

ICSI 526 - Spring 2023 - Homework 1

Jacob Clouse

February 8, 2023

1 - Question 1a Answer:

First of all, this IS breakable. Here is my explanation of why:

For my First name: J A C O B, I found that the combine total is $9 + 0 + 2 + 14 + 1$. $(9 + 0 + 2 + 14 + 1)$ is equal to 26, so we use $(26) \bmod 26$ which is equal to 0. So in $C1 = (a * P1 + b) \bmod 26$, C1 is equal to 0 (for the most common letter E). E is normally valued at 4 in plaintext.

For my Last name: C L O U S E, I found that the combine total is $2 + 11 + 14 + 20 + 18 + 4$. $(2 + 11 + 14 + 20 + 18 + 4)$ is equal to 69, so we use $(69) \bmod 26$ which is equal to 17. So in $C2 = (a * P2 + b) \bmod 26$, C2 is equal to 17 (for the second most common letter T). T is normally valued at 19 in plaintext.

Here are the equations:

For E / First name: **$C1 = (a * P1 + b) \bmod 26$ OR $0 = (a * 4 + b) \bmod 26$**

For T / Last name: **$C2 = (a * P2 + b) \bmod 26$ OR $17 = (a * 19 + b) \bmod 26$**

To find the difference between the two we can subtract the first from the second:

$$17 = (a * 19 + b) \bmod 26 \quad (1)$$

$$0 = (a * 4 + b) \bmod 26 \quad (2)$$

Subtracting (2) from (1) yields:

$$\mathbf{17 = 15a \bmod 26} \quad (3)$$

We now need to take this function and solve for a. To do this, we need to move the mod operator over in (3) to the left hand side. We now have:

$$17 \bmod 26 = 15a \quad (4)$$

We use the Euclidean Algorithm to find the Greatest Common Divisor (or GCD) of 15 and 26 and check to see if its equal to 1. It turns out that the GCD between 15 and 26 is 1.

So this becomes:

$$17 * 15^{-1} \bmod 26 = 1 \quad (5)$$

Then:

$$17 * 7 \bmod 26 = a \quad (6)$$

$$119 \bmod 26 = a \quad (7)$$

Finally, we find that:

$$\mathbf{a = 15} \quad (8)$$

Now we need to solve for b. We do this by substituting in our a value for one of our equations:

$$17 = (\mathbf{15} * 19 + b) \bmod 26 \quad (9)$$

Then:

$$17 = 285 + b \bmod 26 \quad (10)$$

$$(17 - 285) \bmod 26 = b \quad (11)$$

$$-268 \bmod 26 \quad (12)$$

Finally, we find that:

$$\mathbf{b = 18} \quad (13)$$

To check our work we need to substitute b into the equation and solve it:

$$(15(19) + 18) \bmod 26 \quad (14)$$

This is equal to 17, which is the value we calculated previously. So it works!

2 - Question 1b Answer:

The answer to 1b depends on if the **d** in **C = [a × (P-d) + b] mod 26** a constant or part of the key.

3 - Question 2a Answer:

For the

For the

4 - Question 2b Answer:

For the

For the