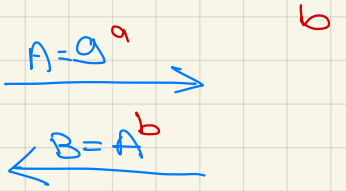
Outline

Digital Signature (over simplified version)

Hash function (over simplified version)

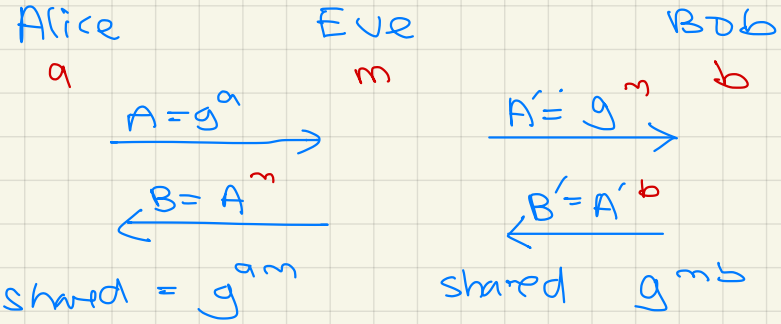
Motivation

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.

Hash Function

Hash : arbitrary length bitstring ⟶ fixed size bitstring

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 : $s = \text{hash}(m)^d \bmod N$

Send (m, s)

Verify : $m' = s^e \bmod N$
Accept m if $\text{hash}(m)$ is equal to m'

Properties of Hash

- Computation of hash(m) should fast and easy, linear time
- One way / pre-image resistant : Given any bit sting y, it should computationaly infeasible to find x such that $\text{hash}(x) = y$.

Given hash which outputs n bits, we would like hash to require $O(2^n)$ time to find preimage.

- Collision resistant : It should be infeasible to find two distinct x and x' such that

$$\text{hash}(x) = \text{hash}(x')$$

Given hash which outputs n bits, we expert to find a collision after $O(2^{n/2})$ trials.

$= O(\sqrt{2^n})$

Why one-way / Preimage resistance

If hash is not one-way.

Eve can compute

- $h' = r^e \bmod N$ where r' is some random integer
- compute preimage of h'

  $m = hash^{-1}(h')$
- Eve has (m, r) where everyone can verify that r is the valid signature for m signed by Alice.

Why collision-resistant

Suppose m_1 and m_2 have the same hash value.

m_1 = "Pay me \$5"

m_2 = "Pay me \$5000"

Alice signs m_1 with r

Signature r is also a valid signature of m_2 signed by Alice.

Eve takes (m_2, r) to the bank.

Birthday Paradox

In a random group of 40 people,

(a) what is the probability that someone has the same birthday as you?

(b) what is the probability that there exists at least two people with the same birthday?

(a) $\Pr(\text{some has same birthday as you})$

$= 1 - \Pr(\text{no one has the same birthday as you})$

$= 1 - \left(\frac{364}{365}\right)^{40}$

$\approx 10.4\%$

(b) $\Pr(\text{two people have the same birthday})$

$= 1 - \Pr(\text{all 40 people have different birthdays})$

$= 1 - \prod_{i=1}^{40} \Pr(\text{i-th person has different birthday than the previous } i-1 \text{ people})$

$= 1 - \frac{365}{365} \cdot \frac{364}{365} \cdot \frac{363}{365} \cdots \frac{326}{365}$

$\approx 89.1\%$

Remark:

(a) It requires 253 people to have better than 50% chance of finding a person with the same birthday.

(b) It requires 23 people to have better than 50% chance of finding two people with the same birthday.

Birthday Paradox

Suppose a bag of n balls, all of different colors.
We draw one ball at a time from the bag, write down the color, replace the ball into the bag and draw again.

The probability that after n balls are drawn, we obtained one matching color is

$$1 - \left(\frac{n}{n}\right)\left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right)\cdots\left(\frac{n-n+1}{n}\right)$$

Expected number of balls that we have to draw before we find a match is

$$\sqrt{\frac{\pi n}{2}} = O\left(\sqrt{n}\right)$$