basic-mod2

picoCTF 2022
Tags: Cryptography

Diberikan sebuah file *message.txt*. File tersebut berisi sebuah barisan yang memiliki beberapa angka.

```
104 290 356 313 262 337 354 229 146 297 118 373 221 359 338 321 288 79 214
277 131 190 377
```

Kita diminta untuk mencari sisa bagi setiap angka ketika dibagi 41 dan mencari inverse modulo nya. Lalu mencocokan hasil tersebut menjadi barisan karakter dimana

- 1 – 26 untuk huruf besar alfabet
- 27 – 36 untuk angka desimal
- 37 untuk garis bawah (*underscore*).

Definisi dari inverse modulo sendiri adalah

$$AX \cong 1 \ (mod\ M)$$

Untuk A, M, dan X merupakan bilangan bulat dengan X dalam rentang $\{1,2,\dots,M-1\}$. Hasil dari inverse modulo A oleh M yaitu X.

Berdasarkan definisi tersebut, maka dapat diartikan bahwa kita perlu mencari X tiap A_i, dimana $A = [104, 290, 356, 313, 262, 337, 354, \dots, 131, 190, 377]$ dan $M = 41$.

Pencarian ini akan lebih mudah jika kita dapat membuat sebuah program yang bisa memecahkan permasalahan tersebut. Disini saya menggunakan Python, untuk mencari nilai X (`j`) untuk setiap elemen A (`i` dalam list `data`).

```python
open_file = open("basic-mod2.txt", "r")
data      = open_file.read().split()
open_file.close()

print("picoCTF{", end = "")
for i in data:
    for j in range(1, 42):
        if (int(i) * j) % 41 == 1:
            num_mod = j
            break
    if 1 <= num_mod <= 26:
        print(chr(ord("A") + num_mod - 1), end = "")
    elif 27 <= num_mod <= 36:
        print(chr(ord("0") + num_mod - 27), end = "")
    elif num_mod == 37:
        print("_", end = "")
print("}", end = "")
```

Dengan program diatas, akan diperoleh suatu flag.
Flag: picoCTF{1NV3R53LY_H4RD_8A05D939}