# Mật mã bất đối xứng
# Public key cryptography

# Điểm yếu của mã đối xứng

- Việc phân phối và quản lý khoá khó khăn, nhất là với các hệ thống có nhiều người sử dụng
  - N người dùng ➔ n(n-1)/2 mối quan hệ ➔ mỗi người cần quản lý (n-1) khoá
- Không thể sử dụng vào chữ ký điện tử
  - Không thể đảm bảo được tính "không chối từ" (sẽ học ở các buổi sau)

# Ý tưởng của Diffie-Hellman về hệ mã bất đối xứng (mã công khai)

- Về nguyên tắc, mã công khai được thiết kế trên quan điểm "hướng tới 1 người dùng", chứ không phải hướng tới 1 cặp người dung (như mã bí mật)
  - Được sử dụng với nhiều mục đích khác ngoài việc mã hoá
- Đề xuất bởi Diffie và Hellman (1976) trong bài báo "New Directions in Cryptography"
  - Cơ chế mã hoá
  - Cơ chế phân phối khoá
    - Thuật toán phân phố khoá Diffie-Hellman
  - Chữ ký điện tử

# Đề xuất của Diffie-Hellman

- Mỗi người dùng tạo 2 khoá: 1 khoá giữ bí mật (secret (private) key) và 1 khoá công khai cho tất cả mọi người khác (public key)
  - Khóa bí công khai được dùng để mã hoá, khoá bí mật được dung để giải mã

    $X = D(z, E(Z, X))$
  - Khóa bí mật được dùng để tạo chữ ký điện tử, khoá công khai được dùng để xác thực chữ ký điện tử

    $X = E(Z, D(z, X))$
- Mã công khai còn được gọi là mã bất đối xứng (asymmetric key cryptosystems)
  - Kể cả biết được bản mã (cipher text) và khoá công khai (public-key) thì cũng không thể tính ngược lại được bản rõ và khoá bí mật

# Hệ mã công khai RSA

- Phát minh năm **1978** bởi **R**ivest, Adi **S**hamir and Leonard **A**dleman
  - Được công bố bởi R L Rivest, A Shamir, L Adleman, "*On Digital Signatures and Public Key Cryptosystems*",Communications of the ACM, vol 21 no 2, pp120-126, Feb 1978
  - Tính an toàn được dựa trên độ khó của bài toán phân tích thừa số nguyên tố của một số rất lớn

# Ý tưởng chính

- Thuật toán mã hoá và giải mã là các hàm đông fduw của các luỹ thừa trong trường $Z_n = \{0,1,2,..n-1\}$
  - Mã hoá : $Y \equiv X^e \ (mod\ n)$
  - Decryption: $X \equiv Y^d \ (mod\ n)$
  - Để đảm bảo tính đúng đắn của thuật toán
    - e & d phải thoả mãn: $X^{ed} \equiv X \ (mod\ n)$

# Ý tưởng chính

- Định lý Euler: $X^{\varphi(n)} \equiv 1\ (mod\ n)$
  - $\varphi(n)$: số lượng các số $k$: $0 < k < n |\ (k, n) \equiv 1\ (mod\ n)$
  - Nếu $n = p \times q$ ($p, q$ nguyên tố) → $\varphi(n) = (p-1)(q-1)$
- Chọn $e$ và tìm $d$ sao cho $ed \equiv 1 (mod\ \varphi(n))$
  - $d \equiv e^{-1} (mod\ \varphi(n))$
  - $X^{ed} \equiv X^{k\varphi(n)+1} \equiv (X^{\varphi(n)})^k \times X \equiv X\ (mod\ n)$
- Chú ý: để giải mã được → cần biết $\varphi(n)$ → cần biết $p, q$ → vì $n$ rất lớn nên việc phân tích $n$ để tìm $p, q$ là không khả thi

# Hệ mã RSA

- **Tạo khoá:**
  - Chọn 2 số nguyên tố rất lớn và có độ lớn tương đương (~512 bit): $p, q$
  - Tính $n = pq$, và $\varphi(n) = (q-1)(p-1)$
  - Chọn 1 số tự nhiên $e$ tuỳ ý, sao cho $1 < e < \varphi(n)$, và $\gcd(e, \varphi(n)) = 1$
  - Tìm $d$, sao cho $1 < d < \varphi(n)$ và $ed \equiv 1 \, mod \varphi(n)$
  - **Khoá công khai : $(e, n)$; khoá bí mật : $d$**
    - **Chú ý: $p$ và $q$ phải giữ bí mật**

# Hệ mã RSA

- **Mã hoá**
  - Cho trước bản rõ $M$ biểu diễn dưới dạng nhị phân → convert M sang hệ cơ số 10: $0 < M < n$
  - Dùng khoá công khai $(e, n)$ và mã hoá:

    $C = M^e \ (mod\ n)$
- **Giải mã**
  - Cho bản mã $C$, sử dụng khoá bí mật $(d)$ và giải mã:
    - $M = C^d \ (mod\ n)$
- Tính đúng đắn
  - $C^d \ (mod\ n) \equiv M^{ed} (mode\ n) \equiv M (mod\ n)$

# Ví dụ

- Parameters:
  - Select $p = 11$ và $q = 13$
  - $n = 11 * 13 = 143$; $m = (p-1)(q-1) = 10 * 12 = 120$
  - Chọn $e = 37$ ➔ $\gcd(37,120) = 1$
  - Tìm $d$ sao cho: $e \times d \equiv 1 \ (mod\ 120)$ ➔ $d = 13$ $(e \times d = 481)$
- Mã hoá
  - Cắt bản rõ thành các đoạn $u$ bits, $2^u \leq 142$ ➔ $u = 7$
    - Mỗi đoạn sẽ là 1 số tự nhiên từ 1 đến 127
  - Tính $Y = X^e (mod\ n)$

  Ví dụ: $X = (0000010) = 2$, ta có $Y \equiv X^{37} \equiv 12 \ (mod\ 143)$ ➔ $Y = (00001100)$
- Giải mã: $X \equiv 12^{13} (mod\ 143) = 2$

# Cách tính nghịch đảo đồng dư

- Định lý Bézout: nếu $d = GCD(a, b)$ thì tồn tại 2 số $x, y$ sao cho $d = xa + yb$ (đồng nhất thức Bézout), $x, y$ được gọi là hệ số của $a, b$
- Nếu $1 = GCD(e, n) \rightarrow 1 = xe + yn \rightarrow xe \equiv 1(mod\ n) \rightarrow x \equiv e^{-1}(mod\ n)$
- Phương trình Diophantine: $ax+by=c$
  - Chỉ có nghiệm khi $c : d = \gcd(a, b)$

# Cách tính nghịch đảo đồng dư

- Thuật toán Ơclit tìm ước số chung lớn nhất của 2 số $r_0, r_1$

$$
\begin{aligned}
r_0 &= q_1 r_1 + r_2, && 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3, && 0 < r_3 < r_2 \\
&\vdots \\
r_{m-2} &= q_{m-1} r_{m-1} + r_m, && 0 < r_m < r_{m-1} \\
r_{m-1} &= q_m r_m.
\end{aligned}
$$

  - Chứng minh được: $\gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{m-1}, r_m) = r_m$

# Cách tính nghịch đảo đồng dư

- Ví dụ
  - Tìm ước số chung lớn nhất của (252, 198)

$$252 = 198 \times 1 + 54$$
$$198 = 54 \times 3 + 36$$
$$54 = 36 \times 1 + 18$$
$$36 = 18 \times 2 + 0$$

⇒ Gcd(252, 198) = 18

# Cách tính nghịch đảo đồng dư

- Ví dụ
  - Giải phương trình nghiệm nguyên: $252x+198y=18$

$$252 = 198 \times 1 + 54$$
$$198 = 54 \times 3 + 36$$
$$54 = 36 \times 1 + 18$$
$$36 = 18 \times 2 + 0$$

$$18 = 54 - 36$$
$$18 = 54 - (198 - 54 \times 3)$$
$$18 = 54 \times 4 - 198$$
$$18 = (252 - 198) \times 4 - 198$$
$$18 = 252 - 198 \times 5$$

$$(x, y) = 1, -5$$

# Cách tính đồng dư luỹ thừa

- Tính $x^a (mod\ n)$
- Cách đơn giản nhất:
  - $x^a\ (mod\ n) = x\ (mod\ n) \times x\ (mod\ n) \times$ ...$\times$ $x\ (mod\ n)$
  - → thực hiện phép lấy đồng dư và phép nhân $a$ lần
- Sử dụng phương pháp **bình phương và nhân**

# Cách tính đồng dư luỹ thừa
# PP: bình phương và nhân

- Biểu diễn $a$ dưới dạng nhị phân: $a = \sum_{i=0}^{l} a_i 2^i$

$z \leftarrow 1$
For $i = l$ down to 0
  $z \leftarrow z^2 \ mod \ n$
  if $a_i = 1$ then
    $z \leftarrow (z \times x) \ (mod \ n)$
  end if
End for
Return $z$

Tìm số dư của $x^{19}$ khi chia cho n
$19 = 16 + 2 + 1 = 2^4 + 2^1 + 2^0 = 10011$
$z \leftarrow 1$
$i = 4: a_4 = 1; z \leftarrow z^2 \times x \equiv 1^2 \times x \equiv x$
$i = 3; a_3 = 0; z \leftarrow z^2 \equiv x^2$
$i = 2; a_2 = 0; z \leftarrow z^2 \equiv x^4$
$i = 1; a_1 = 1; z \leftarrow z^2 \times x \equiv x^8 \times x \equiv x^9$
$i = 0; a_1 = 1; z \leftarrow z^2 \equiv x^{18} \times x \equiv x^{19}$

Tìm số dư của $3^{19}$ khi chia cho 5
$19 = 10011$
$z \leftarrow 1$
$i = 4: a_4 = 1; z \leftarrow 1^2 \times 3 \equiv 3$
$i = 3; a_3 = 0; z \leftarrow 3^2 \equiv -1$
$i = 2; a_2 = 0; z \leftarrow (-1)^2 \equiv 1$
$i = 1; a_1 = 1; z \leftarrow 1^2 \times 3 \equiv 3$
$i = 0; a_1 = 1; z \leftarrow 3^2 \times 3 \equiv -3 \equiv 2$

# Bài tập

1. Tính
   1. $28^{-1} \bmod 75$
   2. $17^{-1}\ mod\ 101$
   3. $357^{-1}\ mod\ 1234$
   4. $3125^{-1}\ mod\ 9987$
2. Chứng minh: $X^{(p-1)(q-1)} \equiv 1\ (mod\ pq)$ với $p, q$ nguyên tố
3. Viết đoạn giả mã của thuật toán tính nghịch đảo đồng dư
4. Chứng minh tính đúng đắn của phương pháp bình phương và nhân
5. Tính
   1. $9726^{3533}\ (mod\ 11413)$

# Bài tập lớn

1. Viết chương trình phá mã thế (1 bảng thế) bằng phương pháp thống kê
2. Viết chương trình phá mã vigenere (mã đã bảng thế)
3. Viết chương trình mã hoá và phá mã RSA như sau
    1. Mã hoá:
        1. Input: bản rõ, khoá công khai $(d, n)$
        2. Bản rõ là 1 văn bản tiếng anh. Mỗi từ được encode theo bảng chữ cái, ví dụ như sau:
            - DOG → $3\times26^2 + 14\times26 + 6 = 2398$
            - CAT → $2\times26^2 + 0\times26 + 6 = 19$
        - Mỗi số (tương ứng với 1 word) trong bản rõ được mã hoá bằng mã RSA với khoá công khai $(d, n)$
            - Áp dụng giải thuật bình phương và nhân để tính đồng dư luỹ thừa
    2. Phá mã
        1. Phân tích $n$ thành tích của 2 thừa số nguyên tố
        2. Tính $\varphi(n)$
        3. Tìm khoá bí mật $e$
            - Áp dụng thuật toán Ơclit mở rộng
        4. Tìm bản rõ
            - Áp dụng giải thuật bình phương và nhân để tính đồng dư luỹ thừa