

# AN TOÀN VÀ BẢO MẬT HỆ THÔNG THÔNG TIN

Giáo viên: Trần Hồng Diệp

Bộ môn: Tin học

Email: [diepth18@yahoo.com](mailto:diepth18@yahoo.com)  
[diepth18@gmail.com](mailto:diepth18@gmail.com)



# Mật mã khóa công khai (PKC)

Còn được gọi là mật mã bất đối xứng.

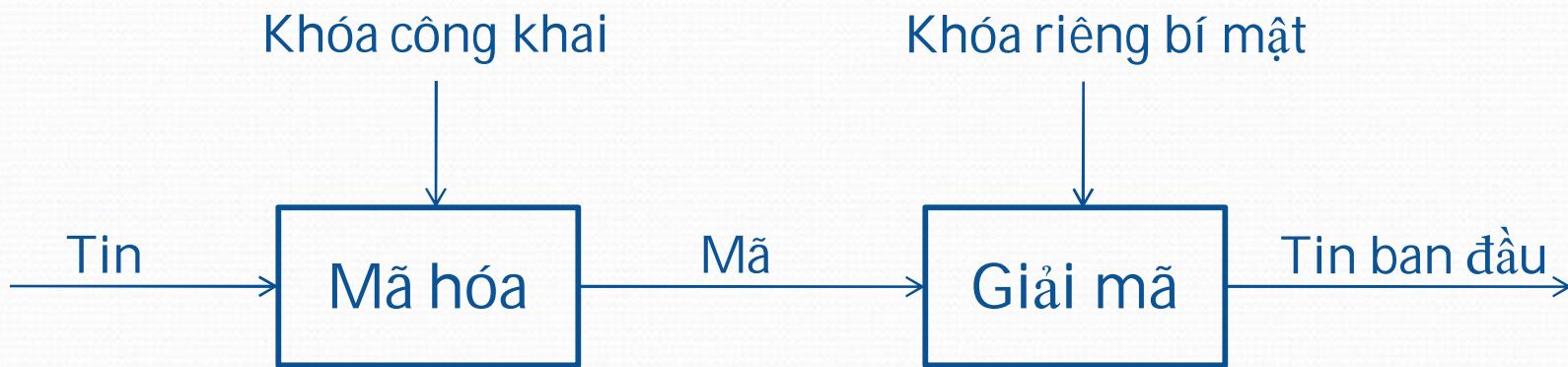
Mô hình mã hóa và giải mã:

- Mã hóa dùng khóa công khai k:

$$C = E (k, C)$$

- Giải mã dùng khóa riêng bí mật K:

$$M = D (K, C)$$



# Tại sao cần mật mã khóa công khai

- Điểm yếu của mã khóa bí mật:
  - N người dùng thì cần  $N^*(N-1)/2$  khoá, lượng người dùng càng tăng thì số lượng khoá càng lớn → khó khăn quản lý khoá
  - Do mã đối xứng nên không có tính năng chống phủ nhận (không thiết lập được chữ ký điện tử)
  - Nếu sử dụng trọng tài → quá tải truyền tin và tốc độ xử lý (bottleneck)
- Các hệ mật mã khóa công khai
  - Khoá mã được gắn liền với từng người dùng
  - Mỗi người dùng có 2 khoá:
    1. Khoá công khai dùng để sinh mã
    2. Khoá bí mật để giải mã

# Mật mã khóa công khai

- Lý thuyết nền tảng
  - Độ phức tạp
  - **Số học đồng dư**
- Các hệ mật mã khóa công khai
  - RSA
  - MerkleHellman
  - ElGamal
  - Rabin
  - ...

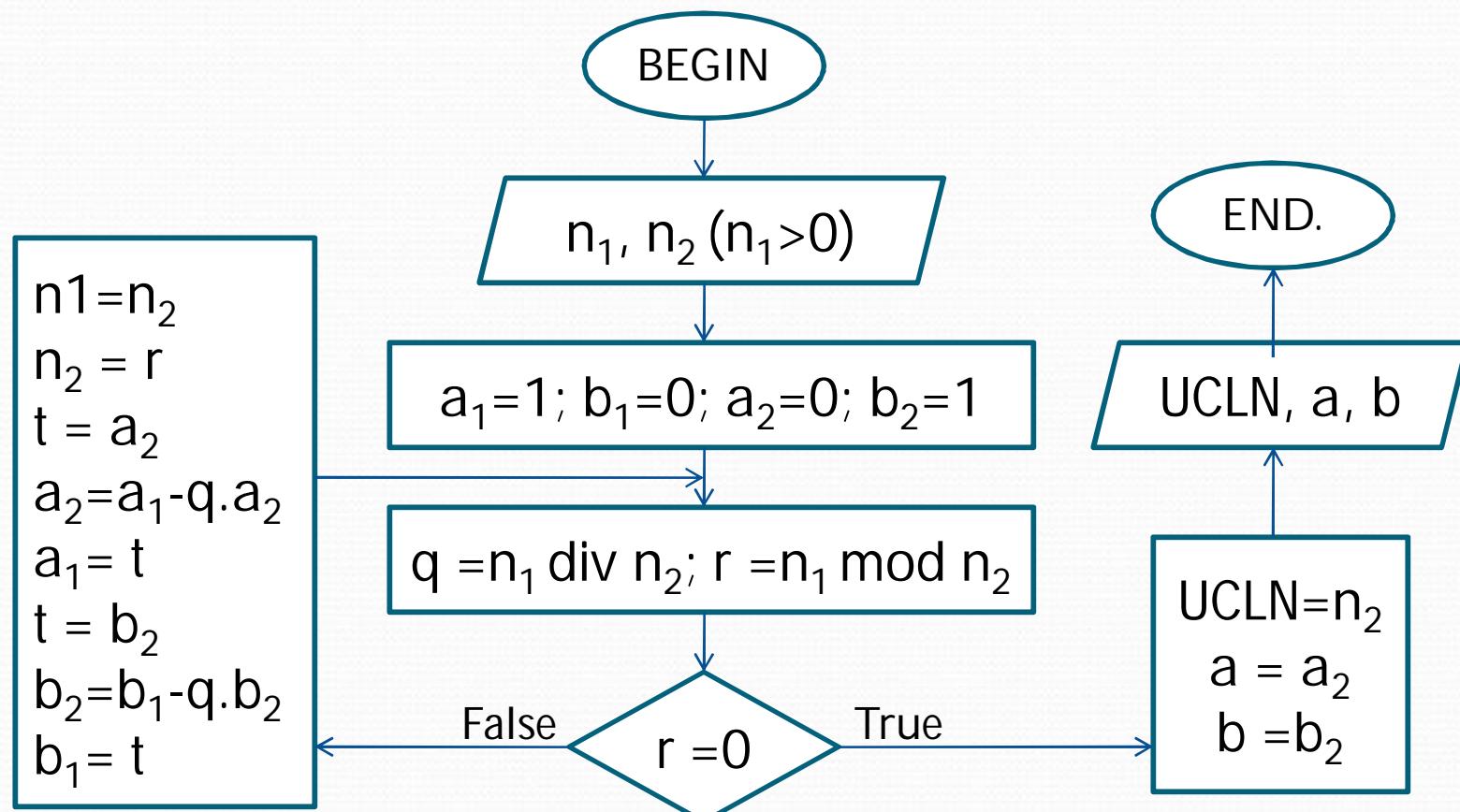
# 1. Nguyên tắc cấu tạo một hệ PK

- Trên cơ sở hàm một chiều (*one – way*):
  - Đối với mọi  $X$ , dễ dàng tính ra  $Y=f(X)$
  - Biết  $Y$  khó khăn để tìm ra  $X$
  - Ví dụ: cho các số nguyên tố  $p_1, p_2, \dots, p_n$ , có thể dễ dàng tìm ra  $N=p_1 \times p_2 \times \dots \times p_n$ , nhưng nếu biết  $N$  thì khó tìm ra các  $p_i$ , nếu các  $p_i$  càng lớn càng khó tìm
- Hàm một chiều có tính chất đặc biệt kiểu cửa bẫy (*Trap-door*):
  - Nếu biết giá trị được gọi là bẫy thì lại tính được  $X$  dễ dàng từ  $f(X)$

## 2. Thuật toán tìm giá trị nghịch đảo theo modul đồng dư

- Còn được gọi là thuật toán Euclidean mở rộng.
  - Thực hiện tìm ước số chung lớn nhất của hai số  $n_1$  và  $n_2$
  - Trong quá trình tìm  $\text{UCLN}(n_1, n_2)$  thì tìm luôn hai giá trị  $a$  và  $b$  sao cho  $\text{UCLN}(n_1, n_2) = a \cdot n_1 + b \cdot n_2$
  - Nếu  $\text{UCLN}(n_1, n_2) = 1$  thì  $a \cdot n_1 + b \cdot n_2 = 1$  như vậy  $n_1$  chính là nghịch đảo của  $a$  theo modul  $n_2$

# Sơ đồ thuật toán tìm giá trị nghịch đảo theo modul đồng dư



# Bảng tính giá trị nghịch đảo theo modul đồng dư

- Ví dụ: Tìm nghịch đảo của 11 theo modul 39:

n1	n2	r	q	a1	b1	a2	b2
39	11	6	3	1	0	0	1
11	6	5	1	0	1	1	-3
6	5	1	1	1	-3	-1	4
5	1	0	5	-1	4	2	-7

### 3. Hệ mật mã khóa công khai RSA

- Tác giả: Rivest, Shamir và Adleman
- Là hệ PK phổ biến và đa năng nhất trong thực tế
- Dựa trên độ khó bài toán phân tích một số lớn ra thừa số nguyên tố
- Bí mật
- Xác thực
- Chống phủ nhận

# RSA – Sinh khoá

- Chọn ngẫu nhiên hai số nguyên tố lớn (thường thực tế khoảng 100 chữ số): p và q
  - 1. Tính  $n = p * q$
  - 2. Tính  $m = (p-1) * (q-1)$
- Chọn e sao cho
  - 1.  $1 \leq e \leq m-1$
  - 2.  $\text{UCLN}(e, m)=1$
- Chọn d sao cho
  - 1.  $1 \leq d \leq m-1$
  - 2.  $e * d \text{ mod } m = 1$
- Khoá công khai:  $(n, e)$
- Khoá bí mật:  $(p, q, d)$

# RSA – Sinh khoá

## □ Ví dụ:

- $p = 11; q = 23$
- $n = 11 * 23 = 253; m = (11-1) * (23-1) = 220$
- Chọn  $e = 3$
- Tìm  $d$  bằng thuật toán Euclide mở rộng sao cho  $e * d \equiv 1 \pmod{220}$ :  
 $d=147$

# RSA – Mã hóa

- Bẻ tin gốc thành nhiều đoạn cùng có độ dài  $u$  bit sao cho:  $2^u \leq m-1$
- Mã hóa từng đoạn:  
$$Y = X^e \text{ mod } n$$
- Ví dụ:  
Tin  $X = 1011010_2 = 165_{10}$  ( $u=7$ ;  $2^7 \leq 220-1$ )  
Mã  $Y = 165^3 \text{ mod } 253 = 110 = 1101110_2$

# RSA – Giải mã

- Giải mã từng đoạn độ dài u:

$$X = Y^d \bmod n$$

- Ví dụ:

$$\text{Mã } Y = 1101110_2 = 110_{10}$$

$$\text{Tin } X = 110^{147} \bmod 253 = 165_{10} = 1011010_2$$

# RSA – Độ an toàn

- Độ an toàn của RSA phụ thuộc vào độ khó của bài toán phân tích thừa số nguyên tố  $p, q$  từ  $n$
- Lựa chọn  $p, q$ :
  - $p, q$  lớn, tối thiểu 512 bit
  - $p, q$  xấp xỉ nhau
  - Tránh trường hợp đặc biệt làm bài toán trở nên dễ dàng hoặc nhiều tin không thay đổi khi mã hóa (bị “phơi tin”)
- Lựa chọn  $e$ :
  - $e$  nhỏ nhất có thể
  - $e$  không nhỏ quá, để tránh tấn công để tránh tấn công bằng thống kê
- Lựa chọn  $d$ :
  - $d$  không quá nhỏ để tránh tấn công vét cạn

# Cảm ơn!

