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

and you know:

1) A 37-letter alphabet was used

$\phi, 1, 2, \cdots, 9, A=10, B=11, \cdots, Z=35, \_=36$

2) An affine cryptosystem

$$X \longmapsto \alpha X + \beta$$

is used on single letter message units with enciphering key (α, β).

3) Plaintext ends with $\phi\phi 7$

Decipher the message.

Solution

Enciphering procedure

"number zero"

$\phi \longmapsto B$

$7 \longmapsto 9$

$11 = \alpha\phi + \beta$

$9 = \alpha 7 + \beta$

Thus

$\boxed{\beta = 11}$

$9 \equiv 7\alpha + \beta \mod 37$

$-2 \equiv 7\alpha \mod 37$

$35 \equiv 7\alpha \mod 37$

"So"

$\boxed{\alpha = 5}$

The enciphering function is

$$X \longmapsto 5X + 11$$

The deciphering function is

$$X \longmapsto 5^{-1}(X - 11)$$

To calculate $5^{-1} \bmod 37$ we first note that

$$\gcd(5, 37) = 1.$$

Let's use the Euclidean algorithm to compute $\gcd(5, 37)$.

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

$$5 = 2 \cdot 2 + \boxed{1} \quad \gcd(37, 5)$$

$$2 = 2 \cdot 1 + 0$$

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

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

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

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

Thus

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

Deciphering function is

$$X \longmapsto 5^{-1}(X - 11)$$

$$\equiv 15(X - 11)$$

$$\equiv 15X - 15.11$$

$$\equiv 15X - 17$$

$$\equiv 15X + 20$$

Deciphering function is

$$X \longmapsto 15X + 20 \mod 37$$