MA 190 Applications - cryptography

enciphering Key

Messages → some enciphering program → broadcast enciphered message

[public communications channel]

message ← some deciphering program ← Reciever enciphered message

deciphering Key

enigma machine → cipher keys were rotor positions

modern comms tech → long integer

Basic Assumptions

- Enciphering & deciphering programs are public knowledge
- Keys are kept secret
- Enciphered message will be intercepted

First example (note: oversimplified)

all public knowledge:
- Reciever : eg Paypal
- Sender : customer
- Public Communications Channel : internet line & wifi
- Alphabet : Capital Latin Letters (26 chars)

hidden:
- Plaintext : "HELLO"
- Enciphering program:

A	B	C	[	]	Y	Z
1	2	3	[...]		25	0

alphabet : $\mathbb{Z}_{26}$: numbers on a 26 hour clock

- Enciphering Key : E : (3, 4)

ENCIPHERING PROGRAM : $f_E : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$, $n \longmapsto 3n + 4$

$\hookrightarrow an + b$, where a and b are given by E

HELLO
↓↓↓↓↓
8 5 12 12 15

$(3(8)+4), (3(5)+4), (3(12)+4), (3(12)+4), (3(15)+4)$

$28 \quad 19 \quad 40 \quad 40 \quad 59 \longrightarrow [\bmod 26]$

$\equiv 2 \quad 19 \quad 14 \quad 14 \quad 23 \pmod{26}$

↓ ↓ ↓ ↓ ↓

B S N N W

ENCIPHERED TEXT : BSNNW

("ciphertext")

DECIPHERING KEY : D - some pair of integers. (α, β)

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

MA 190 In this example with $E:(3,4)$, what should $D:(a,\beta)$ be?

Encipher

$$n \longmapsto \overbrace{3n+4}^{m}$$

Decipher

$$m \longmapsto (m-4)\,3^{-1} \mod 26$$

$$\equiv 9(m-4) \mod 26$$

$$f_D(m) \equiv 3^{-1}(m-4) \mod 26$$

$$\equiv 9m - 10 \mod 26$$

$$\equiv 9m + 16 \mod 26$$

$$\therefore D(9,16)$$

MA 190

↳ gonna put up a podcast about the homework later

Problem (note, O, not 0)

You intercept the following ciphertext - "OH7F86BB46R3627026BB9"

And you know the following:

1) 37-letter alphabet

↳ 0, 1, 2, [...], 9, A=10, B=11, [...], Z=35, ␣ (␣ is space)

2) An affine cryptosystem is used on single-letter message units with $E(\alpha, \beta)$

$x \longmapsto \alpha x + \beta \mod 37$

3) plaintext ends with BB7

↳ $7 \longmapsto 9$

$0 \longmapsto B$

Enciphering function:

$x \longmapsto \alpha x + \beta \mod 37$

$0 \longmapsto \alpha 0 + \beta \mod 37 \equiv B$

$11 \equiv \beta$

$7 \longmapsto \alpha 7 + 11 \mod 37 \equiv 9$

$7\alpha \equiv 35 \mod 37$

Euclidean Algorithm: $\alpha \equiv 7^{-1} \cdot -2 \mod 37$

$37 = 5 \cdot 7 + 2$ ← gcd

$7 = 3 \cdot 2 + 1$

$1 = 7 - 3 \cdot 2$

$1 = 7 - 3(37 - 5 \cdot 7)$

$1 = 16 \cdot 7 - 3 \cdot 37$

$1 \equiv 16 \cdot 7 \mod 37$ → $7^{-1} \mod 37 = 16$

$\alpha \equiv 7^{-1} \cdot -2$

$\alpha \equiv 16 \cdot -2$

$\alpha \equiv -32 \equiv 5 \mod 37$ → [E (5, 11)]

$f_E : x \longmapsto 5x + 11$

$f_D : y \longmapsto (y - 11) \cdot 5^{-1}$

$: y \longmapsto (y - 11)15$

↳ $15y - 17 \equiv 15x + 20$ → [D (15, 20)]

GA: $37 = 7 \cdot 5 + 2$, $5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2$

$1 = 5 - 2(37 - 7 \cdot 5)$

$1 = 15 \cdot 5 - 2 \cdot 37$

$5^{-1} \equiv 15 \mod 37$

ciphertext: OH7F86BB46R3627026BB9

↓

$15 \cdot 24 + 20$

↓

$\equiv 15 \cdot 2 \cdot 12$

$\equiv 30 \cdot 12$

$\equiv -7 \cdot 12$