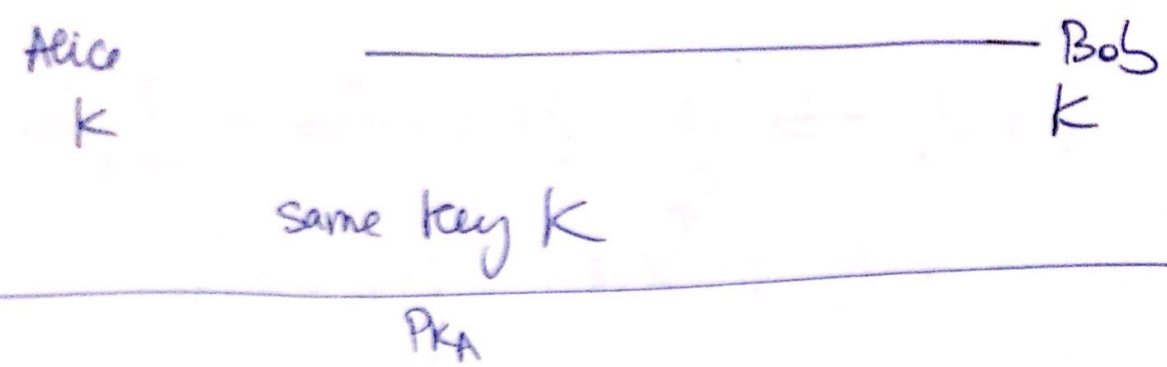
Asymmetric cryptography

Last time : Symmetric



PK_A

Alice

Bob

SK_A, PK_A = public key (known to everyone)

SK_B, PK_B

||

secret key (only known to Alice)

can encrypt using public key

$C = Enc(PK_B, M)$

decrypt only with secret key

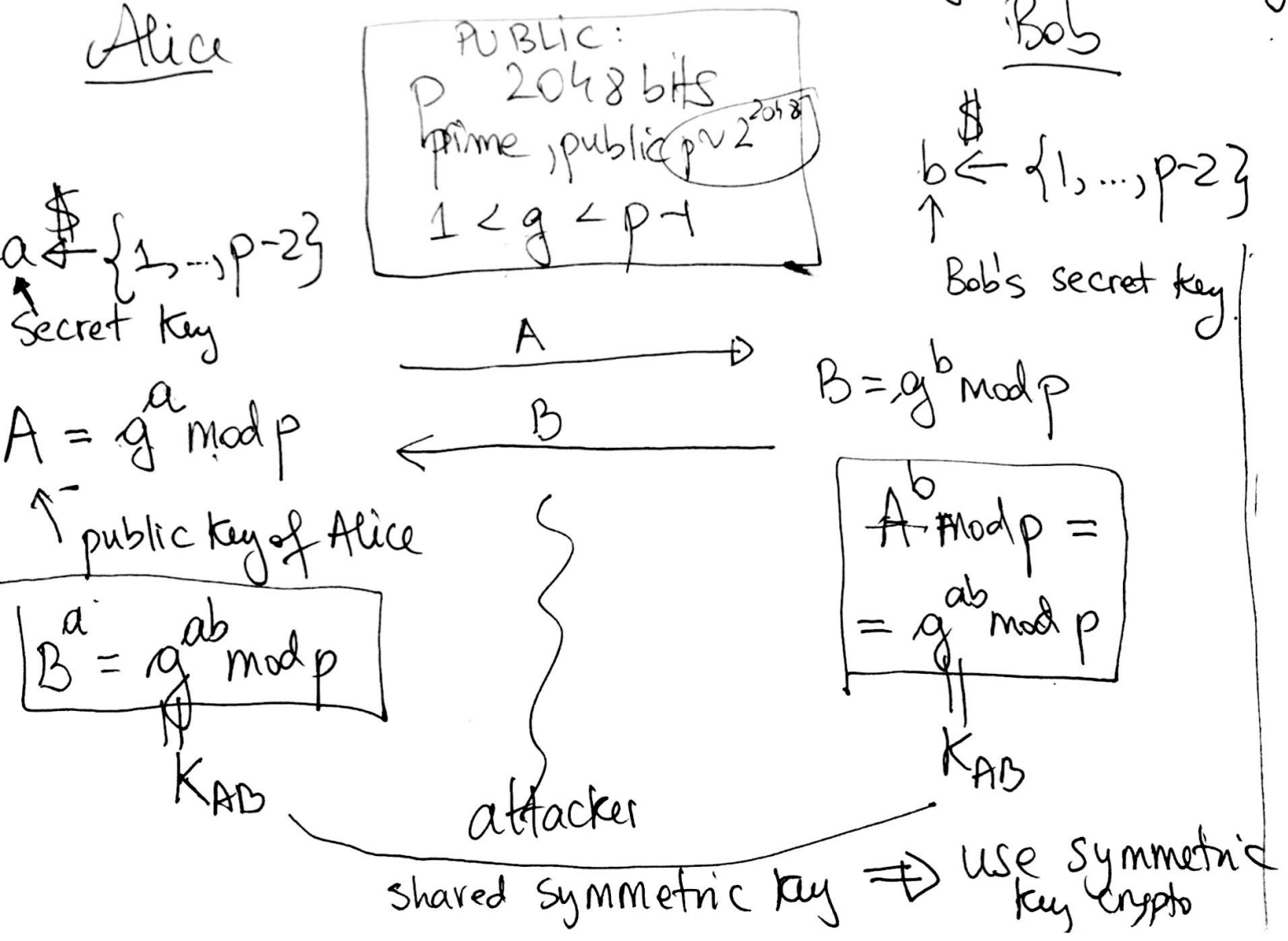
$Dec(SK_B, C) \rightarrow M$

OWF:

For all polynomial time Adv (adversaries algorithm),

$$\text{Probability}\left[x \xleftarrow{\$} \{0,1\}^n;\ y \leftarrow f(x);\ Adv(y) \to x' : f(x') = y \right] = negl \leq \frac{1}{2^{large}}$$

Diffe Hellman key exchange (1970s)
- allows Alice & Bob to share a key without meeting



Discrete Log Assumption:

chosen uniformly at random

Probability $[g \xleftarrow{\$} [1, p-1];$ p is 2048 bits

$\forall$ probabilistic p.p. polynomial $x \xleftarrow{\$} [1, p-1];$ $p \sim 2^{2048}$

$y \leftarrow g^x \bmod p:$

adversary $\mathcal{A}$ $\mathcal{A}(g, p, y) = x^*] = \text{negl}$

s.t. $g^{x^*} \bmod p = y$

One-way functions (OWF)

A function f is one-way function iff

1) Given x, it is easy to compute $f(x)$
   poly time

2) Given y, it is hard to find any value x
   s.t. $f(x)=y$
   no poly time

$x^* \xrightarrow{f} f(x^*)=y$

x s.t. $f(x)=y$

$\Pr[x \xleftarrow{\$} \{0,1\}^n; y \leftarrow f(x): Adv(y)=x' \text{ s.t. } f(x')=y] = negl$

$f(x)=x$ NO

$f(x)=1$ NO

Discrete loganithm problem/assumption

large prime 2048 bits

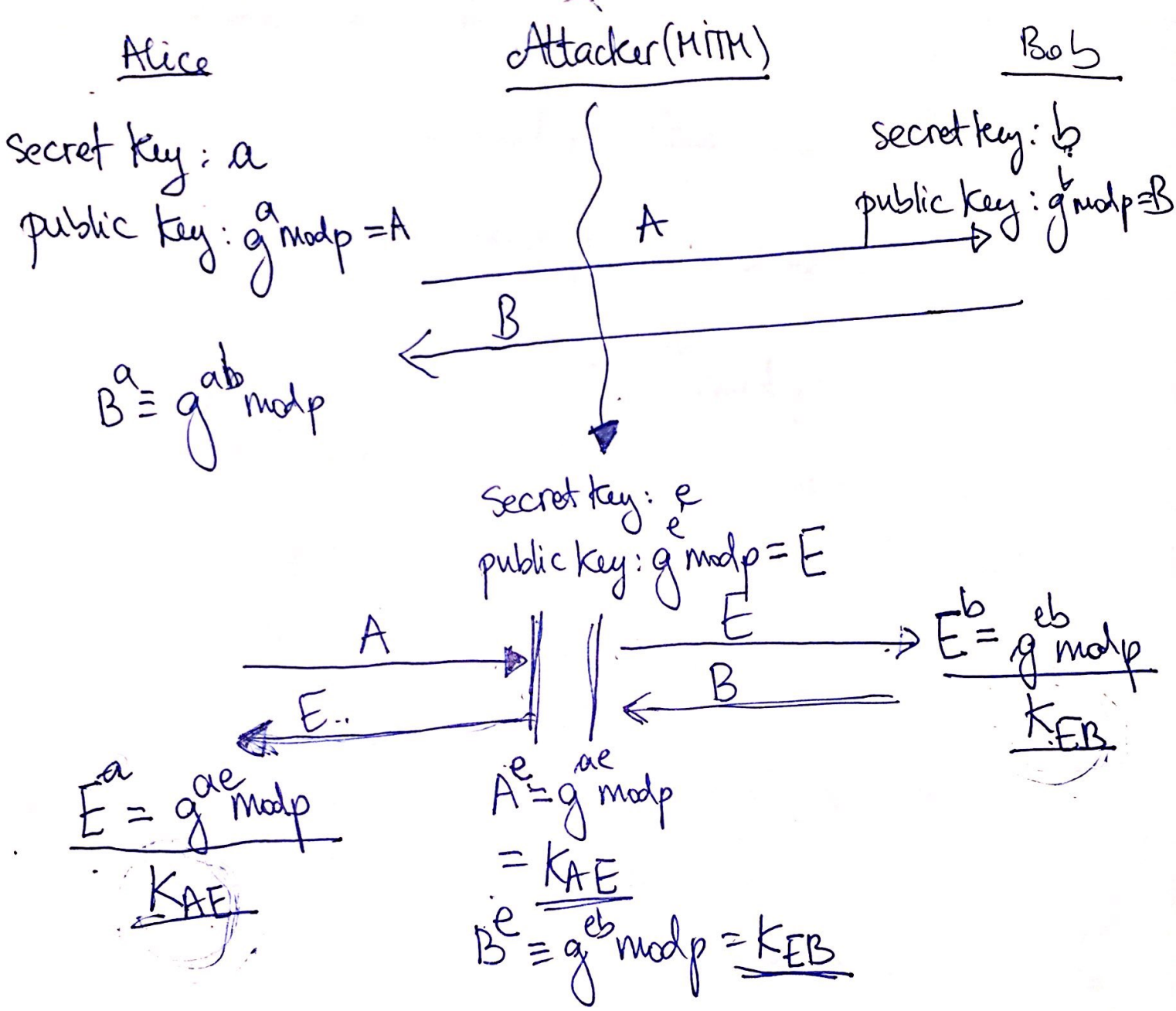
$1 \leq g < p-1$

↓ chosen randomly from $[2, p-2]$

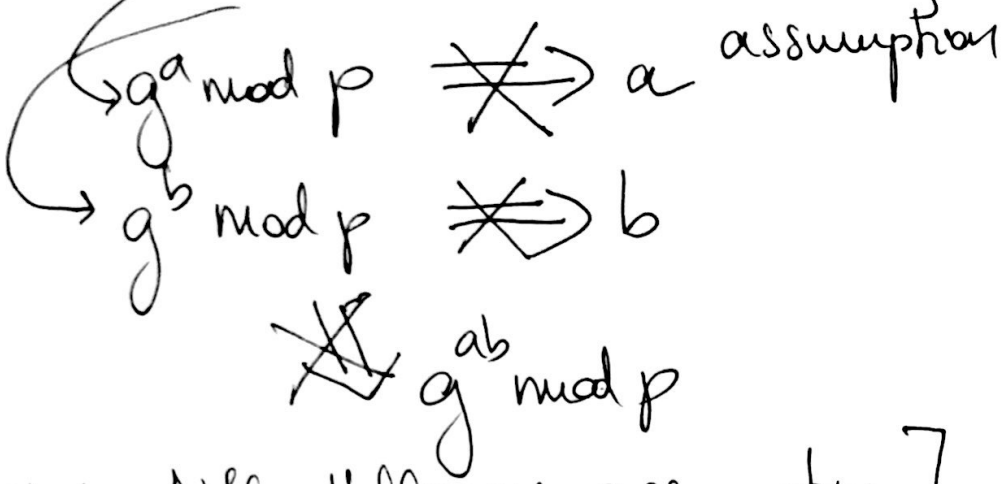
$f(x)=g^x \bmod p$ is OWF

assumption

Man-in-the-middle attack (MITM)



Attacker sees A, B



[Decision Diffie Hellman assumption]

$g^a \bmod p$ is efficient to compute (polynomial time)

$a \sim 2^{2048}$

$p \sim 2^{2048}$

$g^a \sim 2^{2048}$

a is 2048 bits

→ cannot compute $g, g^1, g^2, \ldots, g^a$

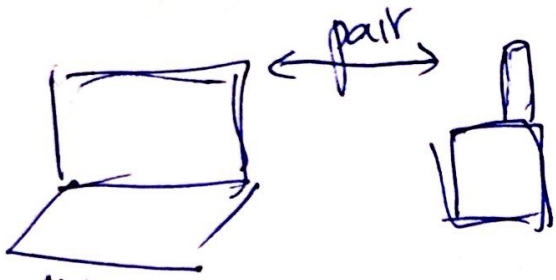
→ but use repeated squaring

$a =$ 10111 . . . . . (2048 bits)

MiTM prevention

1) Certificates [Later in class]

2)



Pairing devices

a, $g^a \bmod p$

b, $g^b \bmod p$

Device A displays code to user

$\| $

Shorter (K_{AE})

User inserts code in device B which checks code $\overset{?}{=}$ (shorter(K_{AB}))

If code mismatch $\Rightarrow$ MiTM attack