How do we find the inverse of, say, 15 mod 26 ?

We first use Euclid's algorithm to calculate gcd(15, 26) = 1.

$26 = 1 \times 15 + 11$

$15 = 1 \times 11 + 4$

$11 = 2 + 4 + 3$

$4 = 1 \times 3 + 1$ = gcd(15, 26)

$3 = 3 \times 1 + 0$

To find 15^{-1} mod 26 do as follows

$$1 = 4 - 3$$

$$= 4 - (11 - 2 \cdot 4)$$

$$= 3 \cdot 4 - 11$$

$$= 3(15 - 11) - 11$$

$$= -4 \cdot 11 + 3 \cdot 15$$

$$= -4(26 - 15) + 3 \cdot 15$$

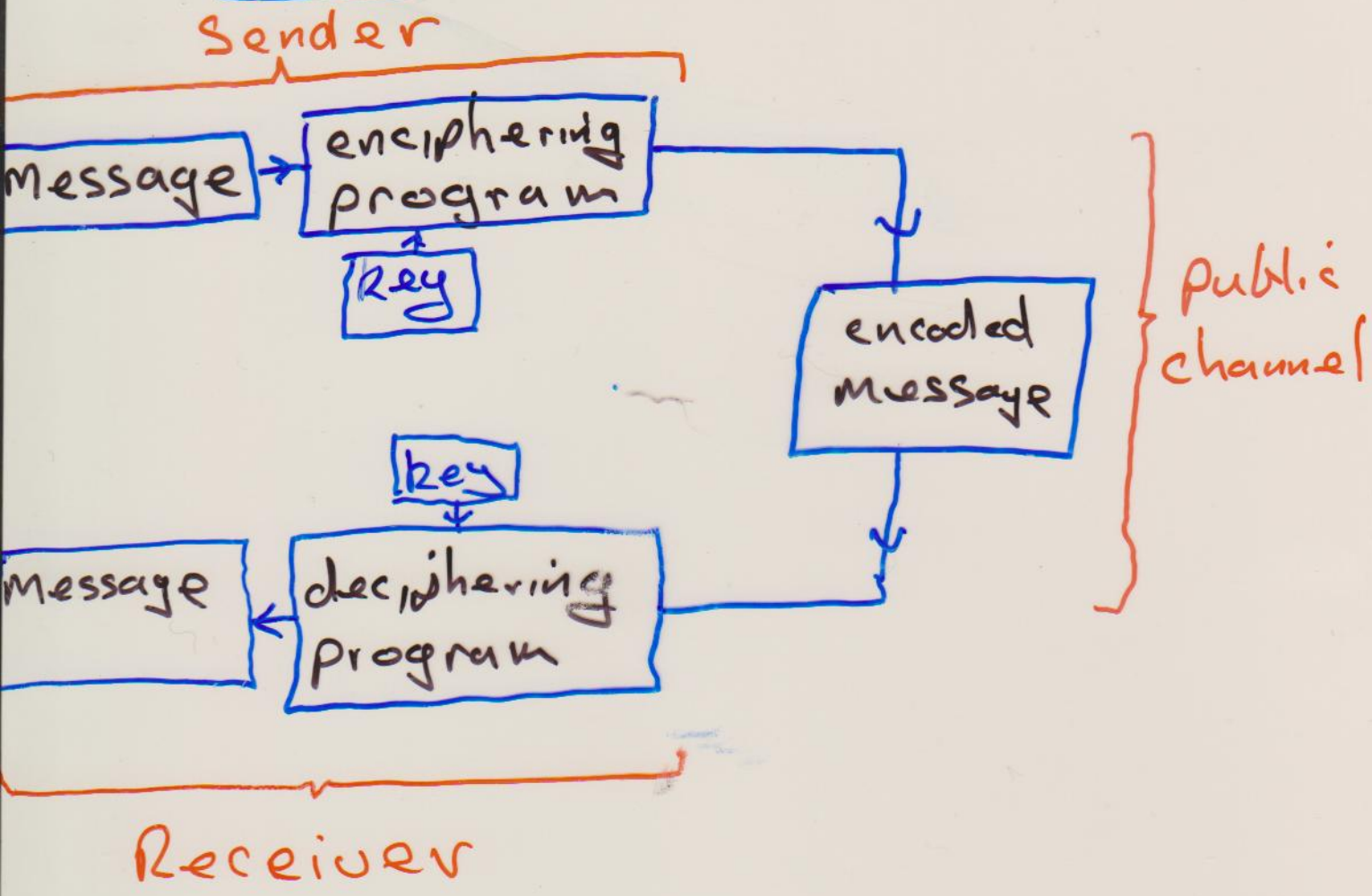
$$= -4 \cdot 26 + 7 \cdot 15$$

$$\equiv 7 \cdot 15 \pmod{26}$$

Hence $15^{-1} \equiv 7 \pmod{26}$.

Third Application

CRYPTOGRAPHY



Basic Assumptions

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

Example

Receiver : Amazon.com

Sender : you at home

channel : internet line

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

message units : single letters

plain text : HELLO

Enciphering Procedure

A $\longleftrightarrow$ 1

B $\longleftrightarrow$ 2

⋮

Y $\longleftrightarrow$ 25

Z $\longleftrightarrow$ 0

Alphabet : $\mathbb{Z}_{26}$

Enciphering key : (3, 4)

Enciphering program :

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

HELLO $\longrightarrow$ 8 5 12 12 15

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

$\longrightarrow$ B S N N W

Deciphering program

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

Deciphering key : some choice of α and β

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

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

what is 3^{-1} mod 26 ?

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

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

Deciphering function is

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

Deciphering key : $(9, 16)$