Problem

You intercept the ciphertext

OH7F86BB46R3627026BB9
ØØ7

and you know:

1) A 37-letter alphabet is used

Ø, 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 ØØ7

Decipher the message.

Enciphering function

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

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

$0 \longmapsto \beta = 11$

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

$7\alpha + \beta = 9$

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

$\beta \equiv 11$

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

$\alpha \equiv (7^{-1})(-2) \mod 37$

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

Let's use the Euclidean algorithm:

$37 = 5.7 + 2$

$7 = 3.2 + 1 = \gcd(37, 7)$

$1 = 7 - 3.2$

$= 7 - 3.(37 - 5.7)$

$= 16.7 - 3.37$

$\equiv 16.7 \mod 37$

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

$\beta = 1$

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

$\equiv (16)(-2)$

$\equiv -32 \mod 37$

$\equiv 5$

$\alpha = 5$

Enciphering function is

$$X \longmapsto 5X + 11$$

Deciphering function:

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

what is $5^{-1} \mod 37$.

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

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

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

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

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

$$\equiv 15 \cdot 5 \mod 37$$

Deciphering function is:

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

$$= 15X - 15 \cdot 11$$

$$\equiv 15X - 17$$

$$\equiv \boxed{15X + 20}$$

Now let's decypher :

$O = 24$

$24 \longmapsto 15.24 + 20$

$\equiv 27 + 20$

$\equiv 10 \mod 37$

$= A$.

The message begins with

A . . . . .