IBAN

GB 82 WEST 12345698765432

GB: Country Code

82: two check digits

WEST 12345698765432: Bank Sort Code + account number

Three steps to validate an IBAN

1) Rearrange

WEST 123456 98765432 GB 82

2) Convert letters to numbers

A ~ 10, B ~ 11, ..., Z ~ 35

32 14 28 29 123456 98765432 16

11 82

3) Calculate this number mod 97

The number mod 97 must equal 1 if the IBAN is correct.

How should we compute the mod 97 value of a big number such as 4321.

One method

Just divide 4321 by 97 and record the remainder.

Alternatively

$$4321 =$$

$$4 \times 1000 + 3 \times 100 + 21$$

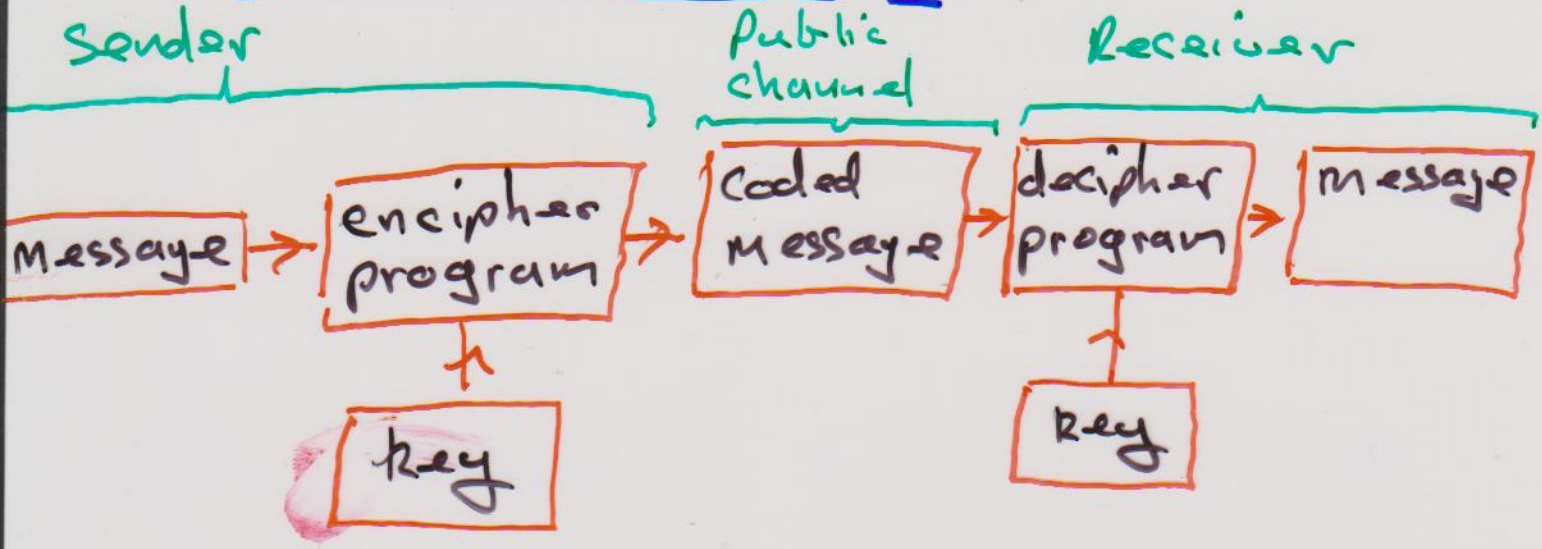
$$\equiv 4 \times 30 + 3 \times 3 + 21 \pmod{97}$$

$$\equiv 23 + 9 + 21 \pmod{97}$$

$$\equiv 53$$

Third Application:

CRYPTOGRAPHY



Basic assumptions

1) enciphering/deciphering program is public knowledge
2) keys are secret/private
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
C $\longleftrightarrow$ 3
⋮
Z $\longleftrightarrow$ 0

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

Enciphering key : (3, 4)

Enciphering program

$$f : \mathbb{Z}_{26} \to \mathbb{Z}_{26},\ n \mapsto 3n + 4$$

HELLO → 8 5 12 12 15

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

→ B S N N W

Deciphering key : $(9, 16)$

Deciphering program

$$f' : \mathbb{Z}_{26} \to \mathbb{Z}_{26}, n \mapsto 9n + 16$$

Note :

$$f'(f(n)) = f'(3n + 4)$$

$$= 9(3n + 4) + 16 \mod 26$$

$$\equiv n + 10 + 16 \mod 26$$

$$\equiv n$$