Very Fine 2.633

September 2023

1 Variables

`keygen()` gives us 3 variables, `a`, `b` and `p`, where

- `p` is a 255 bit prime
- $2 < a < \lfloor \frac{p}{2} \rfloor$
- $0 < b < \texttt{len(flag)}^2$

2 Encryption

From `encrypt()`, we can see that affine cipher is used. For a message `m`, it is encrypted as:

$$am + b \pmod{p}$$

3 Cryptanalysis

We can encrypt whatever numbers we want twice. This gives us a way to attack the cipher using chosen plaintext attack.

Two pieces of ciphertexts corresponds to two equations, but since `b` is small, we can simply bruteforce it. So we should set our equations such that they can help us find `a` and `p`.

When $m = 1$, we have:

$$a + b \pmod{p} \tag{1}$$

When $m = -1$, we have:

$$\begin{aligned} &-a + b \pmod{p} \\ \Longrightarrow &p - a + b \pmod{p} \end{aligned} \tag{2}$$

Note that modulo `p` has no effect here as `a` and `b` are simply too small. So we can just write

$$\begin{cases} a + b & (1) \\ p - a + b & (2) \end{cases}$$

(1) - (2) gives us:

$$a + b - (p - a + b) = 2a - p \tag{3}$$

As we are bruteforcing `b`, we can obtain `a` by (1) - `b`.

$$(a + b) - b = a$$

Then we can do 2`a` - (3)

$$2a - (2a - p) = p$$

which gives us p