Homework 3

Number Theory and Cryptography (201912400327)

Due Date: June 2, 2024

Question 1.

Encrypt the message "HOMEWORK SUCKS" using:

- Caesar Cipher
- Shift Cipher with $k = 13$
- Affine Cipher with $f(x) = 5x + 14 \pmod{26}$
- Transposition Cipher based on permutation σ of the set $\{1, 2, 3, 4, 5\}$ with $\sigma(1) = 4, \sigma(2) = 3, \sigma(3) = 1, \sigma(4) = 5, \sigma(5) = 2$. (HINT: fill out the final block!)

Question 2.

Decrypt the ciphertext message "LIFE IS GOOD" using:

- Caesar Cipher
- Shift Cipher with $k = 13$
- Affine Cipher with $f(x) = 5x + 14 \pmod{26}$
- Transposition Cipher based on permutation σ of the set $\{1, 2, 3, 4, 5\}$ with $\sigma(1) = 4, \sigma(2) = 3, \sigma(3) = 1, \sigma(4) = 5, \sigma(5) = 2$. (HINT: fill out the final block!)

Question 3.

Consider an RSA cryptosystem with $p = 17, q = 13$, and $e = 35$.

- What is the value of d?
- Let (e, n) be the public key of Alice. If we use it to encrypt a message $m = 78$, what is the ciphertext C?
- Let (d, n) be the private key of Alice. If she receives a ciphertext $C = 65$, what is the original message m?
- If you receive a message $m = 93$ from Alice and her digital signature 188, do you think that this message indeed comes from her?

Question 4.

Using the RSA public key $(n, e) = (441484567519, 238402465195)$ to encrypt the year that you will graduate from HEU.