DIS 4B

RSA: MOTIVATION

→ Alice wants to send a message to Bob without Eve being able to figure out what it is.

→ Alice uses public information to encode the message (no scheme agreed on beforehand)

→ Bob is the only one who can decode the message

how?, using mod arithmetic!

RSA

we define

p and q: 2 large primes → $N = pq$

e: relativey prime to $(p-1)(q-1)$

d: e^{-1} (mod $(p-1)(q-1)$)

then we have

public key: (N, e) ← Bob's public key, everyone knows

private key: d ← only Bob knows

$E(x) = x^e \pmod N$ (encryption)

$D(y) = y^d \pmod N$ (decryption)

Alice and Bob do the following:

1. Alice encrypts x, sends $y = E(x)$ to Bob
2. Bob decodes by computing $D(y) = x$

RSA: WHY DOES IT WORK?

① Bob can correctly decode the message.

Claim: $D(E(x)) = x$.

★ prove using FERMAT'S LITTLE THEOREM

$a^{p-1} \equiv 1 \pmod{p}$ for prime p

② Eve can't decode the message.

→ can't guess x from $x^e \pmod{N}$

(too many values to try)

→ can't factor $N = pq$ to calculate $d = e^{-1} \pmod{(p-1)(q-1)}$

p and q are large → N is large.

factoring is hard.