JUNE 6TH CRYPTOGRAPHY + MODULAR ARITHMETIC PROBLEM SET

Quis custodiet ipsos custodes? (Who will watch the watchmen) – Juvenal

We will now apply modular arithmetic to the our study of cryptography. Indeed for each integer $0, 1, \ldots, 25$ we have the corresponding letter $A, B, \ldots, Z$. Caesar shift can then be described by the following algorithm.

(1) Convert each letter $\mathtt{L}_i$ to a number N_i.
(2) Compute $M_i = N_i + 3 \pmod{26}$.
(3) Convert M_i back into a letter $\mathtt{K}_i$.

For example the word ZOO has letters $\mathtt{L}_0 = \mathtt{Z}, \mathtt{L}_1 = \mathtt{O}, \mathtt{L}_2 = \mathtt{O}$. The corresponding numbers are $N_0 = 25, N_1 = 14, N_2 = 14$. These get turned into

$$\begin{aligned} M_0 &= 25 + 3 \pmod{26} = 2 \\ M_1 &= 14 + 3 \pmod{26} = 17 \\ M_2 &= 14 + 3 \pmod{26} = 17 \end{aligned}$$

which get converted back into letters $\mathtt{K}_0 = \mathtt{C}, \mathtt{K}_1 = \mathtt{R}, \mathtt{K}_2 = \mathtt{R}$ so ZOO is turned into CRR. Indeed, any shift cipher, with shift b, can also be viewed as a function

$$x \mapsto x + b \pmod{26}.$$

There is a natural way to generalize this, to the class of Affine Ciphers. These are ciphers given by functions

$$x \mapsto mx + b \pmod{26}$$

where m is another integer. Let's try some examples.

1. Consider the function with $m = 9$ and $b = 0$, $x \mapsto 9x \pmod{26}$. Encrypt the word CAT with this function.

2. Verify that the function $x \mapsto 3x \pmod{26}$ decrypts what you produced in 1.

3. Figure out why the function from 2. decrypts the function from 1. Explain it to everyone in your group.

Hint: What is $3 \cdot 9 \pmod{26}$?

4. Suppose that $x \mapsto mx + b \pmod{26}$ is a function representing an affine cipher. If $m \cdot e \equiv_{26} 1$, figure out a general formula for how to decrypt an affine cipher.

5. Consider the affine cipher $x \mapsto 13x + 2$. Use it to encrypt the word `HELLO`. Why is it impossible to decrypt this?

***6.** Show that a and b have the same remainder when divided by n if and only if[1] n divides into $a - b$ evenly.

This let's us define $\pmod{n}$ even if a and b are negative. For instance $-2 \equiv_5 3$ or in other words, $-2 \pmod{5} = 3$.

[1]This means that you must show both directions.