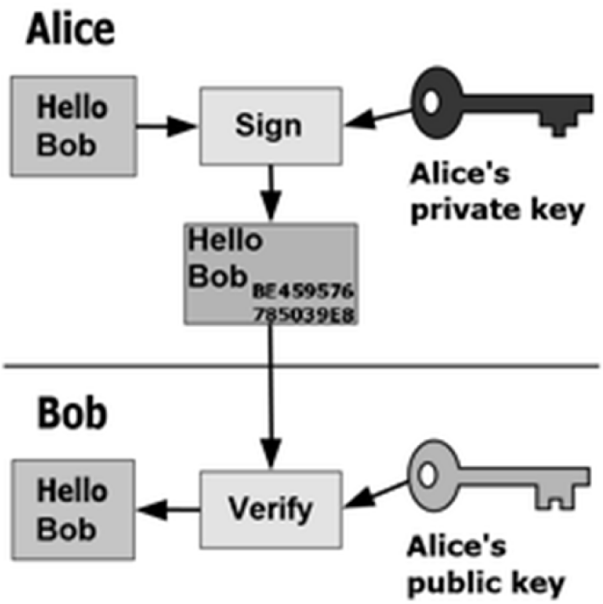
Chữ ký số

- Chữ ký số (Digital signature): là thông điệp (có thể là văn bản, hình ảnh, hoặc video...) đã được ký bằng khóa bí mật của người dùng nhằm mục đích xác định người chủ của thông điệp đó.

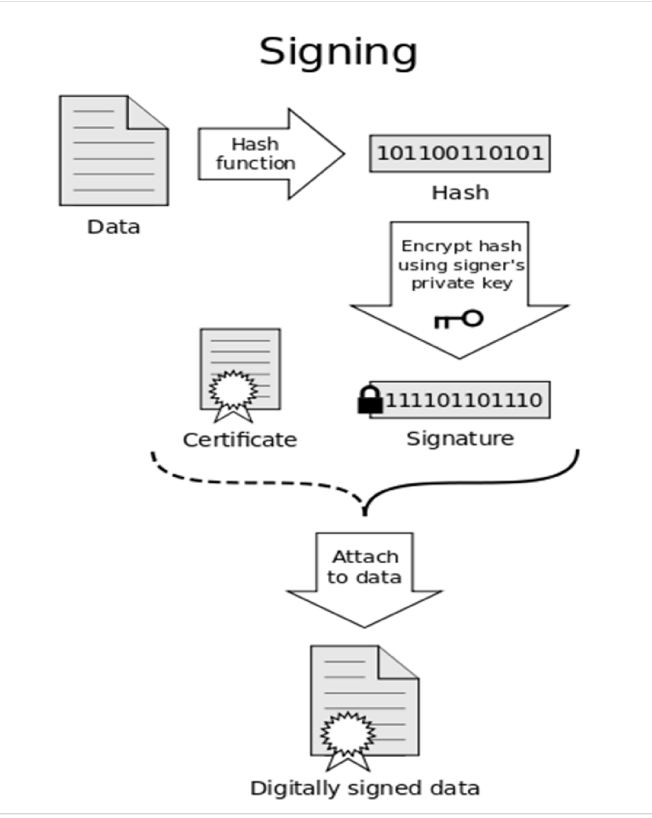
- Mục đích của chữ ký số:
  - Xác thực: xác định ai là chủ của thông điệp
  - Tính toàn vẹn : kiểm tra xem thông điệp có bị thay đổi
  - Tính chống thoái thác: ngăn chặn việc người dùng từ chối đã tạo ra và gửi thông điệp

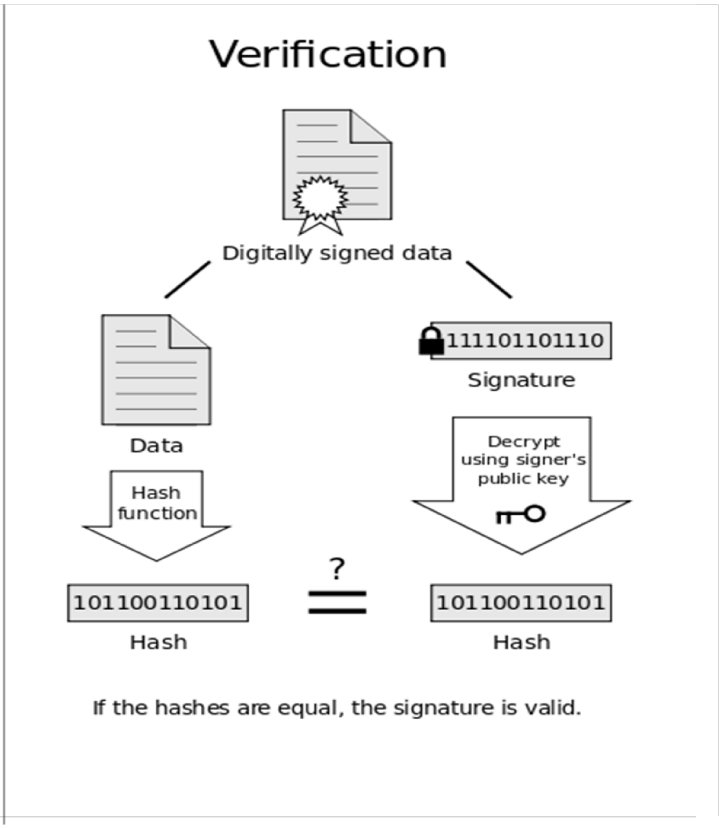
Chữ ký số

- **Thực hiện**:
  - Dùng khóa bí mật để ký (mã hóa) lên thông điệp ⇨ chữ ký
  - Dùng khóa công khai để xác thực (giải mã) chữ ký

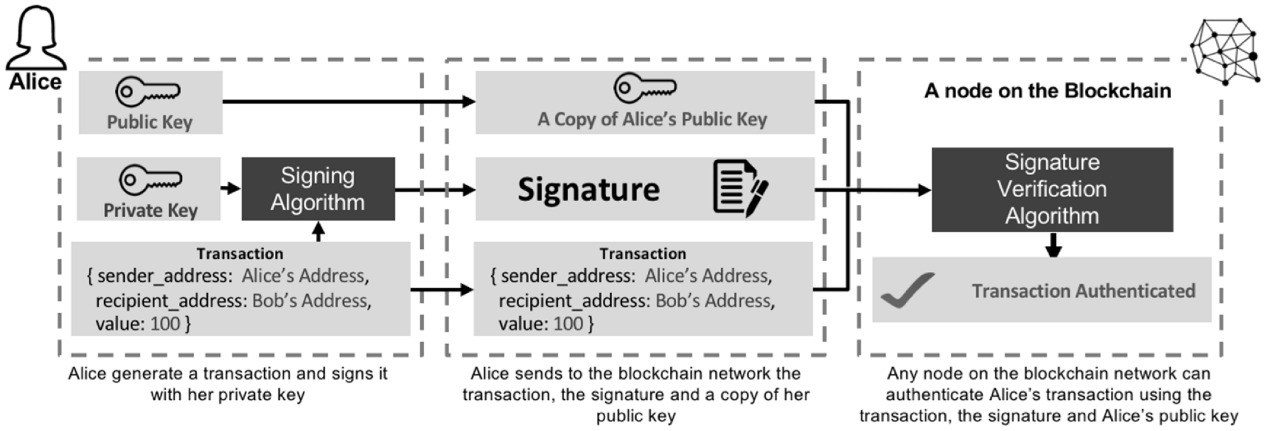


Chữ ký số





Chữ ký số và Blockchain



Authentication Process for Transactions on the Blockchain