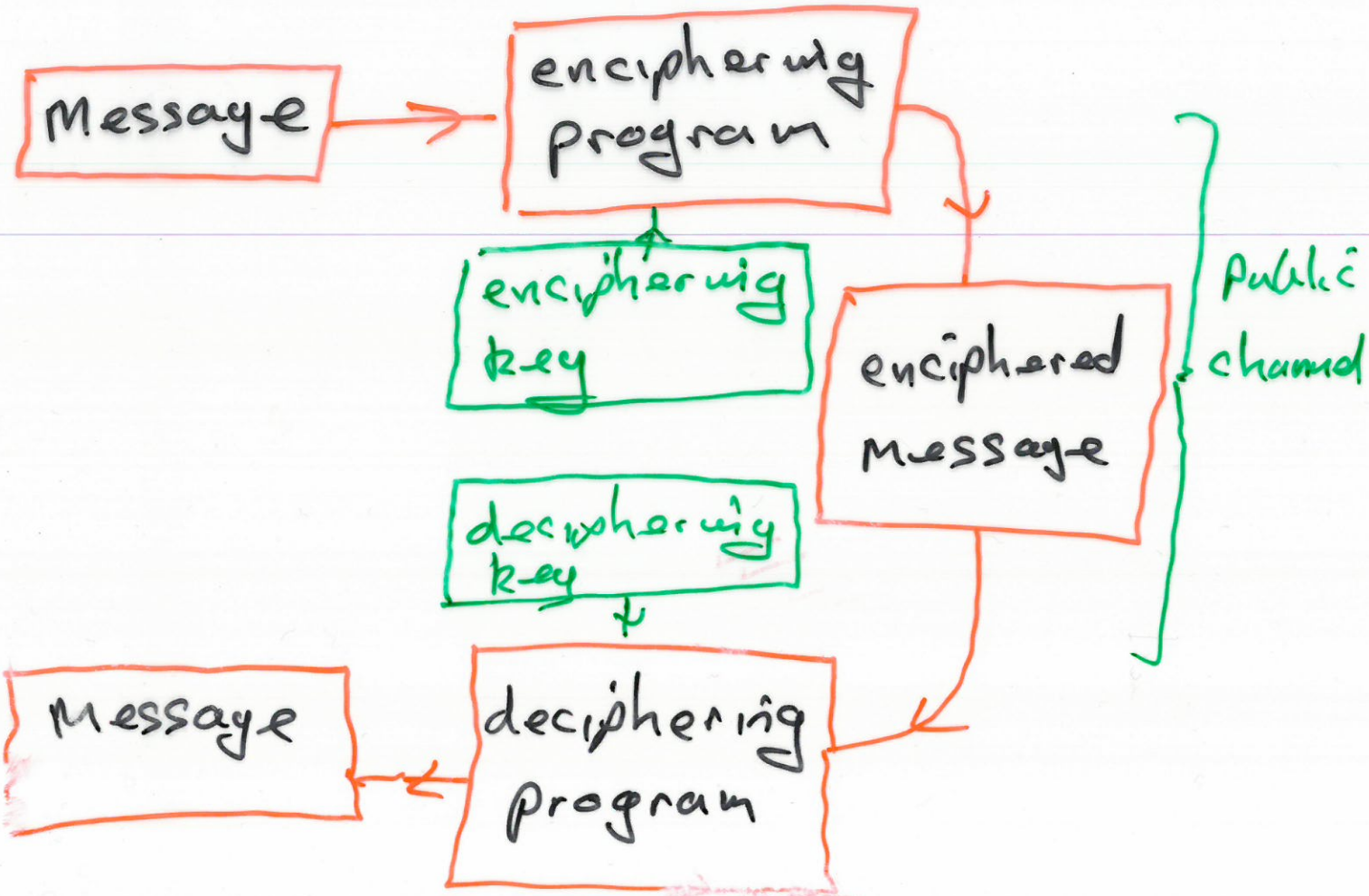
Cryptography



Basic assumptions

1) Enciphering & deciphering programs are public knowledge
2) keys are kept secret.
3) Enciphered message will be intercepted.

Example

Receiver : Pay Pal

Sender : you at home

channel : internet line / wifi

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

plaintext : HELLO

Enciphering program

A $\longleftrightarrow$ 1

B $\longleftrightarrow$ 2

C $\longleftrightarrow$ 3

⋮

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 $\leftrightarrow$ 8 5 12 12 15

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

$\leftrightarrow$ B S N N W

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

Deciphering procedure:

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

In this example with $E = (3, 4)$ what should $D = (\alpha, \beta)$ be?

Encipher:

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

Decipher:

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

What is 3^{-1} mod ?

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

because $3 \cdot 9 \equiv 1 \mod 26$

Deciphering function:

$$f_D(m) = 3^{-1}(m-4)$$
$$= 9(m-4)$$
$$= 9m - 10$$
$$= 9m + 16.$$

Deciphering key is $D = (9, 16)$.