Question How do we find $5^{-1} \bmod 37$?

Answer

Step 1: use Euclidean algorithm to show $1 = \gcd(5, 37)$

Step 2: use output from the algorithm to find a number a such that

$$5 \cdot a \equiv 1 \bmod 37$$

Step 1

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

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

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

Step 2

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

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

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

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

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

Example

You intercept the ciphertext

OH7F86BB46R3627026BB9 ... ØØ7

and you know:

1) A 37-letter alphabet was used

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

2) Affine enciphering function

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

is used on single letter message units.

3) Plaintext ends with $\phi\phi$

Decipher the message.

Solution

Enciphering procedure

$\phi \longmapsto B = 11$ | $11 = \alpha \cdot 0 + \beta$

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

$\boxed{\beta = 11}$

$9 = 7\alpha + 11 \mod 37$

$-2 = 7\alpha \mod 37$

$35 = 7\alpha \pmod{37}$

$\boxed{\alpha = 5}$

The enciphering function is

$$\boxed{X \longmapsto 5X + 11 \pmod{37}}$$

The deciphering function is

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

Need to find $5^{-1} \pmod{37}$

$$5^{-1} = 15$$

Deciphering function

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

$$\boxed{X \longmapsto 15X - 17}$$

To decipher

$$O = 24 \longmapsto 15.24 - 17$$

$$= -10 - 17$$

$$= -27$$

$$= 10$$

$$= A$$

"A" is the first letter of plaintext.

How can we overcome the method of frequency analysis for cracking the above type of code?