Nội dung

- Hàm cửa sập
- Hệ mật mã RSA

Hàm cửa sập (Trapdoor functions - TDF)

ĐN: hàm cửa sập $X \longrightarrow Y$ là bộ ba thuật toán hiệu quả (G, F, F^{-1})

- $G()$: thuật toán *ngẫu nhiên* output cặp khóa (pk, sk)
- $F(pk,\cdot)$: thuật toán *đơn định* định nghĩa một hàm $X \longrightarrow Y$
- $F^{-1}(sk,\cdot)$: hàm từ $Y \longrightarrow X$ tính nghịch đảo $F(pk,\cdot)$

Cụ thể: $\forall (pk, sk)$ sinh bởi hàm G

$\forall x \in X$: $F^{-1}(sk, F(pk, x)) = x$

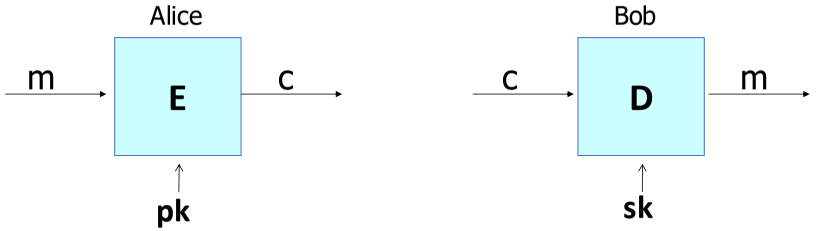
ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Nhập môn An toàn thông tin

Hệ mật mã RSA

Mật mã khóa công khai

Bob: sinh cặp khóa (pk, sk) và đưa pk cho Alice



Xây dựng hệ mật khóa công khai từ TDFs

- (G, F, F^{-1}): TDF an toàn $X \longrightarrow Y$
- (E_s, D_s) : hệ mật mã khóa đối xứng an toàn trên (K,M,C)
- H: $X \longrightarrow K$: hàm băm

Ta xây dựng hệ mật khóa công khai (G, E, D):

Sinh khóa G: giống như G cho TDF

Sử dụng không đúng hàm Cửa sập (TDF)

Không mã hóa bằng cách áp dụng F để mã hóa bản rõ:

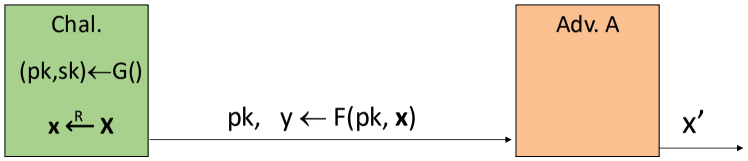
E(pk, m) :
output $c \longleftarrow F(pk, m)$

D(sk, c) :
output $F^{-1}(sk, c)$

Vấn đề:
- Đây là hệ mã đơn định: không an toàn !
- Tồn tại nhiều cách tấn công

Hàm cửa sập an toàn

(G, F, F^{-1}) là an toàn nếu $F(pk, \cdot)$ là hàm "một chiều" :
có thể tính xuôi, nhưng không thể tính nghịch đảo mà không có sk



ĐN: (G, F, F^{-1}) là TDF an toàn nếu với mọi thuật toán hiệu quả A:

$Adv_{OW}[A,F] = Pr[x = x'] <$ "cực nhỏ"

Hệ mật mã khóa công khai từ TDFs

- (G, F, F^{-1}): TDF an toàn $X \longrightarrow Y$
- (E_s, D_s) : hệ mã hóa đối xứng an toàn trên (K,M,C)
- H: $X \longrightarrow K$: hàm băm

E(pk, m) :
$x \longleftarrow_R X$, $y \longleftarrow F(pk, x)$
$k \longleftarrow H(x)$, $c \longleftarrow E_s(k, m)$
output (y, c)

D(sk, (y,c)) :
$x \longleftarrow F^{-1}(sk, y)$,
$k \longleftarrow H(x)$, $m \longleftarrow D_s(k, c)$
output m

Nhắc lại: Số học modun hợp số

Xét $N = p \cdot q$ với p,q là các số nguyên tố

$Z_N = \{0,1,2,\ldots,N-1\}$; $(Z_N)^* = \{\text{các phần tử khả nghịch trong } Z_N\}$

Bổ đề: $x \in Z_N$ là khả nghịch $\Leftrightarrow$ $\gcd(x,N) = 1$

- Số các phần tử của $(Z_N)^*$ là $\varphi(N) = (p-1)(q-1) = N-p-q+1$

Định lý Euler: $\forall x \in (Z_N)^* : x^{\varphi(N)} = 1$

Hoán vị cửa sập RSA

G(): chọn hai số nguyên tố $p,q \approx 1024$ bits. Đặt **N=pq**.

chọn các số nguyên **e , d** thoả mãn **$e \cdot d = 1 \pmod{\varphi(N)}$**

output pk = (N, e) , sk = (N, d)

F(pk, x): $\mathbb{Z}_N^* \to \mathbb{Z}_N^*$ **RSA(x) = x^e** (in Z_N)

F^{-1}(sk, y) = y^d ; y^d = **$RSA(x)^d$** = x^{ed} = $x^{k\varphi(N)+1}$ = $\left(x^{\varphi(N)}\right)^k \cdot x = x$

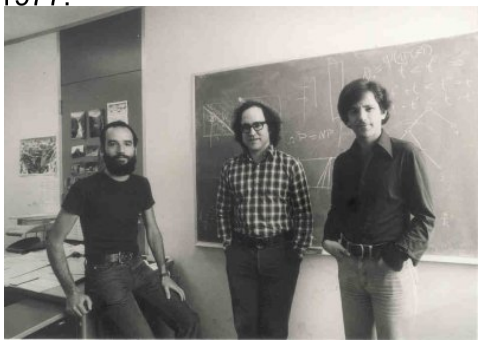
Nội dung

- Hàm cửa sập
- **Hệ mật mã RSA**

Hoán vị cửa sập RSA

Ronald Rivest, Adi Shamir, và Leonard Adleman

Công bố: Scientific American, 8/1977.



Được sử dụng rộng rãi trong:

- SSL/TLS: chứng thư số và trao đổi khóa
- e-mail và hệ thống file an toàn

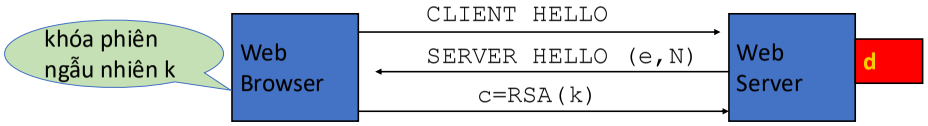
… và nhiều hệ thống khác

Hệ mật mã RSA (chuẩn ISO)

(E_s, D_s): hệ mật mã đối xứng an toàn.
H: $Z_N \to K$ với K là không gian khóa của (E_s, D_s)

- **G**(): sinh tham số RSA : pk = (N,e), sk = (N,d)
- **E**(pk, m): (1) chọn số ngẫu nhiên x thuộc Z_N
  (2) $y \leftarrow RSA(x) = x^e$, $k \leftarrow H(x)$
  (3) output (y , $E_s(k,m)$)
- **D**(sk, (y, c)): output $D_s(\ H(RSA^{-1}(y))\ ,\ c)$

Một tấn công đơn giản textbook RSA



Giả sử k là 64 bit: $k \in \{0,\ldots,2^{64}\}$. Eve nhìn thấy: $c = k^e$ thuộc Z_N
If $\mathbf{k = k_1 \cdot k_2}$ với $k_1, k_2 < 2^{34}$ (prob. ≈20%) thì $\mathbf{c/k_1^e = k_2^e}$ in Z_N

Bước 1: xây dựng bảng: $c/1^e, c/2^e, c/3^e, \ldots, c/2^{34e}$. time: 2^{34}

Bước 2: với $k_2 = 0,\ldots, 2^{34}$ kiểm tra nếu k_2^e nằm trong bảng. thời gian: 2^{34}

Output cặp (k_1, k_2). Tổng thời gian tấn công: $\approx 2^{40} << 2^{64}$

Giả sử RSA

Giả sử RSA: RSA là hoán vị "một chiều"

Với mọi kẻ tấn công *hiệu quả* A:

$$\Pr[\ A(N,e,y) = y^{1/e}\ ] < \text{"cực nhỏ"}$$

ở đó $p,q \xleftarrow{R}$ số nguyên tố n-bit, $N \leftarrow pq$, $y \xleftarrow{R} Z_N^*$

Textbook RSA là không an toàn

Textbook RSA :

- khóa công khai: **(N,e)** Mã hóa: $\mathbf{c \leftarrow m^e}$ (in Z_N)
- khóa bí mật: **(N,d)** Giải mã: $\mathbf{c^d \to m}$

Hệ mật mã này không an toàn !

⇒ Mã hõa trực tiếp với hoán vị cửa sập RSA không phải là sơ đồ an toàn !

Độ dài khóa

Tính an toàn của hệ mật mã khóa công khai nên được so sánh với tính an toàn của hệ mật mã khóa đối xứng:

Khóa đối xứng	RSA Kích thước Modulus N
80 bits	1024 bits
128 bits	3072 bits
256 bits (AES)	**15360** bits

RSA với số mũ công khai nhỏ

Để tăng tốc việc mã hóa RSA, sử dụng số mũ e nhỏ: $c = m^e \pmod N$

- Giá trị nhỏ nhất: **e=3** (gcd(e, φ(N)) = 1)
- Giá trị nên dùng: **$e=65537=2^{16}+1$**

Mã hóa: 17 phép nhân

Tính bất đối xứng của RSA: mã hóa nhanh / giải mã chậm

- Hệ ElGamal (bài tiếp theo): thời gian gần như nhau trong cả hai trường hợp

Bài tập (Tấn công RSA với modun nhỏ)

- Khoá công khai RSA của Bob có modun $N = 12191$ và số mũ $e = 37$.
- Alice gửi cho Bob bản mã $c = 587$.
- Không may, Bob đã chọn modun kích thước quá nhỏ.
- Bạn hãy giúp Oscar giải mã bằng cách phân tích thừa số nguyên tố của N và giải mã thông điệp của Alice.
- (*Gợi ý*. N có một thừa số nguyên tố nhỏ hơn 100.)

Bài tập (Mã hoá với Textbook RSA)

Alice đưa cho Bob khoá công khai RSA của cô ấy:

modun $N = 2038667$ và số mũ $e = 103$.

a) Bob muốn gửi cho Alice thông điệp $m = 892383$. Bản mã mà Bob gửi cho Alice là gì?

b) Alice biết rằng modun N của cô ấy là tích của hai số nguyên tố, một trong hai số là $p = 1301$. Hãy tìm số mũ giải mã d cho Alice.

c) Alice nhận được bản mã $c = 317730$ từ Bob. Hãy giải mã.