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) mod 26 which is equal to 0. So in C1 = (a * P1 + b) mod 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) mod 26 which is equal to 17. So in C2 = (a * P2 + b) mod 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) mod 26** *OR* **0 = (a * 4 + b) mod 26**
For T / Last name: **C2 = (a * P2 + b) mod 26** *OR* **17 = (a * 19 + b) mod 26**

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

$$17 = (a * 19 + b) mod 26 \tag{1}$$

$$0 = (a * 4 + b) mod 26 \tag{2}$$

Subtracting (2) from (1) yields

$$\textbf{17 = 15a mod 26} \tag{3}$$

2 - Question 1b Answer:

For the

For the

3 - Question 2a Answer:

For the

For the

4 - Question 2b Answer:

For the

For the