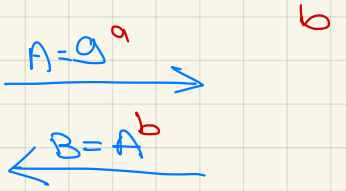
Outline

Digital Signature (over simplified version)

Hash function (over simplified version)

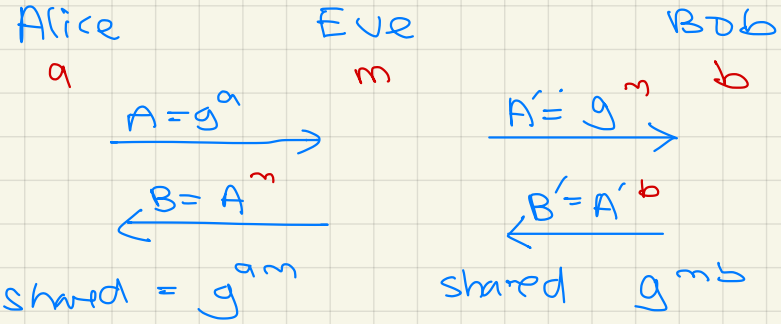
Motivation

DHP : Alice (a) Bob (b)



Shared value g^{ab}

man-in-the-middle attack



Eve acts as router between the two.

Solution : Digital Signature

Idea : Alice signs the message and sends to Bob
Bob signs the message and sends to Alice.
Given the signature signed by Alice, Bob can verify that it is indeed Alice who signs it and vice versa.

Concepts : Only the signer can produce that signature.
Everyone can verify it.

General idea:

To sign: private key + message = Signature

To verify: message + Signature + public key → True / False

RSA Digital Signature.

public : N, e

private : p, q, d

$N = pq$

$ed \equiv 1 \pmod{(p-1)(q-1)}$

$\gcd(e, (p-1)(q-1)) = 1$

Sign : $s = m^d \bmod N$

Send (m, s)

Verify : $m' = s^e \bmod N$

Accept m if m is equal to m'

Inefficient of signing long messages : the number of bits of signature could be as long as message.