Asymmetric cryptography

PK_A, PK_B

Alice — C → Bob

Attacker

(PK_A, SK_A)

PK_A: public key known to everyone

SK_A: secret key only known to Alice

(PK_B, SK_B)

$Dec(SK_B, C) = M$

$\boxed{C = Enc(PK_B, M)}$

$M, PK_B \xrightarrow{Enc} C$

$\cancel{\longleftarrow}$

One-way functions (OWF)

A function f such that:

- given x, it is easy to compute $f(x)$ → polynomial time
- given y, it is hard to compute any x s.t. $f(x) = y$ → no polynomial time machine can compute

any x: Does not have to be the original x

$f(a,b) = 1$ Not OWF

$f(x) = x$ ✗ no, easy to invert

$f(x) = 1$ No because any x leads to 1

$f(x) = E_k(x)$ → block cipher with random secret key

YES, OWF

$f(a,b) = 1$

Discrete Log Problem (DLP) - OWF

large prime p (2048 bits) ; random $g \in [1, p-1]$

$\boxed{f(x) = g^x \bmod p}$

large numbers

Given y, not known how to compute any x s.t. $g^x \bmod p = y$

DLP necessary to hold

Diffie-Hellman Key Exchange (1976)

large prime p ; $g \in [1, p-1]$

Alice

$a \in [1, p-1]$ randomly chosen

secret key

public key $g^a \bmod p = PK_a$

$(PK_B)^a = (g^b \bmod p)^a \bmod p$

$= \boxed{g^{ab} \bmod p} = K_{ab}$

PK_A

PK_B

$g^a \bmod p$

$g^b \bmod p$

Bob

secret $b \in [1, p-1]$

public key $g^b \bmod p = PK_B$

$(PK_A)^b = (g^a \bmod p)^b \bmod p$

$= \boxed{g^{ab} \bmod p} = K_{ab}$

use them for symmetric-key enc

a, b, r chosen randomly

Assumption (informal): Decisional Diffie Hellman (DDH): given g^a, g^b, g^{ab} and g^a, g^b, g^r ; no attacker can distinguish

Use the agreed-upon symmetric key to communicate securely via symmetric-key encryption, which is preferable to public-key encryption because of

1. performance
2. cipher chaining modes allow encrypting arbitrary length

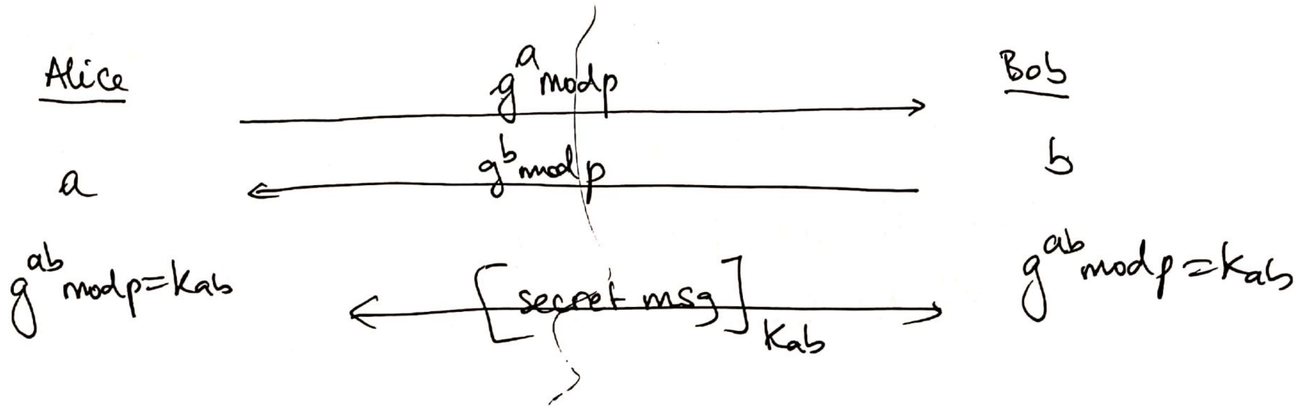
DDH:

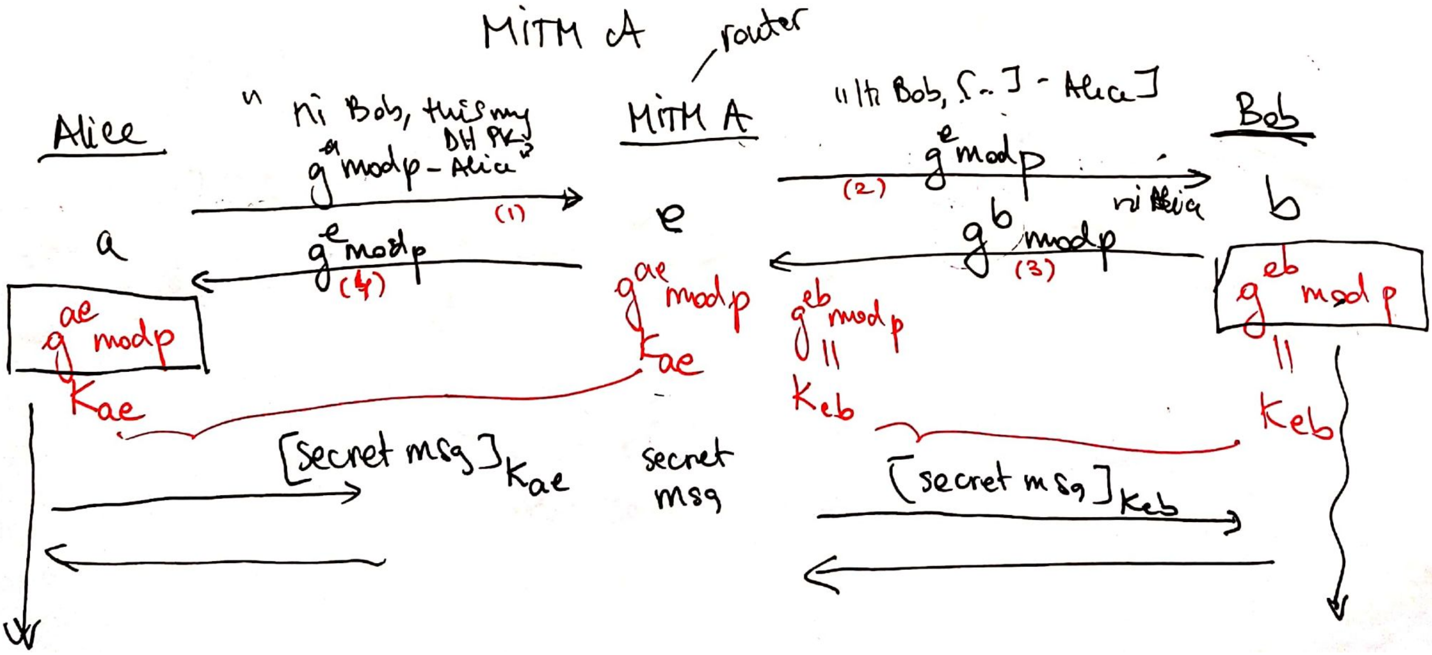
$$
\begin{array}{ccc}
\underline{\text{Cha}} & & \\
 & \xrightarrow{g^a,\, g^b,\, g^{ab}} & \text{Adv} \\
\$\ a, b, r & \text{OR} & ? \\
 & \xrightarrow{g^a,\, g^b,\, g^r} &
\end{array}
$$

Repeated squaring algorithm enable computing $g^x \bmod p$ (x ~ 2048 bits) in $\log p$ steps.

$g^2, (g^4), g^8, g^{16}$

Man-in-the-middle attack





Solutions

1) Certificates – LATER

2) Bob could publish PK on a trusted service

3) Displaying code | QR | English text to users so they check they agreed on same key