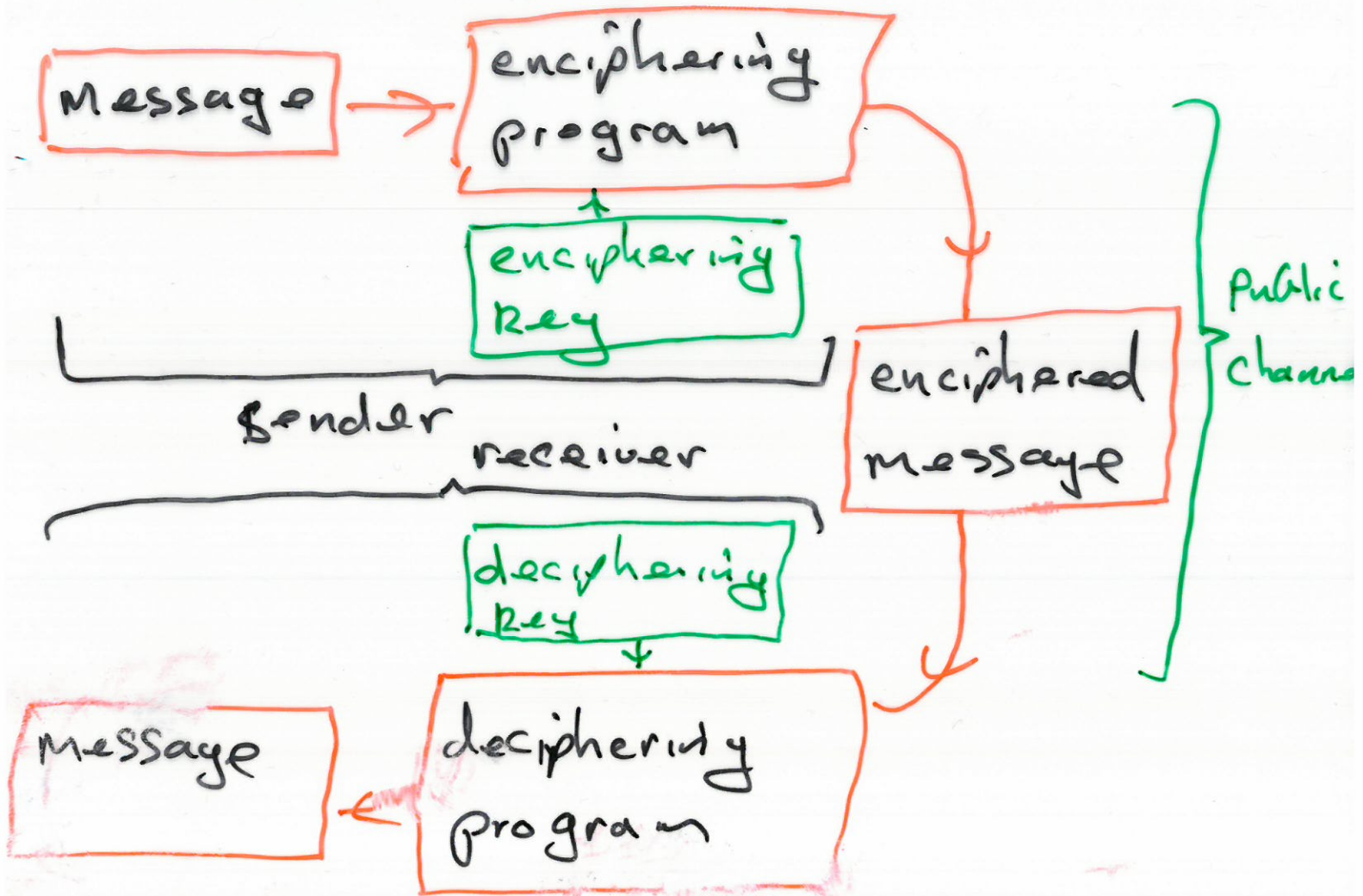


Cryptography



Basic assumptions

- 1) Encrypting and decrypting programs are public knowledge
- 2) keys are kept secret
- 3) encoded message will be intercepted.

Example

Receiver: Pay Pal
Sender: you at home
Channel: internet wire/wifi
alphabet: A, B, C, ..., Z
plaintext: HELLO

Enciphering Program

A	$\longleftrightarrow$	1
B	$\longleftrightarrow$	2
C	$\longleftrightarrow$	3
$\vdots$		
Y	$\longleftrightarrow$	25
Z	$\longleftrightarrow$	0

alphabet = $\mathbb{Z}_{26}$ = numbers on a 26-hour clock

Enciphering key: $E = (3, 4)$

Enciphering program :

$$f_E: \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}, n \mapsto 3n + 4$$

HELLO $\longleftrightarrow$ 8 5 12 12 15

$\xrightarrow{f_E}$ 2 19 14 14 23

$\longleftrightarrow$ B S N N W

Deciphering
key :

Some pair of
integers $D = (\alpha, \beta)$

Deciphering
procedure :

$$f_D: \mathbb{Z}_{26} \longrightarrow \mathbb{Z}_{26}, n \mapsto \alpha n + \beta$$

Encipher

$$n \rightsquigarrow 3n \rightsquigarrow \overbrace{3n+4}^m$$

Decipher

$$m \rightsquigarrow m-4 \rightsquigarrow 3^{-1}(m-4)$$

what is $3^{-1} \bmod 26$?

Answer $3^{-1} \equiv 9 \bmod 26$

(because $3 \times 9 \equiv 1 \bmod 26$)

Deciphering function:

$$f_D(m) = 3^{-1}(m-4)$$

$$\equiv 9(m-4)$$

$$\equiv 9m - 36$$

$$\equiv 9m - 10$$

$$\equiv 9m + 16$$

Deciphering
key :

$$D = (9, 16)$$