

Problem: you intercept the ciphertext

O H 7 F 8 6 B B 4 6 R 3 6 2 7 0 2 6 B B 9

ciphertext

and you know:

$\phi \phi 7$

plaintext

1) A 37-letter alphabet is used

$\phi, 1, 2, 3, 4, 5, 6, 7, 8, 9, A=10, B=11, \dots, Z=35, _=36$

2) An affine cryptosystem

$$x \mapsto \alpha x + \beta \pmod{37}$$

is used on single letter message units
with enciphering key $E = (\alpha, \beta)$

3) plaintext ends $\phi \phi 7$

Enciphering function

$$x \mapsto \alpha x + \beta \pmod{37}$$

$$\phi \mapsto \alpha \phi + \beta = 8$$

$$\phi \mapsto \beta = 11$$

$$7 \mapsto 7\alpha + \beta = 9$$

$$\begin{aligned} 7\alpha + \beta &= 9 \pmod{37} \\ \beta &= 11 \end{aligned}$$

$$7\alpha = -2$$

$$\alpha = 7^{-1}(-2) \pmod{37}$$

To find $7^{-1} \pmod{37}$ we use the Euclidean algorithm.

$$37 = 5 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1 \leftarrow \gcd(7, 37)$$

$$1 = 7 - 3 \cdot 2$$

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

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

$$\equiv 16 \cdot 7 \pmod{37}$$

so $7^{-1} \equiv 16 \pmod{37}$

$$\alpha = 7^{-1}(-2) \equiv 16(-2) \equiv -32 \equiv 5$$

$$\alpha = 5, \beta = 11$$

Deciphering function

$$Y \mapsto 5^{-1}(Y-11) \pmod{37}$$

What is $5^{-1} \pmod{37}$

$$37 = 7 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

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

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

$$\equiv 15 \cdot 5 \pmod{37}$$

$$\boxed{5^{-1} \equiv 15 \pmod{37}}$$

Deciphering function:

$$Y \mapsto 5^{-1}(Y-11) \pmod{37}$$

$$\equiv 15(Y-11) \pmod{37}$$

$$\equiv 15Y - 165 \pmod{37}$$

$$\equiv 15Y - 17$$

$$\equiv 15Y + 20$$

$$\boxed{-17 \equiv +20 \pmod{37}}$$

Deciphering key $D = (15, 20)$.

Now we need to decipher the ciphertext, one letter at a time.

$$0 \mapsto 15 \cdot 0 + 20 \pmod{37}$$

$$0 = 24$$

$$\begin{array}{r} 240 \\ 120 \\ \hline 360 \end{array}$$

$$24 \mapsto 15 \cdot 24 + 20 \pmod{37}$$

$$= 360 + 20 \pmod{37}$$

$$= 380 \pmod{37}$$

$$\equiv 10 \pmod{37}$$

$$= A$$