Problem

You intercept the ciphertext

OH7F86BB46R3627026BB9
A ϕϕ7

and you know:

1) A 37-letter alphabet is used

ϕ, 1, 2, ..., 9, A=10, B=11, ..., Z=35, _=36

2) An <u>affine</u> cryptosystem

$$X \longmapsto \alpha X + \beta \quad \text{Mod } 37$$

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

3) plaintext ends with ϕϕ7

Enciphering function

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

$\phi \longmapsto \alpha\phi + \beta = B$

$0 \longmapsto \boxed{\beta = 11}$

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

$\boxed{7\alpha + \beta = 9}$

$7\alpha + \beta = 9 \pmod{37}$

$\beta = 11$

$7\alpha = -2$

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

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

$37 = 5 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$ ✓

$1 = 7 - 3 \cdot 2$

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

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

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

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

$\boxed{\beta = 11}$

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

$\equiv (16)(-2)$

$\equiv -32 \pmod{37}$

$\boxed{\alpha_1 \equiv 5}$

Deciphering function is :

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

$$= 15(Y - 11)$$

$$= 15Y - 165$$

$$= 15Y - 17$$

$$= 15Y + 20 .$$

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

Now let's decipher :

$$O = 24$$

$$24 \mapsto 15.24 + 20$$

$$= 27 + 20$$

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

$$= A$$

Enciphering function

$$x \longmapsto \underbrace{5x + 11}_{y}$$

Deciphering function:

$$y \longmapsto 5^{-1}(y - 11) \mod 37$$

What is $5^{-1} \mod 37$:

$37 = 7 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$ ✓

$1 = 5 - 2 \cdot 2$

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

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

$\equiv 15 \cdot 5 \mod 37$

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