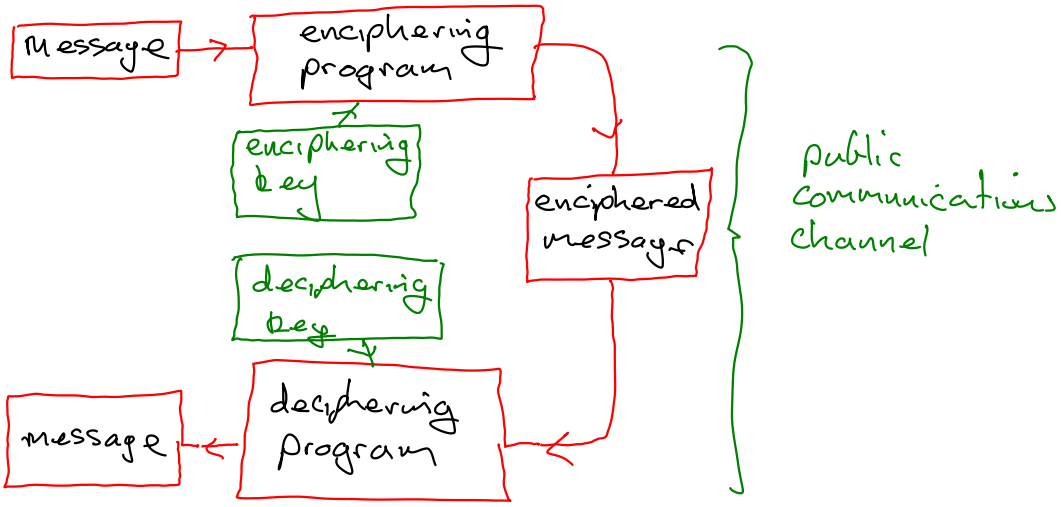
Yesterday

we find n^{-1} mod m by first using the Euclidean algorithm to compute $\gcd(n, m) = 1$.

Conclusion: n^{-1} mod m exists if, and only if, $\gcd(n, m) = 1$.

Cryptography



Basic Assumptions

1) Enciphering and deciphering programs are public knowledge.

2) Keys are kept secret

3) Enciphered messages will be intercepted.

Example

Receiver : PayPay

Sender : you at home

channel : internet line + LAN

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

plaintext : HELLO

Enciphering Program

A ↔ 1
B ↔ 2
C ↔ 3
⋮
Y ↔ 25
Z ↔ 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 ↔	8	5	12	12	15
$\xrightarrow{f_E}$	2	19	14	14	23
↔	B	S	N	N	W

Ciphertext

Deciphering key : Some pair of integers

$D = (\alpha, \beta)$

Deciphering function :

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

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

Encipher

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

Decipher

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

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

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

Deciphering function:

$$\begin{aligned} f_D(k) &\equiv 3^{-1}(k-4) \bmod 26 \\ &\equiv 9(k-4) \\ &\equiv 9k - 10 \\ &\equiv 9k + 16 \end{aligned}$$

Deciphering key is

$D = (9, 16)$.