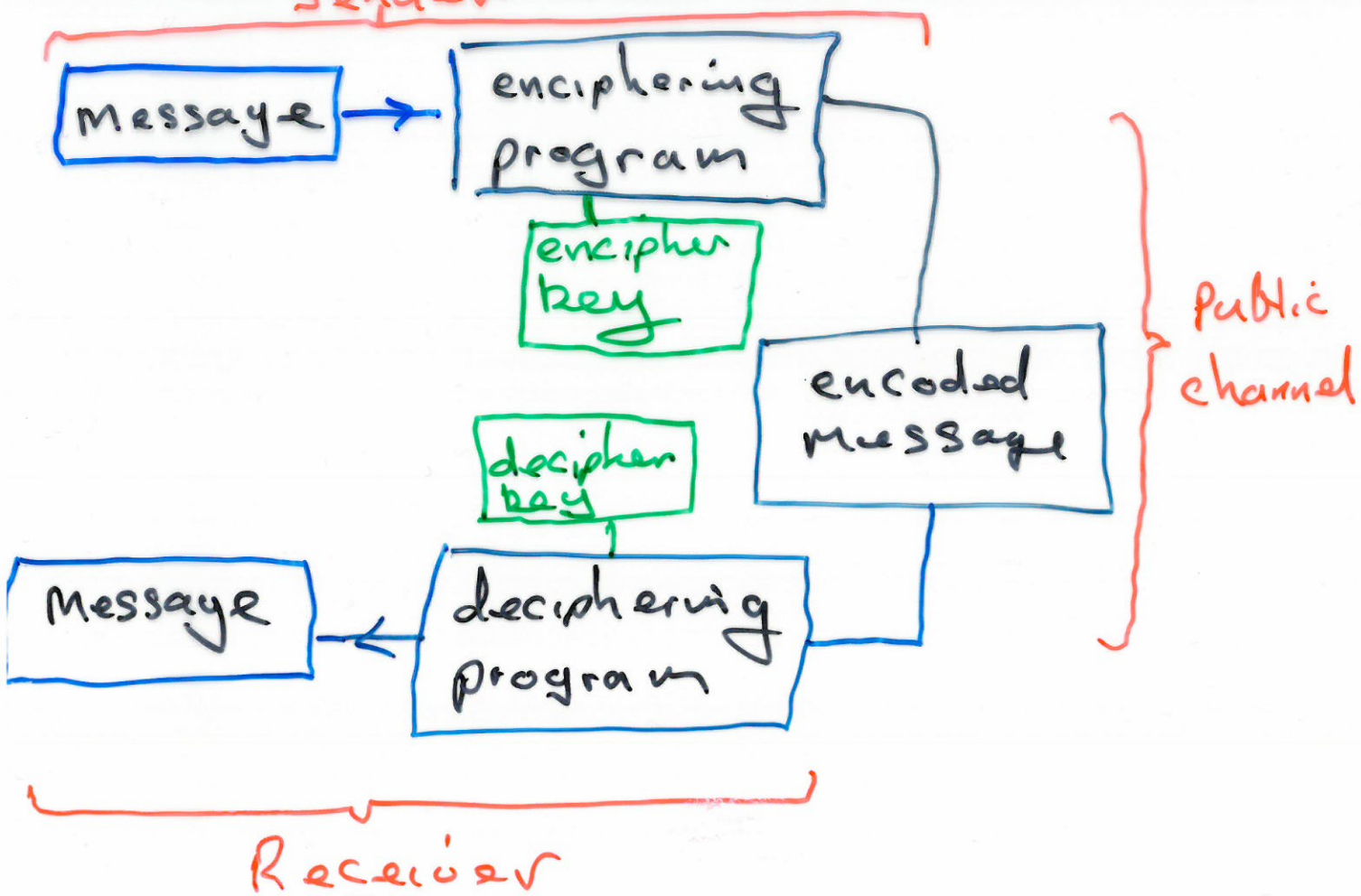
Cryptography



Basic Assumptions

1) Enciphering & deciphering 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 line & Wifi

alphabet : A, B, C, ..., Z

message units : single letter

plain text : HELLO

Enciphering Program

A ⟷ 1

B ⟷ 2

⋮

Y ⟷ 25

Z ⟷ 0

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

Enciphering key : $(3, 4)$

Enciphering procedure :

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

HELLO $\longleftrightarrow$ 8 5 R 12 15

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

$\longleftrightarrow$ B S N N W

encoded message.

Deciphering key : some pair of integers (α, β)

Deciphering procedure :

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

Encipher :

$$n \longrightarrow 3n \longrightarrow \underbrace{3n+4}_{m}$$

Decipher

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

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

$$3 \times 9 \equiv 1 \pmod{26}$$

So $3^{-1} \equiv 9 \pmod{26}$

Deciphering function

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

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

$$\equiv 9m - 10$$

$$\equiv 9m + 16$$

Deciphering key : $(\alpha, \beta) = (9, 16)$