ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

TOÁN RỜI RẠC VÀ THUẬT TOÁN

Bài 8

Mật mã học và ứng dụng

(*Cryptography and its applications*)

Nguyễn Thị Hồng Minh
minhnth@gmail.com

Nội dung

1. **Số nguyên tố**
2. **Số học mô đun**
3. **Mật mã học**
   - *Mật mã khóa bí mật, khóa công khai*
   - *Hàm băm*
   - *Chữ kí số*

Chú ý: Hầu hết các hình vẽ trong các bài giảng được sưu tầm từ internet và được trình bày theo quan điểm của giảng viên.

Số nguyên tố

- **Khái niệm**
  - Số nguyên chỉ chia hết cho 1 và chính nó
- **Định lí**
  - Một số nguyên bất kì có thể viết thành tích của các thừa số nguyên tố

Ví dụ:

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$,

$641 = 641$,

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$,

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$

  - Có vô số các số nguyên tố (Rosen Book – P260 Ed7)

Số nguyên tố

- **Định lí Số nguyên tố (Prime Number Theory)**
  - Tỉ lệ giữa số các số nguyên tố nhỏ hơn n và n/log(n) tiến tới 1 khi n lớn

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\log(n)} = 1$$

- **Hệ quả**
  - Xấp xỉ cho số nguyên tố thứ *n*: $p_n \sim n \log(n)$

    (Rosen Book – P262 Ed7)

Số nguyên tố

- **Một số giả thuyết với số nguyên tố**
  - Tồn tại hàm $f(n)$ mà giá trị của nó là số nguyên tố?

    Ví dụ: $f(n) = n^2-n+41$

    $f(1)=41, f(2) =43, f(2)= 47, f(4)=53,\ldots$

    Điều này có ý nghĩa trong mật mã học và các ứng dụng

  - Giả thuyết Goldbach: mọi số nguyên lẻ $n > 5$, là tổng của 3 số nguyên tố.
  - Giả thuyết về cặp số nguyên tố sinh đôi (twin prime): có vô hạn các cặp số nguyên tố sinh đôi (hơn kém nhau 2 đơn vị)

Số nguyên tố

- **Một số nghiên cứu tính toán với số nguyên tố**
  - *Xác định tính nguyên tố của số nguyên*
  - *Sinh số nguyên tố*

The **largest known prime** (1/2018)

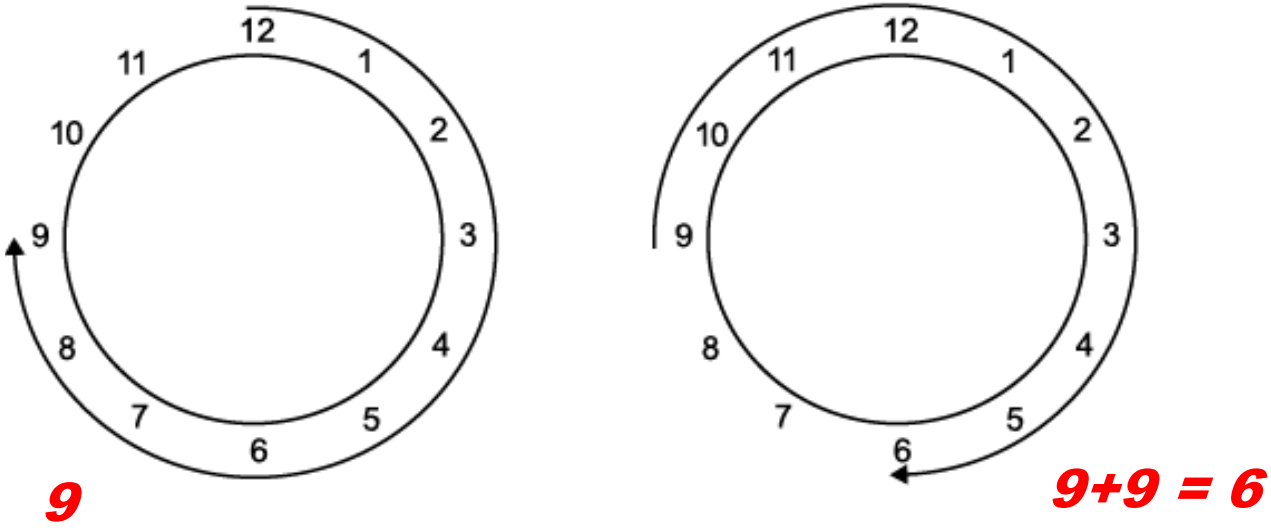
$2^{77,232,917}-1$ (23,249,45 digits)

$2^{82,589,933}-1$ with 24,862,048 digits (7/2018)

https://primes.utm.edu/largest.html

Số học mô đun

- ***Số học mô đun (modulo arithmetic)***



Đồng hồ: modulo 12

Phép modulo: $a \equiv b \pmod{n}$

$\Leftrightarrow \; a = k*n + b$ (k – *số nguyên*)

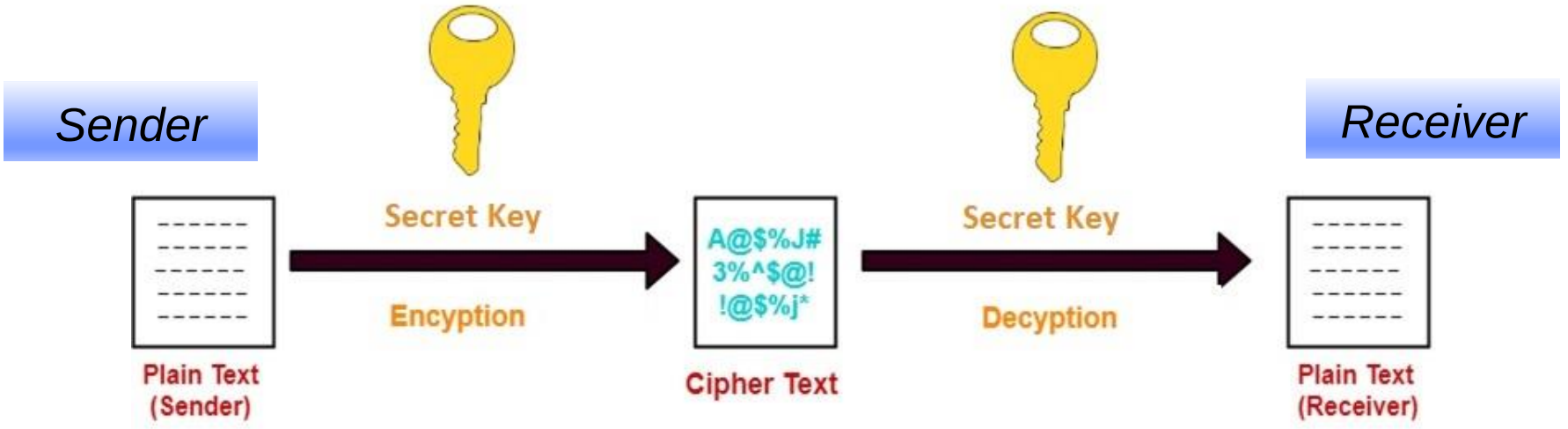
http://inversed.ru/Blog_1.htm

Mật mã học

- **Mật mã (cryptography)**
  - Lĩnh vực đảm bảo an toàn thông tin
  - 2 quá trình: Mã hóa (Encryption), Giải mã (Decryption)
  - Đảm bảo tính chất:
    - Tính bí mật (confidentiality)
    - Tính toàn vẹn (integrity)
    - Tính xác thực (authentication)
    - Tính chống chối bỏ (non-repudiation)

Mật mã học

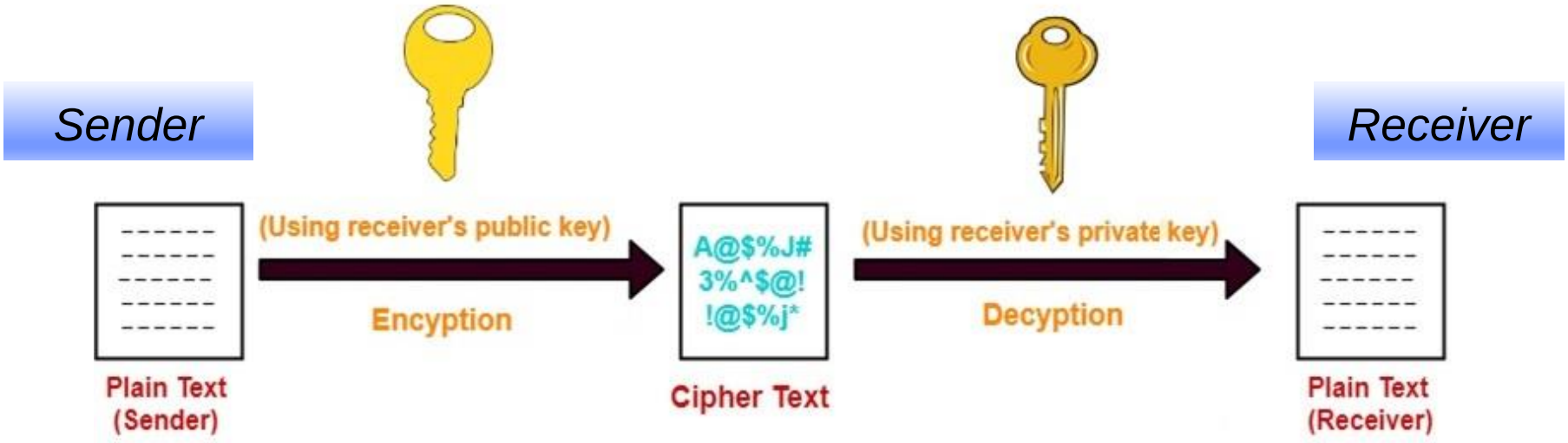
- **Mật mã khóa đối xứng (Symmetric Cryptography)**
  - *Tên gọi khác: Secret/Private Key Cryptography*



  - *2 bên gửi nhận thống nhất thuật toán mã hóa*
  - *Khóa được truyền bí mật giữa 2 bên*

Mật mã học

- **Mật mã khóa bất đối xứng (Asymmetric Cryptography)**
  - *Tên gọi khác: Public Key Cryptography*



  - *Mã hóa và giải mã dùng 2 khóa khác nhau*
  - *Public key (công bố), Private key (bí mật)*

Mật mã học

- **Mật mã khóa bất đối xứng (Asymmetric Cryptography)**
  - **Hệ mã RSA (The RSA Cryptosystem) - 1977**
    - Ronald Rivest (1948, USA); Adi Shamir (1952, Israel), Leonard Adleman (1945, USA)
    - Mã hóa công khai với 2 khóa (K_u,K_r). Trong đó:
      - K_u – public, K_r – private, có mối quan hệ, nhưng không thể suy ra nhau (*sử dụng hàm một chiều phân tích số thành thừa số nguyên tố*).
      - 1 khóa dùng mã hóa, 1 khóa dùng giải mã.
      - Mã hóa bí mật (chỉ gửi cho người nhận), mã hóa chứng thực (nhiều người nhận xác thực).

Mật mã học

- **Mật mã khóa bất đối xứng (Asymmetric Cryptography)**
  - Thuật toán RSA

Sinh khóa

1. Chọn 2 số nguyên tố lớn p,q
2. Tính $N = p.q$; $n = (p-1)(q-1)$
3. Chọn số u (nhỏ) sao cho:
   $\gcd(u,n) = 1$
4. Tính số r sao cho:
   $r.u \equiv 1 \pmod n$ $(r.u)\%n=1$
5. Public key: $K_u = (u,N)$
   Private key: $K_r = (r,N)$

Mã hóa và giải mã (M ⇨ C ⇨ M)

6. Mã hóa : $C = E(M,K_u) = M^u \bmod N$
7. Giải mã: $M = D(C,K_r) = C^r \bmod N$

Mật mã học

- **Mật mã khóa bất đối xứng (Asymmetric Cryptography)**
  - Thuật toán RSA

Sinh khóa

1. Chọn 2 số nguyên tố lớn p,q
2. Tính N = p.q; n = (p-1)(q-1)
3. Chọn số u (nhỏ) sao cho:
   gcd(u,n) = 1
4. Tính số r sao cho:
   $r.u \equiv 1 \pmod n$ (r.u)%n=1
5. Public key: K_u =(u,N)
   Private key: K_r =(r,N)

Ví dụ:

p=11; q=3

N=33;n=20

u=3; r=7

Public key:

K_u=(u,N)=(3,33)

Private key

K_r=(r,N)=(7,33)

Mã hóa và giải mã (M ⇨ C ⇨ M)

6. Mã hóa : $C = E(M,K_u) = M^u \bmod N$
7. Giải mã: $M = D(C,K_r) = C^r \bmod N$

Mật mã học

❖ Mật mã khóa bất đối xứng (Asymmetric Cryptography)

- Thuật toán RSA

Sinh khóa

1. Chọn 2 số nguyên tố lớn p,q
2. Tính $N = p.q$; $n = (p-1)(q-1)$
3. Chọn số u (nhỏ) sao cho:
   $\gcd(u,n) = 1$
4. Tính số r sao cho:
   $r.u \equiv 1 \pmod n$ $(r.u)\%n=1$
5. Public key: $K_u = (u,N)$
   Private key: $K_r = (r,N)$

Ví dụ:

p=11; q=3

N=33;n=20

u=3; r=7

Public key:

$K_u=(u,N)=(3,33)$

Private key

$K_r=(r,N)=(7,33)$

Mã hóa và giải mã (M ⇨ C ⇨ M)

6. Mã hóa : $C = E(M,K_u) = M^u \bmod N$
7. Giải mã: $M = D(C,K_r) = C^r \bmod N$

Mã hóa: M=25

$C = E(M,K_u) = (25^3)\%33 = 16$

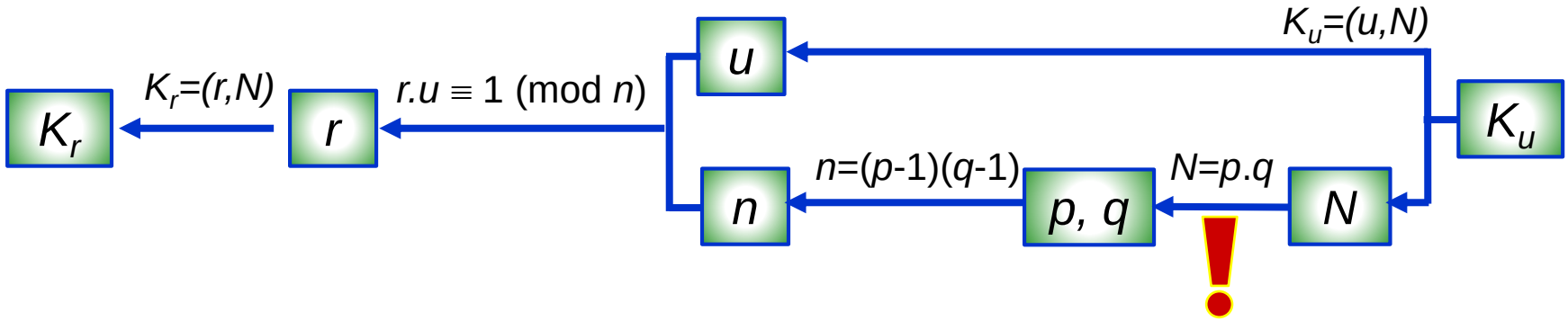
Giải mã:

$D(C,K_r) = (16^7)\%33 = 25 = M$

Mật mã học

- **Mật mã khóa bất đối xứng (Asymmetric Cryptography)**
  - **RSA đảm bảo nguyên tắc mã hóa**
    - ✓ Bản giải mã là bản rõ ban đầu

- ✓ Không thể (khó) thám mã: $K_u \not\leftrightarrow K_r$



Mật mã học

- **Hàm băm (Hash Function)**
  - *Mã hóa một chiều (không giải mã)*

Dữ liệu
Độ dài bất kì

Hàm băm

Giá trị băm
Chuỗi độ dài nhất định

Mật mã học

- **Hàm băm (Hash Function)**
  - Tính chất:
    - Dữ liệu giống nhau cho giá trị băm giống nhau
    - Dữ liệu khác nhau cho giá trị băm khác nhau
    - **Không thể** khôi phục giá trị băm về dữ liệu ban đầu
  - Sử dụng
    - Hash function để kiểm tra tính toàn vẹn/đúng của dữ liệu
  - Một số thuật toán băm
    - MD (Message Digets): MD2, MD4, MD5 (128bits)
    - SHA (Secure Hash Algorithm): SHA-1 (160bits), SHA-256 (256bits), SHA-384, SHA-512 (512bits)
    - *https://emn178.github.io/online-tools/sha256.html*

Mật mã học

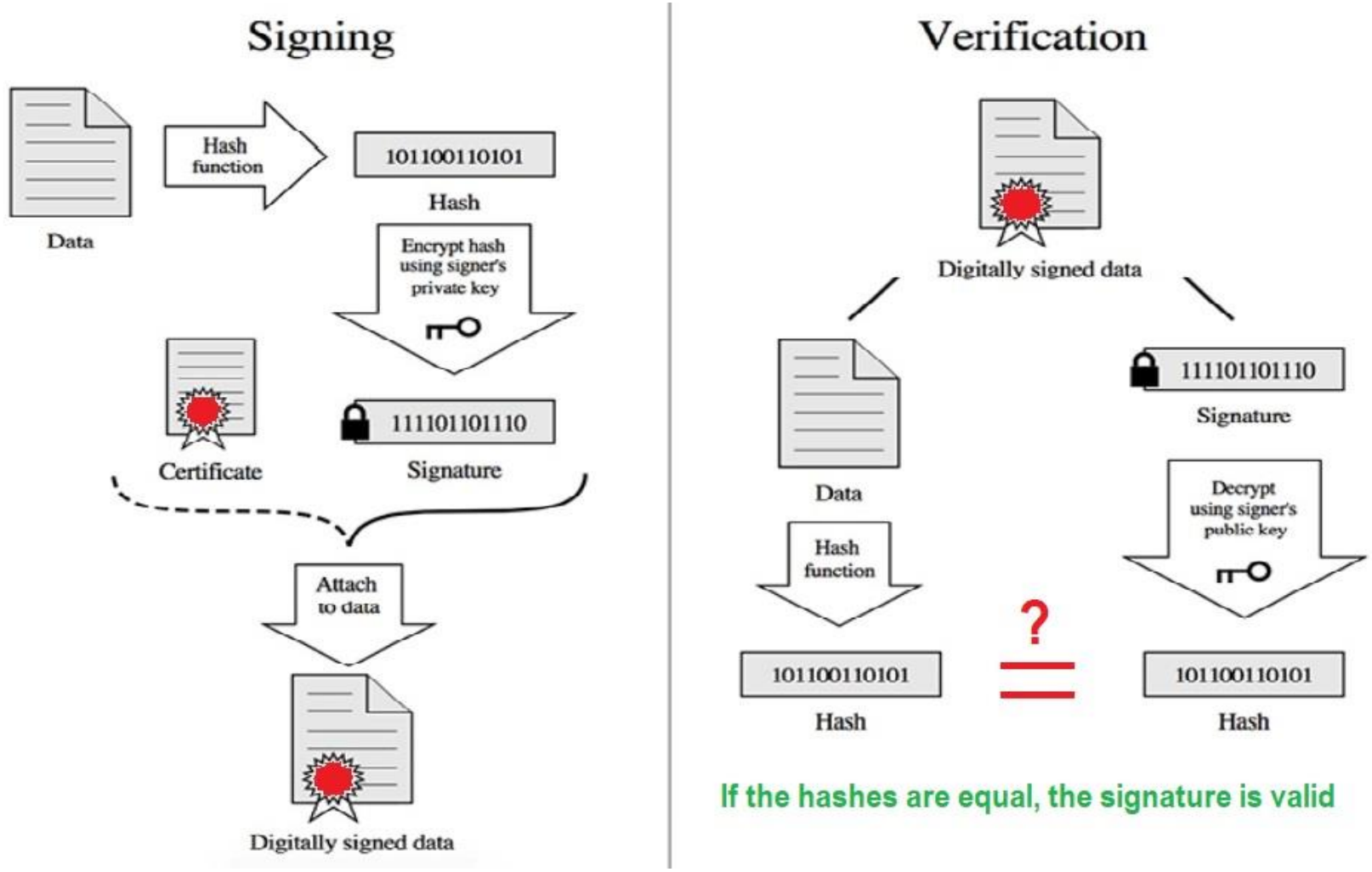
- **Hàm băm (Hash Function)**
  - Ứng dụng
    - Quản lí mật khẩu
    - Đấu giá trực tuyến
    - Kiểm tra file được truyền/tải đúng bản gốc
    - Chữ kí số

Mật mã học

- **Chữ kí số (digital signature)**
  - Đoạn dữ liệu số đặc trưng được đính kèm vào thông điệp phục vụ cho xác thực. Kết hợp *hash* và *cryptography*
  - Tính chất:
    - Là đặc trưng duy nhất cho mỗi thông điệp (tài liệu)
    - Không thể giả mạo: Có cơ chế phát hiện sự giả mạo.
    - Không thể chối bỏ: Có cơ chế phát hiện tác giả của chữ ký.
  - Quy trình
    - Người gửi kí (signing) – khóa bí mật (mã hóa chứng thực)
    - Người nhận giải mã, xác thực (verification) – khóa công khai

Mật mã học

- **Chữ kí số (digital signature)**



Vấn đề nghiên cứu thêm

- **Mật mã học trong công nghệ blockchain**
  - **Lý thuyết, công nghệ kết hợp trong blockchain**
    - Mật mã học
    - Mạng và truyền thông
    - Trò chơi
  - **Blockchain từ các góc nhìn**
    - Business: Cơ sở dữ liệu chứa đựng tài sản, có giao dịch
    - Kĩ thuật: Phương thức bất biến lưu trữ lịch sử giao dịch
    - Xã hội: Thiết lập thể chế mới về niềm tin, sự đồng thuận