Problem

You intercept the ciphertext

OH7F86BB46R36270216BB9
ϕϕ7

and you know:

1) A 37 letter alphabet is used

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

2) An affine cryptosystem

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

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

3) plaintext ends with ϕϕ7

Decipher the message.

Sol^n

Enciphering function

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

$\phi \longmapsto \alpha\phi + \beta = B$ (Because $\phi\phi 7 \longmapsto BB9$)

$0 \longmapsto \beta = 11$

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

$7\alpha + \beta = 9$

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

$\beta = 11$

$7\alpha = -2$

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

To find $7^{-1} \pmod{37}$

Let's use the Euclidean algorithm:

$37 = 5.7 + 2$

$7 = 3.2 + 1$

$1 = 7 - 3.2$

$= 7 - 3(37 - 5.7)$

$= 16.7 - 3.37$

$\equiv 16.7 \pmod{37}$

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

So $\boxed{\beta = 11}$

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

$\boxed{\alpha = 5}$

Enciphering function is:

$X \longmapsto 5X + 11$

Deciphering function:

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

What is $5^{-1} \bmod 37$.

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

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

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(37 - 7 \cdot 5) \\ &= 15 \cdot 5 - 2 \cdot 37 \\ &\equiv 15 \cdot 5 \pmod{37} \end{aligned}$$

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

Deciphering function:

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

$$= 15x - 15 \cdot 11$$

$$= 15x - 17$$

$$\boxed{= 15x + 20} \quad \text{mod } 37$$

Let's now decipher:

$$O = 24$$

$$24 \longmapsto 15 \cdot 24 + 20$$

$$= 27 + 20$$

$$= 10 \quad \text{mod } 37$$

$$= A$$

The first letter of the message is "A".

etc.