Decryption of Affine Cipher

We now see how to **decrypt** messages encrypted using an affine cipher. Suppose that $c = (ap + b) \bmod 26$ with $\gcd(a, 26) = 1$.

To decrypt we need to show how to express p in terms of c.

To do this, we apply the encrypting congruence $c \equiv ap + b \pmod{26}$, and solve it for p.

We first subtract b from both sides, to obtain $c - b \equiv ap \pmod{26}$.

Since $\gcd(a, 26) = 1$, we know that there is an inverse $\bar{a}$ of a modulo 26.

Multiplying both sides of the last equation by $\bar{a}$ gives us $\bar{a}(c - b) \equiv \bar{a}\, ap \pmod{26}$.

Since $\bar{a}\, a \equiv 1 \pmod{26}$, this gives that $p \equiv \bar{a}(c - b) \pmod{26}$.

This determines p because p belongs to $\boldsymbol{Z}_{26}$.

CRYPTANALYSIS

- The process of recovering plaintext from ciphertext without knowledge of both the encryption method and the key is known as **crytanalysis** or **breaking codes**.

- In general, cryptanalysis is a difficult process, especially when the encryption method is unknown.

- We will not discuss cryptanalysis in general, but we will explain how to break messages that were encrypted using a shift cipher.

BLOCK CIPHERS

- Shift ciphers and affine ciphers proceed by replacing each letter of the alphabet by another letter in the alphabet.
- Because of this, these ciphers are called **character** or **monoalphabetic ciphers**.
- Encryption methods of this kind are vulnerable to attacks based on the analysis of letter frequency in the ciphertext, as we just illustrated.
- We can make it harder to successfully attack ciphertext by replacing blocks of letters with other blocks of letters instead of replacing individual characters with individual characters; such ciphers are called **block ciphers**.

Transposition Cipher

- A simple type of block cipher, called the **transposition cipher**.
- As a key we use a permutation σ of the set $\{1, 2, \ldots, m\}$ for some positive integer m, that is, a one-to-one function from $\{1, 2, \ldots, m\}$ to itself.
- To encrypt a message we first split its letters into blocks of size m.

Note: If the number of letters in the message is not divisible by m we add some random letters at the end to fill out the final block.

- We encrypt the block $p_1 p_2 \ldots p_m$ as $c_1 c_2 \ldots c_m = p_{\sigma(1)} p_{\sigma(2)} \ldots, p_{\sigma(m)}$.
- To decrypt a ciphertext block $c_1 c_2 \ldots c_m$, we transpose its letters using the permutation σ^{-1}, the inverse of σ .
- The example given below illustrates encryption and decryption for a transposition cipher.

EXAMPLE

Using the transposition cipher based on the permutation σ of the set $\{1, 2, 3, 4\}$ with $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$,

(a) Encrypt the plaintext message PIRATE ATTACK.

(b) (b) Decrypt the ciphertext message SWUE TRAE OEHS, which was encrypted using this cipher.

Solution: (a) We first split the letters of the plaintext into blocks of four letters. We obtain PIRA TEAT TACK. To encrypt each block, we send the first letter to the third position, the second letter to the first position, the third letter to the fourth position, and the fourth letter to the second position. We obtain IAPR ETTA AKTC.

(b) We note that σ^{-1}, the inverse of σ , sends 1 to 2, sends 2 to 4, sends 3 to 1 and sends 4 to 3

that is $\sigma^{-1}(1) = 2$, $\sigma^{-1}(2) = 4$, $\sigma^{-1}(3) = 1$, and $\sigma^{-1}(4)$.

Applying $\sigma^{-1}(m)$ to each block gives us the plaintext:

USEW ATER HOSE. (Grouping together these letters to form common words, we surmise that the plaintext is USE WATER HOSE.)