Fermat's little theorem

If p is a prime then,

$$a^{p-1} \equiv 1 \bmod p \quad \text{if } p \nmid a$$

$$a^{p} \equiv a \bmod p \quad \text{for every integer } a.$$

Ex^m $7^{222} \bmod 11$

Here $11 \nmid 7$ then by Fermat's little theorem.

$$7^{10} \equiv 1 \bmod 11$$

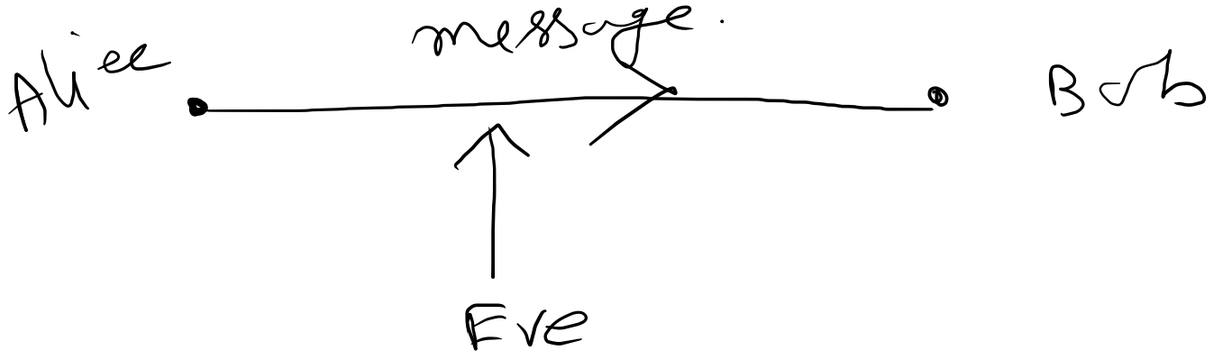
$$7^{222} \equiv \left(7^{10}\right)^{22} \cdot 7^{2} \mod 11$$

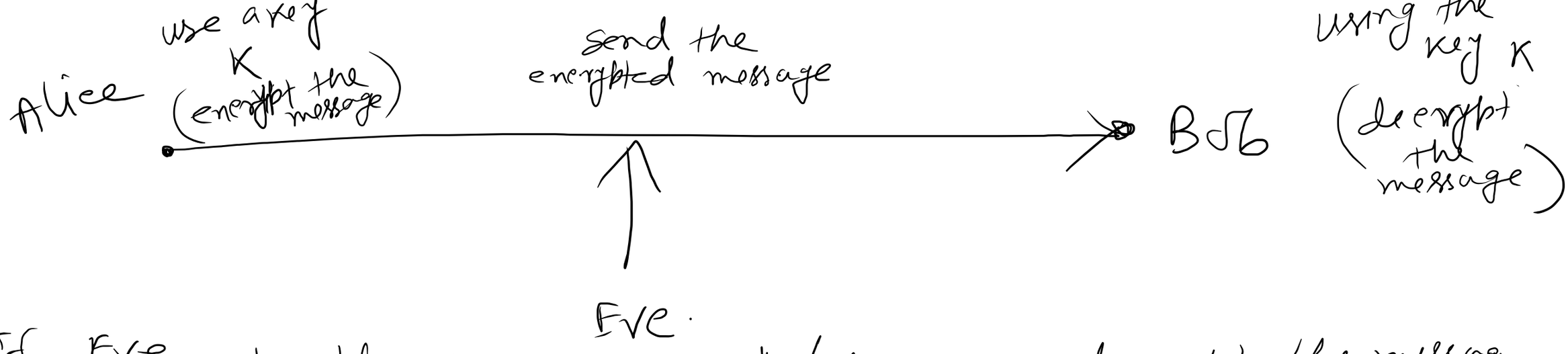
$$\equiv 1 \cdot 7^{2} \mod 11$$

$$\equiv 49 \mod 11$$

$$\equiv 5 \mod 11$$

Cryptography





If Eve gets the key K. then he/she can decrypt the message

Private key cryptosystem

Public key cryptosystem

Public keys.

send some keys.

Alice

Bob. (generates some keys) (send some of the keys to Alice)

uses Bob's public key.
to encrypt the message and send

- upon receiving the encrypted message uses its private key to decrypt the message.

cryptography:- It is encoding and decoding of messages.

plain text: The message that needs to be encoded.

cipher text: The encoded message.

Encryption: Process of encoding the message (plain to cipher)

Decryption: Process of decoding the message. (cipher to plain)

The caesar cipher

A	B	C	D	. . . .	Z
0	1	2	3	. . . .	25

Encoding some message.

$$c = x + 17 \mod 26$$

'HELLO' is the message.

H → 7 so $7 + 17 \mod 26 \equiv 24 \mod 26$ → Y

E → 4 $\equiv 21$ → V

C

C

F

HELLO ⟷ YVCCF

Decryption:

$$C \equiv x + 17 \mod 26.$$

$$x \equiv C - 17 \mod 26$$

YVCCF

Y → 24 $\quad 24 - 17 \mod 26 \equiv 7 \mod 26 \rightarrow$ H

V E

C L

C L

F O

RSA cryptosystem

It is a public key cryptosystem.

In RSA there are two phases.

Phase 1: key generation.

- choose two large primes p and q. (secret)
- compute $n = pq$ and $K = (p-1)(q-1)$
- choose e such that $\gcd(e, K) = 1$
- choose $d \equiv e^{-1} \bmod K$

n and e are public keys.
d is the private key.

Phase 2: Encryption and decryption.

Encryption

- A message M needs to send $\quad m < n$
- compute $C \equiv M^e \bmod n$
- send C to Bob.

Decryption

. compute $M = C^d \bmod n$

Exm $p = 5$, $q = 11$

$n = pq = 5 \times 11 = 55$ $\quad k = 4 \times 10 = 40$

choose e such that $\gcd(e, k) = 1$

let us take e as 3

compute $d \equiv e^{-1} \bmod k$ $\quad d \equiv 3^{-1} \bmod 40$

$\Rightarrow d = 27$

(n, e) are public keys ie, $(55, 3)$

d is private key ie, 27