Problem

You intercept the ciphertext

OH7F86BB46R3627026BB9

and you know:

1) A 37-letter alphabet is used

$\phi, 1, 2, \ldots, 9, A=10, B=11, \ldots, Z=35, -=36$

2) An affine cryptosystem

$$X \longmapsto \alpha X + \beta \pmod{37}$$

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

$\phi \longmapsto B$

$7 \longmapsto 9$

$11 \equiv \alpha \cdot \phi + \beta$

$9 \equiv \alpha \cdot 7 + \beta$

Thus

$\boxed{\beta \equiv 11}$

$9 \equiv 7\alpha + 11$

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

$35 = 7\alpha \mod 37$

"So"

$\boxed{\alpha = 5}$

The enciphering function is

$$X \longmapsto 5X + 11 \mod 37$$

The deciphering function is

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

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

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

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

$$37 = 7.5 + 2$$

$$5 = 2.2 + 1 \qquad \gcd(5, 37)$$

$$1 = 5 - 2.2$$

$$= 5 - 2.(37 - 7.5)$$

$$= -2.37 + 15.5$$

$$\equiv 5.15 \pmod{37}$$

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

Deciphering function is :

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

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

$$\equiv 15X - 15.11$$

$$\equiv 15X - 17$$

$$\equiv 15X + 20 \pmod{37}.$$

Deciphering function is ;

$$X \longmapsto 15X + 20 \pmod{37}.$$