

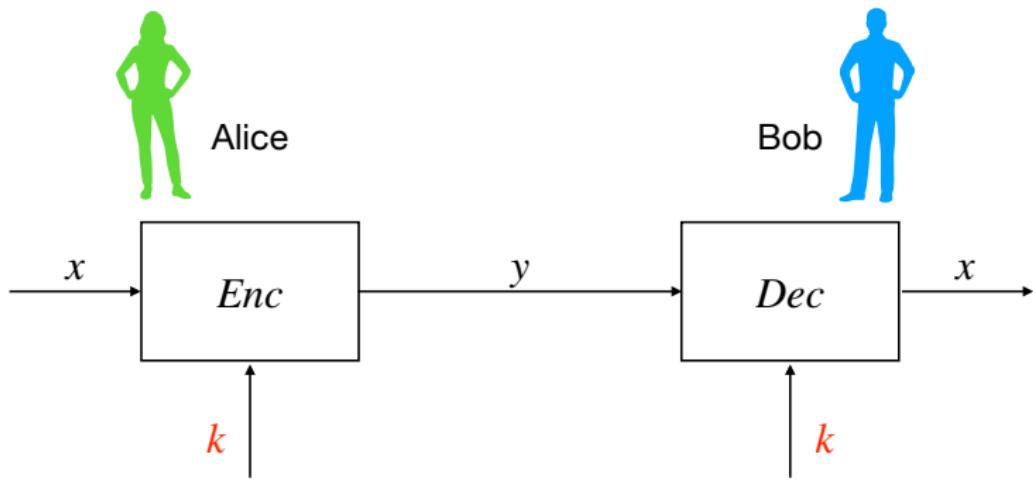


ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Nhập môn An Toàn Thông Tin

Giới thiệu về Mật Mã Khoá Công Khai

Mã hoá khoá đối xứng



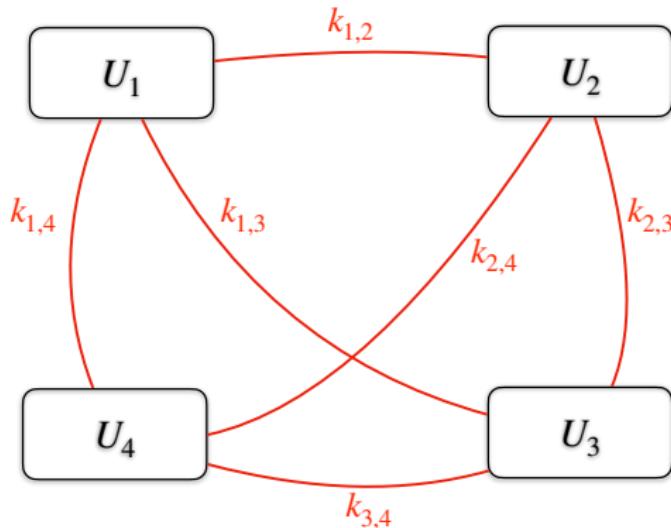
- Cùng khoá k cho cả việc mã hoá và giải mã;
- Hàm mã hoá và giải mã là tương tự (thậm chí trùng) nhau.

Mã hoá khoá đối xứng

- Thuật toán mã đối xứng AES hay 3DES rất an toàn, hiệu quả, và được dùng phổ biến; tuy nhiên
- **Khoá đối xứng k phải được trao đổi an toàn!**

Vấn đề của mã khoá khoá đối xứng

- Có n người dùng.
- Lưu trữ các cặp khoá phân biệt rất khó.



Hình: $O(n)$ khoá cho mỗi người dùng

Vấn đề của mã hoá khoá đối xứng

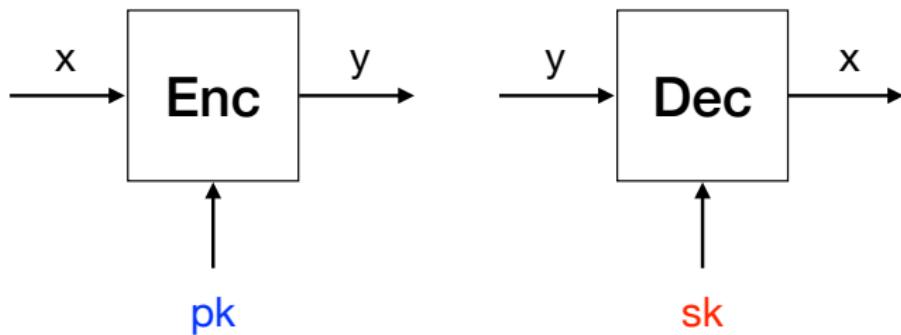
- Alice và Bob có thể **lừa** nhau;
- Ví dụ: Alice có thể khẳng định rằng cô ấy chưa bao giờ đặt hàng TV trực tuyến từ Bob (anh ấy có thể đã bịa đặt hàng của cô ấy).
- Để ngăn chặn điều này: Tính “không chối bỏ được”.

Mật mã khoá công khai

Whitfield Diffie, Martin Hellman, và Ralph Merkle năm 1976

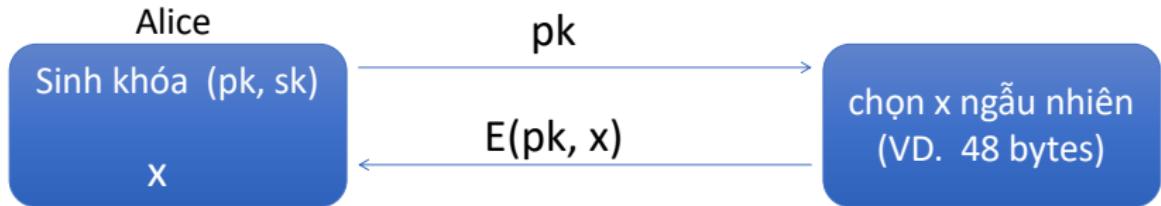


Mật mã khoá công khai



Bob sinh cặp khóa $k = (pk, sk)$ và đưa pk cho Alice.

Ứng dụng: Thiết lập khoá phiên



Ứng dụng không cần tương tác: (VD. Email)

- Bob gửi email được mã hóa với pk_{alice} cho Alice
- Chú ý: Bob cần biết pk_{alice} (quản lý khóa công khai)

Mật mã khoá công khai

Định nghĩa

Một **hệ mật mã khoá công khai** là bộ ba thuật toán

$$(G, \text{Enc}, \text{Dec})$$

trong đó:

- $G()$: thuật toán **ngẫu nhiên** output cặp khóa (pk, sk)
- $\text{Enc}(pk, m)$: thuật toán **ngẫu nhiên** nhận $m \in M$ và output $c \in C$
- $\text{Dec}(sk, c)$: thuật toán **đơn định** nhận $c \in C$ và output $m \in M$ hoặc \perp

Tính đúng đắn: Với mọi (pk, sk) sinh bởi G :

$$\forall m \in M : \quad \text{Dec}(sk, \text{Enc}(pk, m)) = m.$$

Hàm cửa sập (Trapdoor functions - TDF)

Định nghĩa

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 $F(pk, \cdot)$

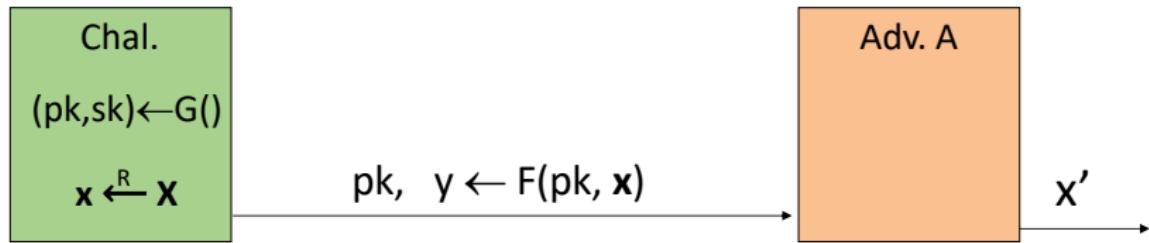
Cụ thể: $\forall(pk, sk)$ sinh bởi hàm $G()$, ta có

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

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



Định nghĩa

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

$\Pr[x = x']$ là “nhỏ không đáng kể”

Xây dựng mật mã khoá công khai từ TDF

Bắt đầu từ

- (G, F, F^{-1}) là TDF an toàn;
- $(\text{Enc}_s, \text{Dec}_s)$ là hệ mã hoá đối xứng an toàn trên (K, M, C) ;
- $H : X \rightarrow Y$ là hàm băm.

Ta xây dựng hệ mật mã khoá công khai

$$(G, \text{Enc}, \text{Dec})$$

với hàm sinh khoá chính là hàm G cho TDF;

Xây dựng mật mã khoá công khai từ TDF

- (G, F, F^{-1}) là TDF an toàn;
- $(\text{Enc}_s, \text{Dec}_s)$ là hệ mã hoá đối xứng an toàn trên (K, M, C) ;
- $H : X \rightarrow Y$ là hàm băm.

$\text{Enc}(\text{pk}, m) :$

$$\begin{aligned}x &\leftarrow_{\$} X, & y &= F(\text{pk}, x) \\k &= H(x), & c &\leftarrow \text{Enc}_s(k, m) \\&\text{return } (y, c)\end{aligned}$$

$\text{Dec}(\text{sk}, (y, c)) :$

$$\begin{aligned}x &= F^{-1}(\text{sk}, y), \\k &= H(x), & m &= \text{Dec}_s(k, c) \\&\text{return } m\end{aligned}$$

Sử dụng không đúng hàm cửa sập

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

$\text{Enc}(\text{pk}, m)$:

return $c = F(\text{pk}, m)$

$\text{Dec}(\text{sk}, c)$:

return $m = F^{-1}(\text{sk}, c)$

Vấn đề:

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

Một số hàm “một chiều”

Các hệ mật khoá công khai dựa trên các **hàm một chiều**:

Tính f **dễ**, tính f^{-1} là **khó**!

- **Phân tích thừa số nguyên tố** (RSA, …):
Cho hợp số n , tìm các thừa số nguyên tố của n
(nhân hai số nguyên tố: **dễ**)
- **Logarit rời rạc** (Diffie Hellman, Elgamma, DSA, …):
Cho a, y , và m , tìm x thoả mãn

$$a^x = y \pmod{m}$$

(Tính mũ a^x : **dễ**)

- **Đường cong Elliptic** (EC) (ECDH, ECDSA, …): tổng quát hoá
của bài toán Logarit rời rạc

Độ dài khoá và mức an toàn

Đối xứng	ECC	RSA, DL	Chú ý
64 Bit	128 bit	\approx 700 bit	an toàn trong ngắn hạn (vài giờ hoặc vài ngày)
80 Bit	160 Bit	\approx 1024 bit	an toàn trong trung hạn (có thể bị tấn công bởi chính phủ hoặc tổ chức lớn)
128 Bit	256 Bit	\approx 3072 bit	an toàn trong dài hạn (trừ khi có máy tính lượng tử)



25
YEARS ANNIVERSARY
SOICT

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

