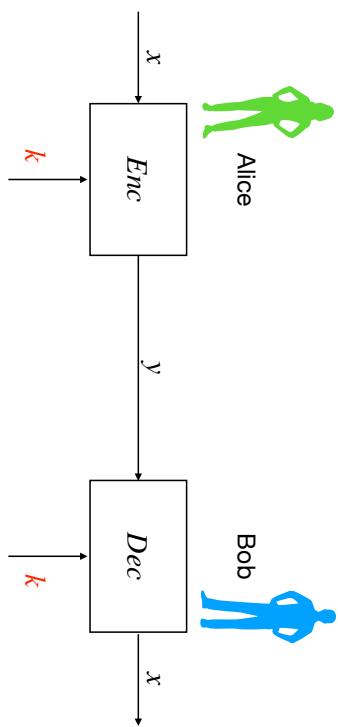


## Mã hoá khoá đối xứng

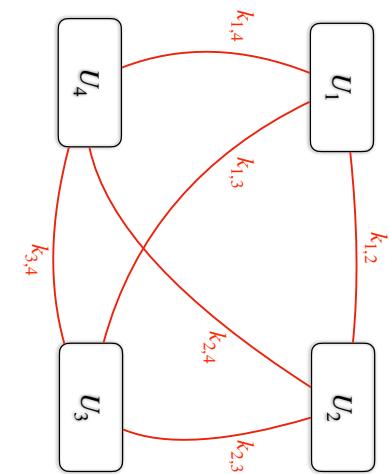
- Có  $n$  người dùng.
- Lưu trữ các cặp khoá phân biệt rất khó.



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

2/17

Hình:  $O(n)$  khoá cho mỗi người dùng



4/17

## Mã hoá khoá đối xứng



### Nhập môn An Toàn Thông Tin

Giới thiệu về Mật Mã Khoa Công Khai

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

1/17



3/17

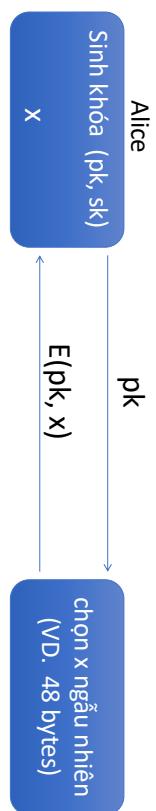
## Mật mã khoá công khai

Whitfield Diffie, Martin Hellman, và Ralph Merkle năm 1976



6 / 17

## Ứng dụng: Thiết lập khoá phiên

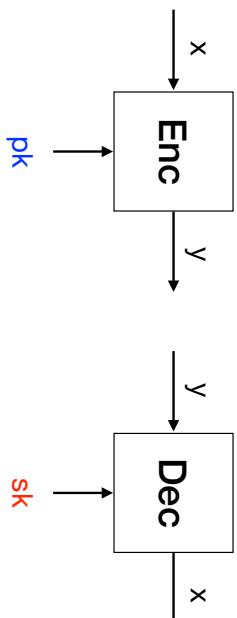


8 / 17

## 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.

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



## Mật mã khoá công khai

## Hàm cửa sập (Trapdoor functions - TDF)

### Xây dựng mật mã khoá công khai từ 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  $(\text{pk}, \text{sk})$
- $F(\text{pk}, \cdot)$ : thuật toán **đơn định** định nghĩa một hàm  $X \rightarrow Y$
- $F^{-1}(\text{sk}, \cdot)$ : hàm từ  $Y \rightarrow X$  tính nghịch đảo  $F(\text{pk}, \cdot)$

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

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

### 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:

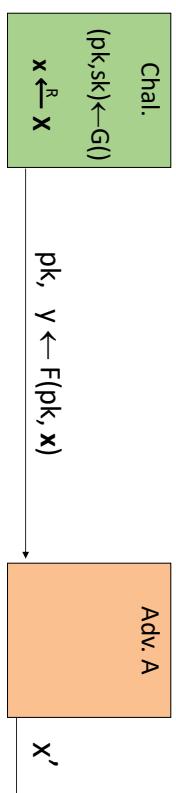
- $G()$ : thuật toán **ngẫu nhiên** output cặp khóa  $(\text{pk}, \text{sk})$
- $\text{Enc}(\text{pk}, m)$ : thuật toán **ngẫu nhiên** nhận  $m \in M$  và output  $c \in C$
- $\text{Dec}(sk, c)$ : thuật toán **đơn định** nhận  $c \in C$  và output  $m \in M$  hoặc  $\perp$

Tính **đúng đắn**: Với mọi  $(\text{pk}, \text{sk})$  sinh bởi  $G$ :

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

### Hàm cửa sập an toàn

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



Định nghĩa

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

$$\Pr[x = x'] \text{ là } "nhỏ không đáng kể"$$

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;

## Sử dụng không đúng hàm của sập

### Độ dài khoá và mức an toàn

Không mã hóa bằng cách áp dụng  $F$  để mã hóa bẩn rỗ:

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



14/17

## 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.

$\text{Enc}(\text{pk}, m)$ :  
 $x \leftarrow_s X,$   
 $y = F(\text{pk}, x)$   
 $k = H(x),$   
return  $(y, c)$

$\text{Dec}(\text{sk}, (y, c))$ :  
 $x = F^{-1}(\text{sk}, y),$   
 $k = H(x),$   
return  $(y, c)$

(Tính mũ  $a^x$ :  $\text{đẽ}$ )

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



16/17

## Một số hàm “một chiều”

Các hệ mật khoá công khai dựa trên các **hàm một chiều**:  
Tính  $f$  **đẽ**, 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:  $\text{đẽ}$ )
- Logarit rời rạc** (Diffie Hellman, Elgamal, DSA, …):  
Cho  $a, y$ , và  $m$ , tìm  $x$  thoả mãn  
$$a^x = y \pmod{m}$$



13/17

