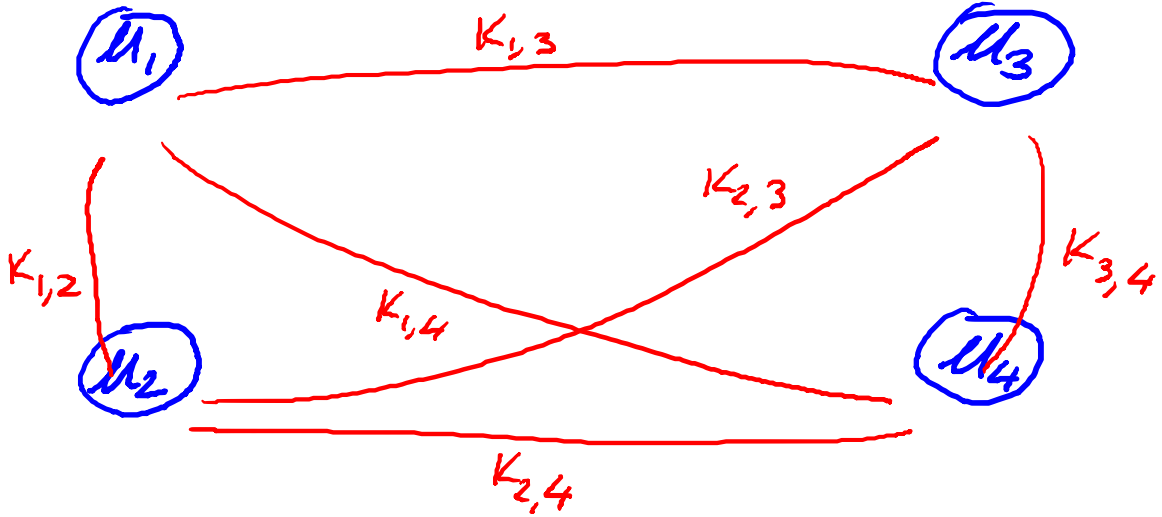
Giao thức trao đổi khoá

Nội dung

1. **Trao đổi khoá**
2. Merkle Puzzles
3. Giao thức Diffie-Hellman
4. Giao thức dựa trên mật mã khoá công khai
5. Hệ mật mã ElGama

Quản lý khoá

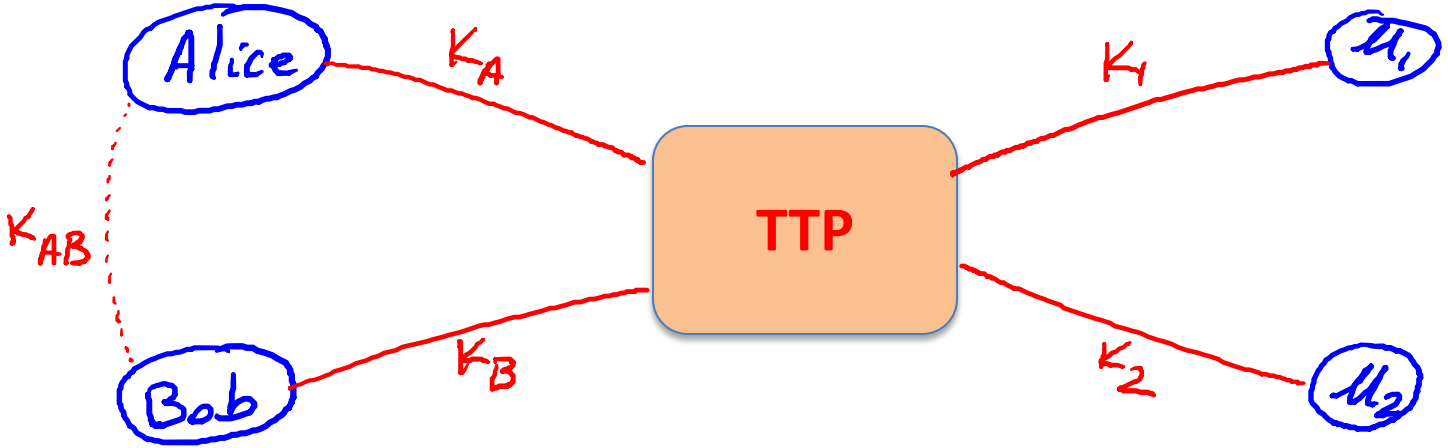
Vấn đề: Có n người dùng. Lưu trữ các cặp khoá phân biệt rất khó



Tổng số: O(n) khoá cho mỗi người dùng

Một giải pháp tốt hơn

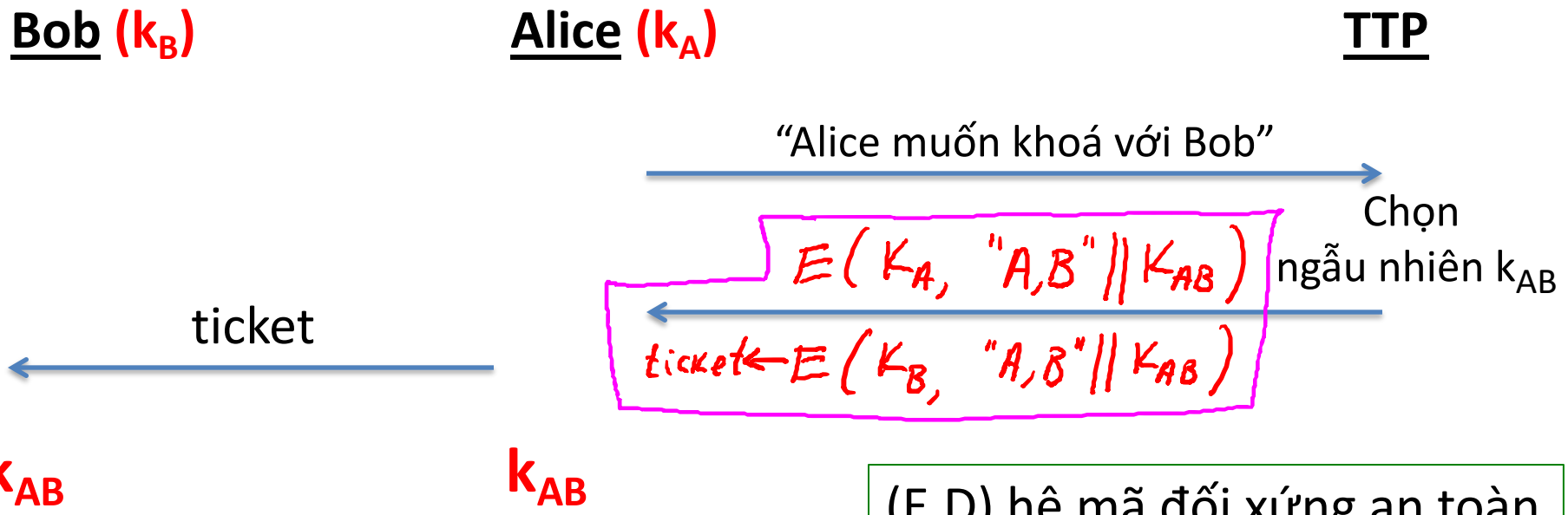
Bên thứ ba tin cậy (Online Trusted 3rd Party (TTP))



Every user only remembers one key.

Giao thức sinh khoá chia sẻ

Alice muốn chia sẻ khoá với Bob.



(E,D) hệ mã đối xứng an toàn

Giao thức sinh khoá chia sẻ

Alice muốn chia sẻ khoá với Bob.

Kẻ tấn công nhìn thấy: $E(k_A, \text{“A, B”} \,||\, k_{AB})$; $E(k_B, \text{“A, B”} \,||\, k_{AB})$

(E,D) an toàn $\Rightarrow$

kẻ tấn công không học được gì về k_{AB}

Chú ý: TTP cần cho mọi lần chia sẻ khoá, TTP biết mọi khoá chia sẻ

(cơ sở cho hệ Kerberos)

Giao thức sinh khoá: không an toàn trước kẻ tấn công chủ động

Ví dụ: không an toàn trước tấn công phát lại

Kẻ tấn công ghi lại phiên giữa người mua Alice và người bán Bob

- Ví dụ, đặt sách qua mạng

Kẻ tấn công phát lại phiên cho Bob

- Bob nghĩ rằng Alice đang đặt mua một bản khác của cuốn sách

Câu hỏi chính

Liệu ta có thể sinh khoá chia sẻ mà không cần bên thứ ba trực tuyến?

Trả lời: có!

Đây là điểm bắt đầu của mật mã khoá công khai:

- Merkle (1974), Diffie-Hellman (1976), RSA (1977)

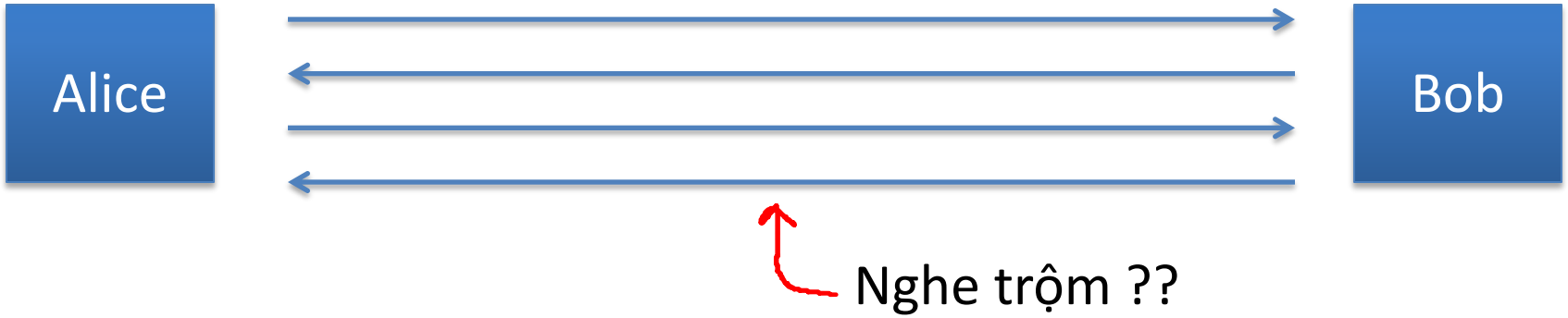
- Gần đây: ID-based enc. (BF 2001), Functional enc. (BSW 2011)

Nội dung

1. Trao đổi khoá
2. **Merkle Puzzles**
3. Giao thức Diffie-Hellman
4. Giao thức dựa trên mật mã khoá công khai
5. Hệ mật mã ElGama

Trao đổi khoá không cần bên thứ ba

Mục đích: Alice và Bob muốn khoá chia sẻ, kẻ tấn công không biết



Liệu ta có thể thực hiện trao đổi khoá chỉ dùng mật mã khoá đối xứng?

Merkle Puzzles (1974)

Trả lời: có thể, nhưng không hiệu quả

<u>Công cụ chính</u>: puzzles

- Các bài toán có thể giải nếu cố gắng
- Ví dụ: E(k,m) là hệ mật mã khoá đối xứng với $k \in \{0,1\}^{128}$
  - **puzzle(P) = E(P, "message")** với $P = 0^{96} \,||\, b_1 \ldots b_{32}$
  - Mục đích: tìm P bằng cách thử 2^{32} khả năng

Merkle puzzles

Alice: chuẩn bị 2^{32} puzzles

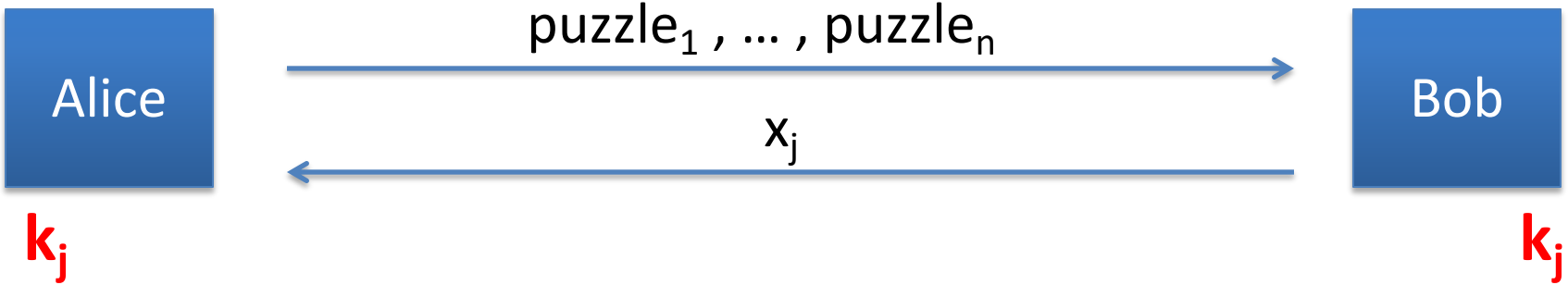
- For i=1, …, 2^{32} :
  - chọn ngẫu nhiên $\mathbf{P_i \in \{0,1\}^{32}}$ và $\mathbf{x_i, k_i \in \{0,1\}^{128}}$
  - đặt $\text{puzzle}_i \longleftarrow E(0^{96} \,||\, \mathbf{P_i}, \text{“Puzzle \# } x_i\text{”} \,||\, k_i)$
- Gửi $\text{puzzle}_1, \ldots, \text{puzzle}_{2^{32}}$ cho Bob

Bob: chọn một puzzle_j ngẫu nhiên, giải để có (x_j, k_j).

- Gửi x_j cho Alice

Alice: tìm puzzle với số x_j. Dùng k_j như khoá chia sẻ

Hình ảnh



Alice thực hiện: O(n) (chuẩn bị n puzzles)

Bob thực hiện: O(n) (giải một puzzle)

Kẻ nghe trộm : $O(n^2)$ (v.d., 2^{64} bước)

Câu hỏi

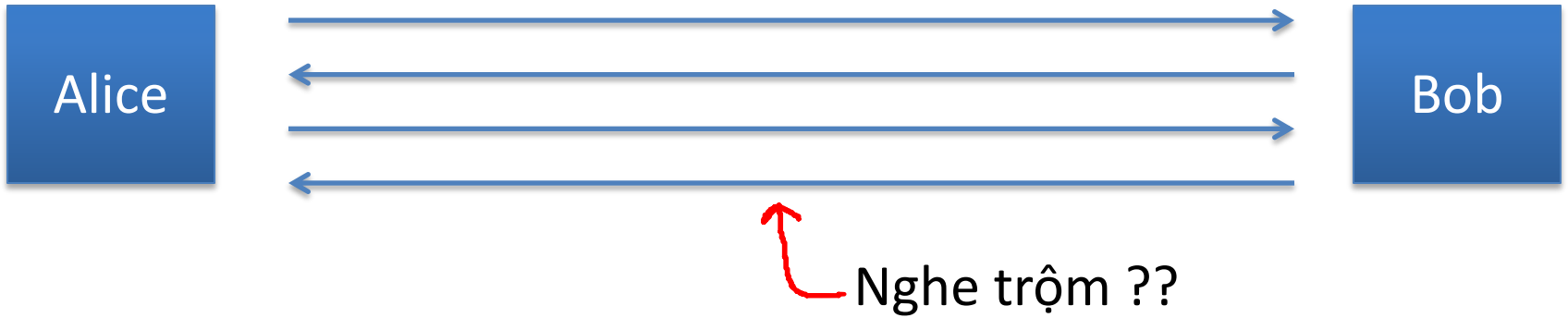
- Liệu có một khoảng cách tốt hơn ($O(n^2) – O(n)$) dùng hệ mã đối xứng?
- Trả lời: không ai biết
- Nhưng: nói một cách thô thiển, khoảng cách bình phương là tốt nhất có thể nếu ta xem hệ mã đối xứng như một truy vấn kiểu hộp đen [IR'89, BM'09]

Nội dung

1. Trao đổi khoá
2. Merkle Puzzles
3. **Giao thức Diffie-Hellman**
4. Giao thức dựa trên mật mã khoá công khai
5. Hệ mật mã ElGama

Trao đổi khoá không cần bên thứ ba

Mục đích: Alice và Bob muốn chia sẻ khoá bí mật, mà kẻ nghe trộm không biết



Liệu ta có thể làm điều này với khoảng cách “hàm mũ”?

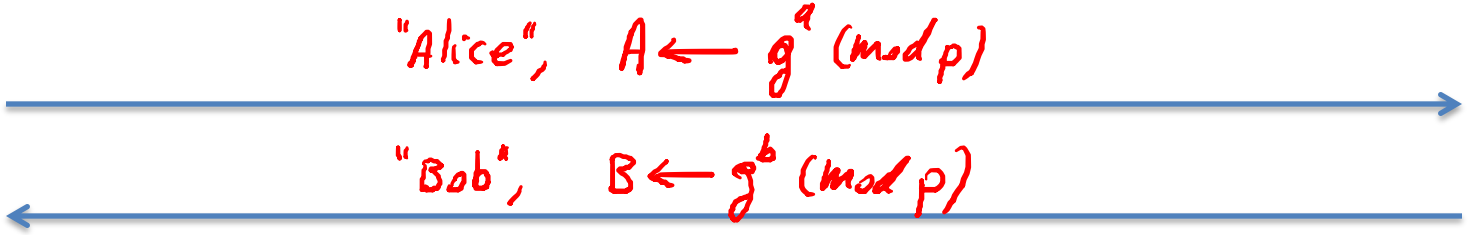
Giao thức Diffie-Hellman

Chọn một số nguyên tố lớn p (v.d. 600 chữ số)

Chọn một số nguyên g thuộc {1, …, p}

Alice **Bob**

Chọn ngẫu nhiên **a** thuộc {1,…,p-1} Chọn ngẫu nhiên **b** thuộc {1,…,p-1}



$$B^a \pmod p = (g^b)^a = k_{AB} = g^{ab} \pmod p = (g^a)^b = A^b \pmod p$$

Tính an toàn

Kẻ nghe trộm nhìn thấy: p, g, $A=g^a \pmod p$, và $B=g^b \pmod p$

Liệu có thể tính $g^{ab} \pmod p$??

Tổng quát: định nghĩa $DH_g(g^a, g^b) = g^{ab} \pmod p$

Hàm DH theo môđun p liệu có khó tính?

Bài tập

Hãy tính hai giá trị sau trong $\mathbb{Z}_{13}^*$.

- $\mathrm{DH}_7(10,5)$
- $\mathrm{DH}_2(12,9)$

biết rằng

$$\langle 2 \rangle = \{1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7\}$$
$$\langle 7 \rangle = \{1, 7, 10, 5, 9, 11, 12, 6, 3, 8, 4, 2\}$$

$$\mathrm{DH}_g(g^a, g^b) = g^{ab} \pmod p$$

Hàm DH theo modun p

Giả sử p là số nguyên tố n dài bits long.

Thuật toán tốt nhất (GNFS): có thời gian ch exp($\tilde{O}(\sqrt[3]{n})$)

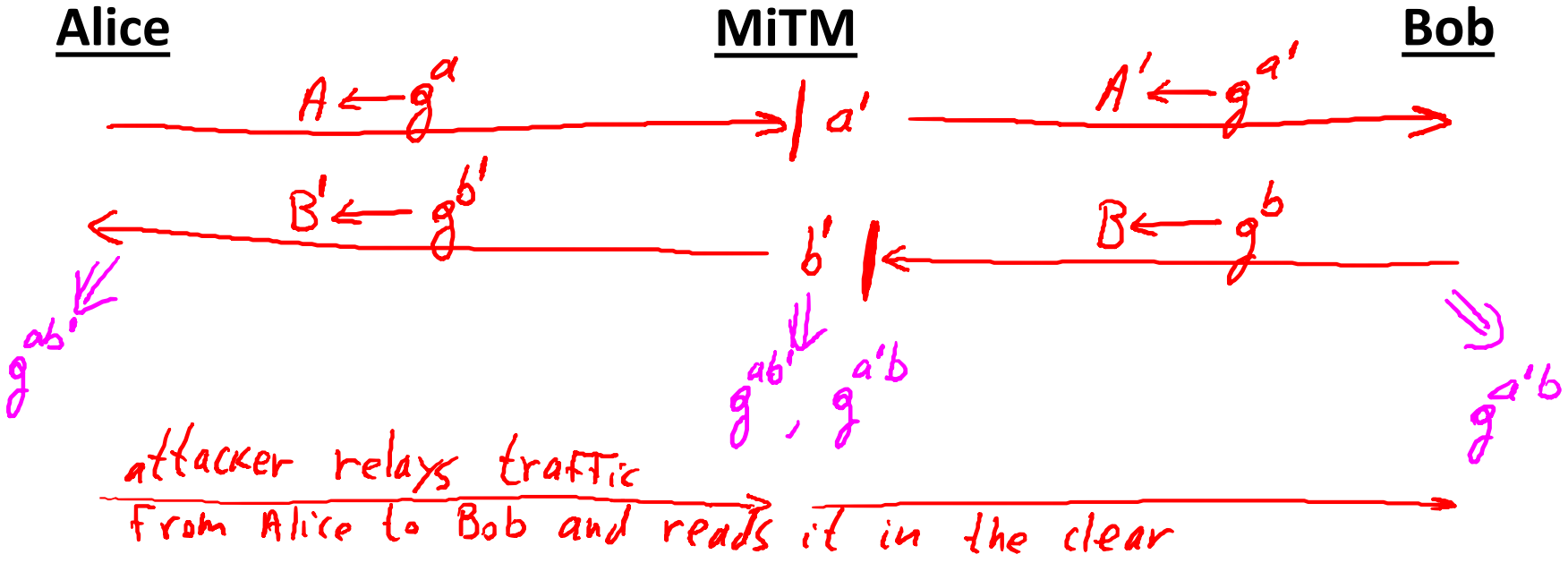
khoá bí mật	kích thước modun	Kích thước Elliptic Curve
80 bits	1024 bits	160 bits
128 bits	3072 bits	256 bits
256 bits (AES)	**15360** bits	512 bits

Hệ quả: chuyển đổi dần từ (mod p) sang đường cong Elliptic

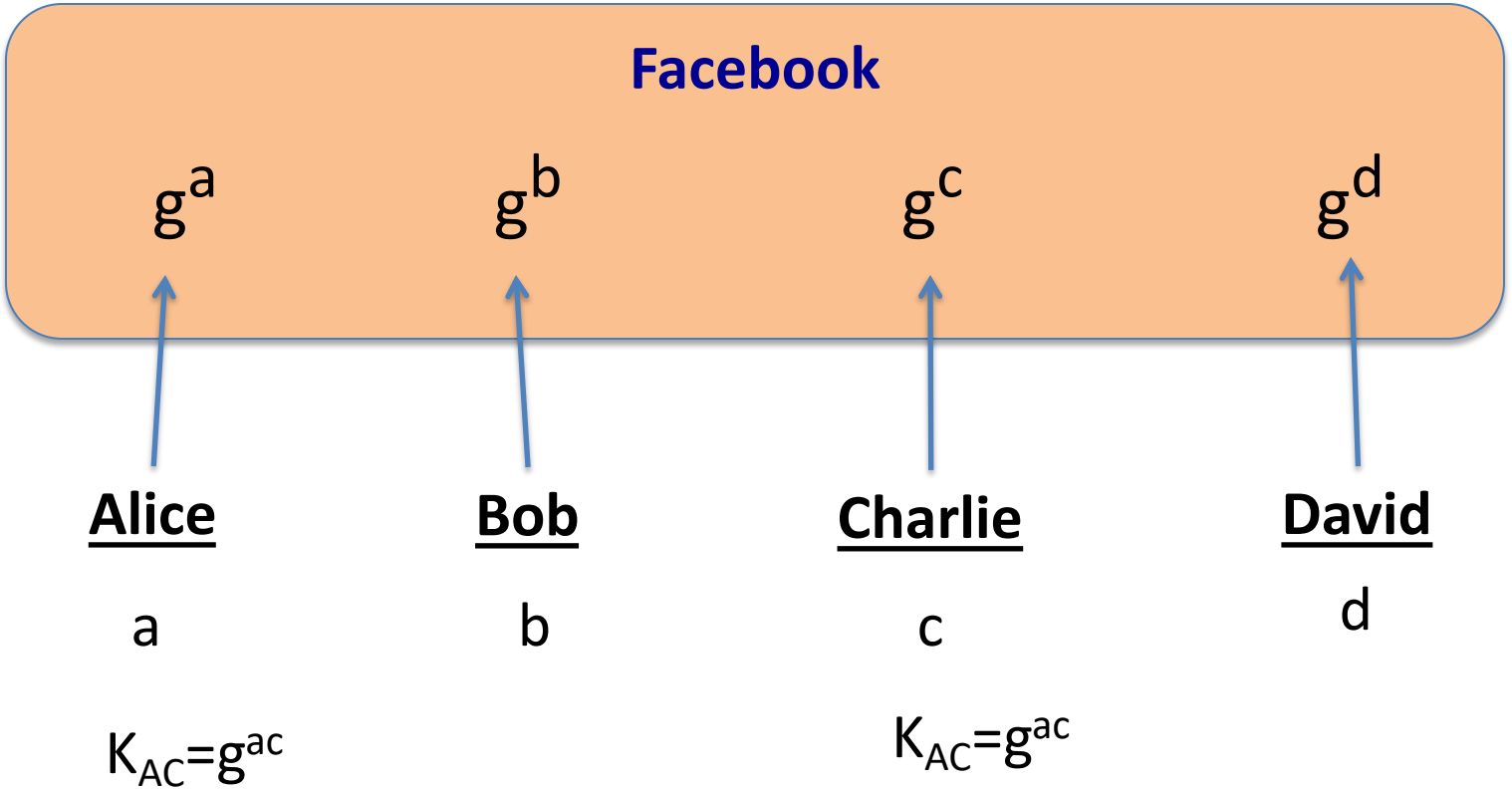
Elliptic curve
Diffie-Hellman

Không an toàn chống lại man-in-the-middle

Giao thức này không an toàn chống lại kẻ tấn công chủ động



Một cách nhìn khác về DH



Một bài toán mở

$n=2$: OH

$n=3$: Khown (Joux)

$n \geq 4$: open

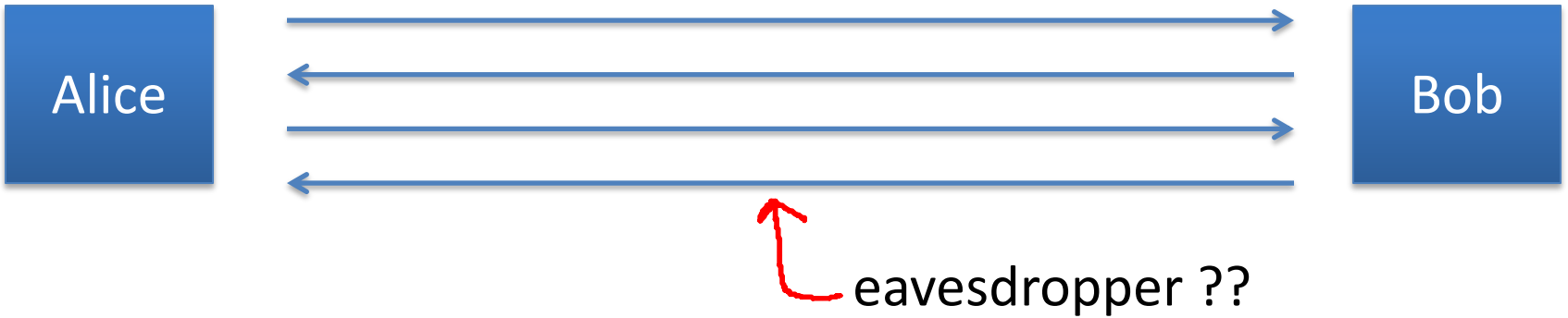
Alice	**Bob**	**Charlie**	**David**	...
a	b	c	d	
K_{ABCD}	K_{ABCD}	K_{ABCD}	K_{ABCD}	

Nội dung

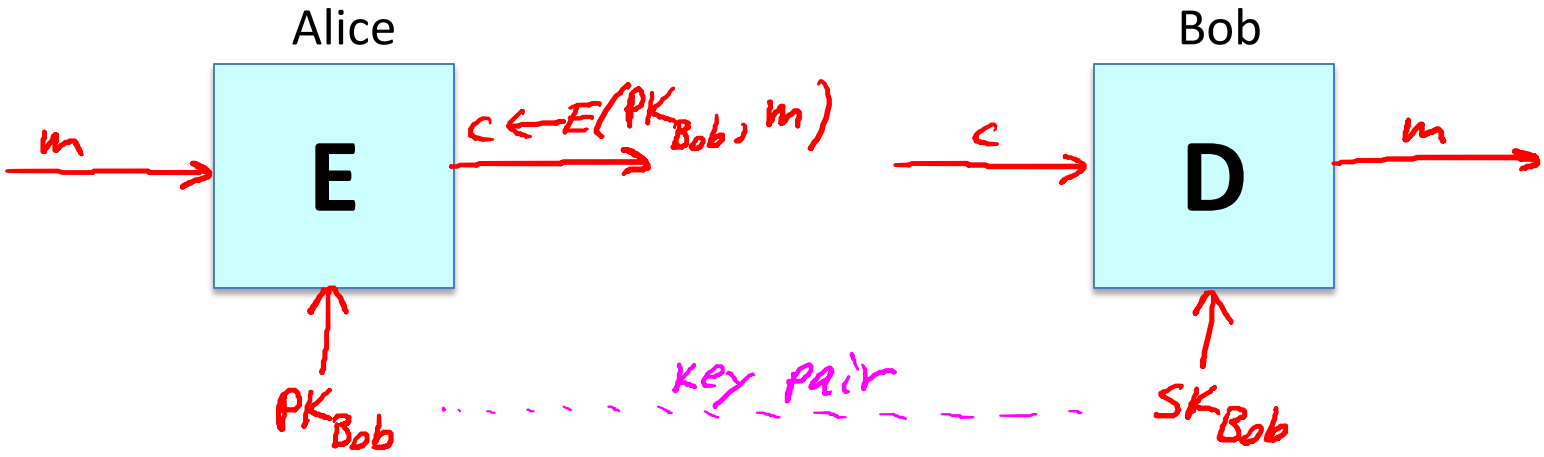
1. Trao đổi khoá
2. Merkle Puzzles
3. Giao thức Diffie-Hellman
4. **Giao thức dựa trên mật mã khoá công khai**

Thiết lập khoá chia sẻ

Mục đích: Alice và Bob muốn chia sẻ khoá bí mật, mà kẻ nghe trộm không biết



Public key encryption



PK: public key, SK: secret key

Mã hóa khóa công khai

ĐN: một hệ mật mã khóa công khai là bộ ba thuật toán (G, E, D)

- G(): thuật toán ngẫu nhiên output cặp khóa (pk, sk)
- E(pk, m): thuật toán ngẫu nhiên nhận $m \in M$ và output $c \in C$
- D(sk,c): thuật toán đơn định nhận $c \in C$ và outputs $m \in M$ hoặc $\perp$

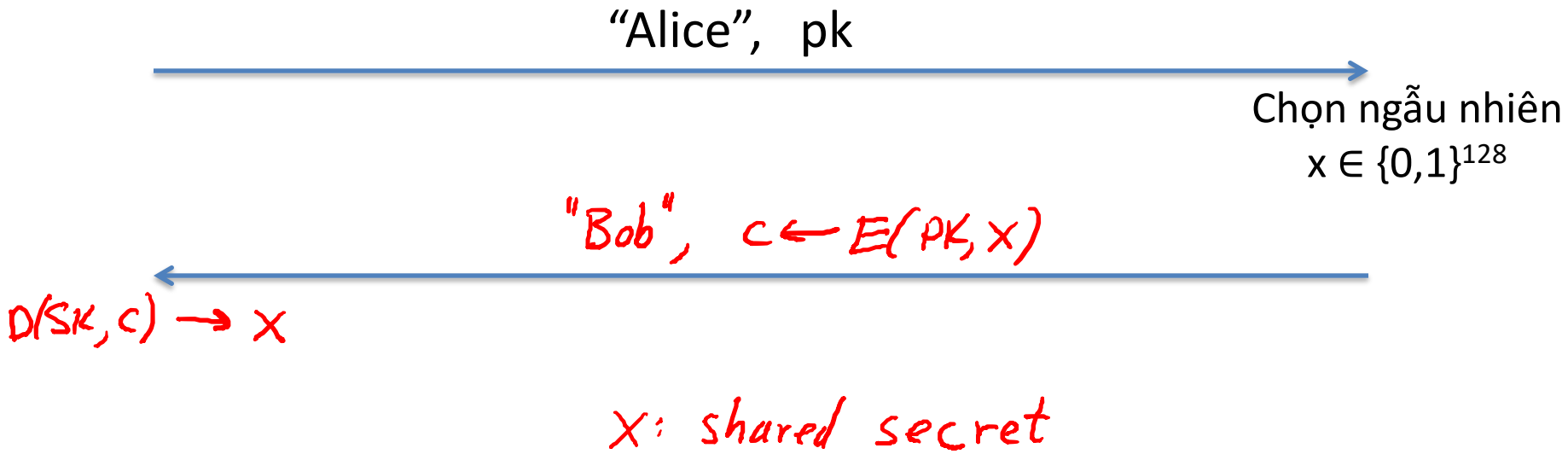
Tính đúng đắn: $\forall$(pk, sk) được sinh bởi G :

$$\forall m \in M: \quad D(sk, E(pk, m)) = m$$

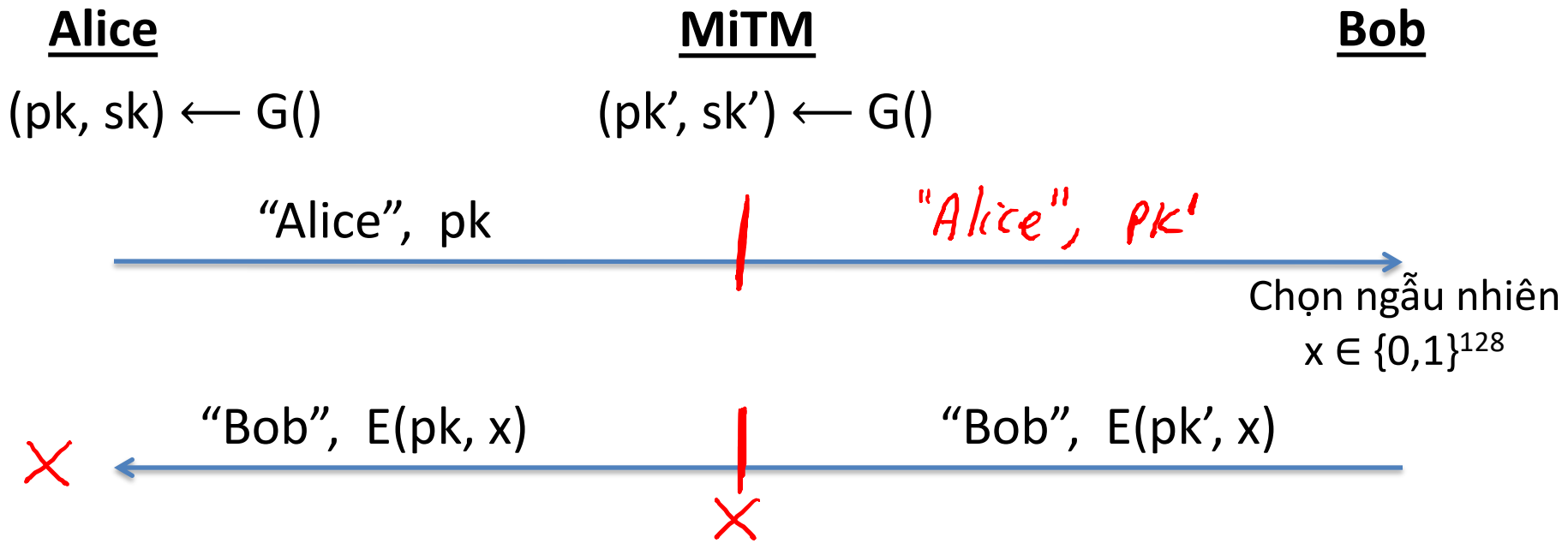
Thiết lập khoá chia sẻ

Alice **Bob**

(pk, sk) ⟵ G()



Không an toàn chống man-in-the-middle



Nội dung

1. Trao đổi khoá
2. Merkle Puzzles
3. Giao thức Diffie-Hellman
4. Giao thức dựa trên mật mã khoá công khai
5. **Hệ mật mã ElGama**

Nhắc lại: Giao thức Diffie-Hellman (1977)

Xét nhóm vòng G (e.g $G = (Z_p)^*$) với cấp n

Lấy một phần tử sinh g thuộc G (i.e. $G = \{1, g, g^2, g^3, \dots, g^{n-1}\}$)

Alice **Bob**

Chọn ngẫu nhiên **a** in {1,…,n} Chọn ngẫu nhiên **b** trong {1,…,n}

$\mathbf{B^a} = (g^b)^a = \mathbf{k_{AB} = g^{ab}} = (g^a)^b = \mathbf{A^b}$

ElGamal: converting to pub-key enc. (1984)

Xét nhóm vòng G (e.g $G = (Z_p)^*$) với cấp n

Lấy một phần tử sinh g thuộc G (i.e. $G = \{1, g, g^2, g^3, \dots, g^{n-1}\}$)

Alice

Chọn ngẫu nhiên **a** thuộc {1,…,n}

Coi a như khoá công khai

$A = g^a$

Bob

Chọn ngẫu nhiên **b** in {1,…,n}

tính $g^{ab} = A^b$,

Dẫn xuất khoá đối xứng k ,

$ct = [\ B = g^b\ ,$ Mã hoá m với k $]$

ElGamal: converting to pub-key enc. (1984)

Xét nhóm vòng G (e.g $G = (Z_p)^*$) với cấp n

Lấy một phần tử sinh g thuộc G (i.e. $G = \{1, g, g^2, g^3, \dots, g^{n-1}\}$)

Alice

Chọn ngẫu nhiên **a** thuộc {1,…,n}

Coi a như khoá công khai

Bob

$A = g^a$

Chọn ngẫu nhiên **b** in {1,…,n}

Để giải mã:
tính $g^{ab} = B^a$,
Dẫn ra k, và giải mã

$ct = [\ B = g^b\ ,$ tính $g^{ab} = A^b$,
Dẫn xuất khoá đối xứng k ,
Mã hoá m với k $]$

Hệ mật ElGamal (cách nhìn hiện đại)

- G: nhóm vòng cấp n
- (E_s, D_s) : mã đối xứng an toàn trên (K,M,C)
- H: $G^2 \longrightarrow K$ hàm băm

Ta xây dung hệ mật khoá công khai (Gen, E, D):

- Sinh khoá Gen:
  - Chọn ngẫu nhiên phần tử sinh g trong G và một số ngẫu nhiên a thuộc Z_n
  - output sk = a , pk = $(g, h=g^a)$

Hệ mật ElGamal

- G: nhóm vòng cấp n
- (E_s, D_s) : mã đối xứng an toàn trên (K,M,C)
- H: $G^2 \longrightarrow K$ hàm băm

E(pk=(g,h), m) :

$b \xleftarrow{R} Z_n$, $u \leftarrow g^b$, $v \leftarrow h^b$

$k \leftarrow H(u,v)$, $c \leftarrow E_s(k, m)$

output (u, c)

D(sk=a, (u,c)) :

$v \leftarrow u^a$

$k \leftarrow H(u,v)$, $m \leftarrow D_s(k, c)$

output m

Hiệu năng ElGamal

E(pk=(g,h), m) :

$b \leftarrow Z_n$, $u \leftarrow g^b$, $v \leftarrow h^b$

D(sk=a, (u,c)) :

$v \leftarrow u^a$

Mã hoá: 2 phép lấy mũ. (cơ sở cố định)

- Có thể tính trước [$g^{(2\hat{}i)}$, $h^{(2\hat{}i)}$ for $i=1,\ldots,\log_2 n$]
- Tốc độ nhanh gấp 3x (hoặc hơn)

Decryption: 1 phép lấy mũ. (cơ sở thay đổi)