



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

Nhập môn An toàn thông tin

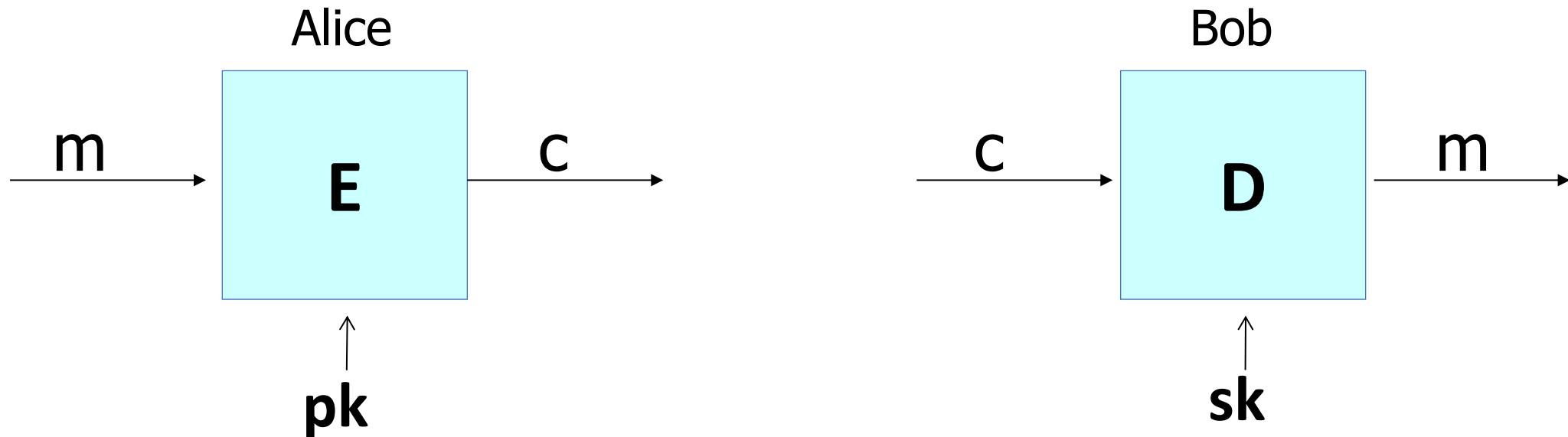
Hệ mật mã RSA

Nội dung

- Hàm cửa sập
- Hệ mật mã RSA

Mật mã khóa công khai

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



Hàm cửa sập (Trapdoor functions - TDF)

ĐN: hàm cửa sập $X \rightarrow Y$ 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 $X \rightarrow Y$
- $F^{-1}(sk, \cdot)$: hàm từ $Y \rightarrow X$ tính nghịch đảo $F(pk, \cdot)$

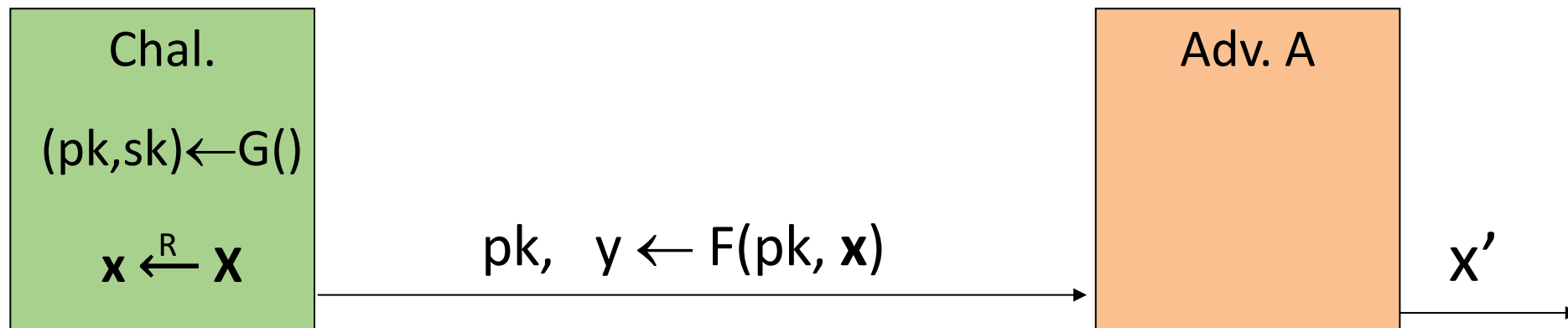
Cụ thể: $\forall (pk, sk)$ sinh bởi hàm G

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

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 :

$$\text{Adv}_{\text{ow}}[A, F] = \Pr[x = x'] < \text{“cực nhỏ”}$$

Xây dựng hệ mật khóa công khai từ TDFs

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

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

Sinh khóa G : giống như G cho TDF

Hệ mật mã khóa công khai từ TDFs

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

$E(pk, m)$:

$x \xleftarrow{R} X, \quad y \leftarrow F(pk, x)$
 $k \leftarrow H(x), \quad c \leftarrow E_s(k, m)$
output (y, c)

$D(sk, (y, c))$:

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

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 $c \leftarrow F(pk, m)$

$D(sk, c)$:

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

Vấn đề:

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

Nội dung

- Hàm cửa sập
- **Hệ mật mã RSA**

Nhắc lại: Số học modun hợp số

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

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

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

- 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

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



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** thỏa mãn **$e \cdot d = 1 \pmod{\varphi(N)}$**

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

$$\mathbf{F(pk, x)}: \mathbb{Z}_N^* \rightarrow \mathbb{Z}_N^* \quad \mathbf{RSA(x) = x^e} \quad (\text{in } \mathbb{Z}_N)$$

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

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 $p, q \xleftarrow{R} \text{số nguyên tố } n\text{-bit}, \quad N \leftarrow pq, \quad y \xleftarrow{R} \mathbb{Z}_N^*$

Hệ mật mã RSA

(chuẩn ISO)

(E_s, D_s) : hệ mật mã đối xứng an toàn.

$H: Z_N \rightarrow K$ 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) $y \leftarrow \text{RSA}(x) = x^e$, $k \leftarrow H(x)$
 - (3) output $(y, E_s(k, m))$
- **D(sk, (y, c))**: output $D_s(H(\text{RSA}^{-1}(y)), c)$

Textbook RSA là không an toàn

Textbook RSA :

- khóa công khai: (N, e)
- khóa bí mật: (N, d)

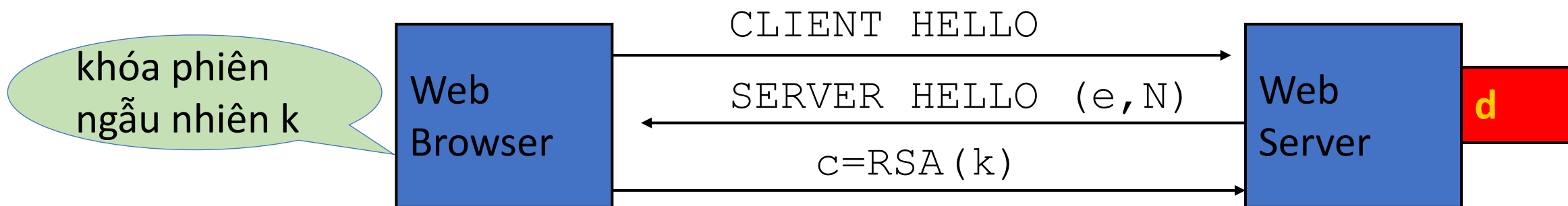
Mã hóa: $c \leftarrow m^e \quad (\text{in } Z_N)$

Giải mã: $c^d \rightarrow m$

Hệ mật mã này không an toàn !

\Rightarrow Mã hóa trực tiếp với hoán vị cửa sập RSA không phải là sơ đồ an toàn !

Một tấn công đơn giản textbook RSA



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

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

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

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

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: **$e=3$** ($\gcd(e, \varphi(N)) = 1$)
- 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

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:

<u>Khóa đối xứng</u>	<u>RSA</u> <u>Kích thước Modulus N</u>
80 bits	1024 bits
128 bits	3072 bits
256 bits (AES)	<u>15360</u> bits

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.

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.)