6.2.1.2 Affine Cipher

Here also, the plaintext space $(\mathcal{P})$ = ciphertext space $(\mathcal{C}) = \mathbb{Z}_{26}$, but the key space is $\mathcal{K} = \{(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \text{ where } gcd(a,26) = 1\}$. For any $k = (a,b) \in \mathcal{K}$ and $x \in \mathcal{P}$, the encryption and decryption process are as follows:

- Encryption: $E_{(a,b)}(x) = (ax+b) \mod 26 = Y$
  An encryption algorithm E_k substitutes any alphabet x by the image under the liner (affine) mapping $ax+b$, hence, the cryptosystem is called affine cipher. Y is the ciphertext corresponding to the plaintext x. Alice repeats the process for each plaintext character and sends the complete ciphertext to Bob.

- Decryption: $D_{(a,b)}(Y) = a^{-1}(Y-b) \mod 26 = x$
  A decryption algorithm D_k substitutes any alphabet by its inverse under the linear mapping $(ax+b) \mod 26$. After receiving the ciphertext, Bob decrypts each character (Y) of ciphertext using the decryption process.

The number of integers less than and relatively prime to m is given by $\phi(m)$ (Euler's phi function). So, the order of key space $\#(\mathcal{K})$ = possible values of $b(=26) \times$ possible values of $a(=12) = 312$, not a big number! Exhaustive key search attack is possible. Hence, this cipher is also not secure, but is more secure in comparison to shift cipher. Number of keys in the affine cipher over Z_m is $m\phi(m)$, if $m = 60$ then $\#\mathcal{K} = 60 \times 16 = 960$.

Example 85 *Consider the key* $k = (9,2)$ *and the message "affine".*

- *Encryption: The numerical value of the message "affine" is* "000505081304″. *Since each alphabet is a plaintext, hence, six plaintexts in this message. Encrypting one by one, using the mapping* $9x+2 \pmod{26}$, *where* $x = 0,5,5,8,13,4$, *we obtain* 022121221512. *Thus, the ciphertext is "CVVWPM″.*

- *Decryption: To decrypt "CVVWPM″, first we convert the ciphertext into corresponding numerical value* "022121221512″. *Now, decrypting the alphabets using the mapping* $9^{-1}(Y-2) \equiv 3(Y-2) \equiv 3Y-6 \equiv 3Y+20 \pmod{26}$, *where* $Y = 02,21,21,22,15,12$, *we obtain* "000505081304″. *Thus, the original message is "affine″.*

Why is the condition $gcd(a,26) = 1$ important? The answer is given in the following theorem.

Theorem 6.1
The congruence $ax \equiv b \pmod{m}$ *has a unique solution* $x \in \mathbb{Z}_m$ *for every* $b \in \mathbb{Z}_m$ *if and only if* $gcd(a,m) = 1$.

If a is not relatively prime to 26, then the equation $ax+b = y \pmod{26}$ may have more than one solutions. We can explain this by an example. Suppose the key is

$(13,4)$, hence, the encryption rule is $13x+4 \pmod{26}$. If we encrypt the plaintext "input", we get the ciphertext "ERRER" and if we encrypt the plaintext "alter", we get the same ciphertext "ERRER". Thus, encryption of two different plaintexts yields the same ciphertext. Encryption is not one-to-one, hence, not a valid encryption. If we decrypt "ERRER", we can get two plaintexts. Observe that $gcd(13,26) \neq 1$.

6.2.1.3 Substitution Cipher

plaintext space $(\mathcal{P})$ = ciphertext space $(\mathcal{C}) = \mathbb{Z}_{26}$ and $\mathcal{K} = S_{26}$ (set of all permutations $\pi : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$). For each permutation mapping π, we define

- Encryption: $E_\pi(x) = \pi(x)$.
- Decryption: $D_\pi(Y) = \pi^{-1}(Y)$.

where π^{-1} is the inverse permutation to π.

Example 86 *Let Alice and Bob agree on a permutation* $\pi = (1,2,3,4,...25)$. *And let plaintext be* $x = ramacceptedbribe$.

- *Encryption: The numerical value of the message is* $= (1700120002020415190$ $4030107080104)$, *thus* $E_\pi(x) = \pi(1700120002020415190403010708010 4) =$ $(1801130103030516200504020809020 5) = SBNBDDFQUFECSJCF$.
- *Decryption: Using the inverse of permutation* π, *Bob decrypt the ciphertext "SBNBDDFQUFECSJCF" as* $D_\pi(Y) = \pi^{-1}(1801130103030516200504020$ $8090205) = (1700120002020415190403010708010 4) = ramacceptedbribe$.

Key space of substitution cipher includes all possible permutations of 26 alphabets. Clearly, the order of the key space $\#\mathcal{K} = 26! > 10^{26}$ is a very large number, therefore, one cannot check case by case even using a computer. So, exhaustive search attack is not possible in this cipher. However, we will see later in cryptanalysis section that this cipher is not secure against some attacks, viz. frequency analysis. The shift cipher and affine cipher are special cases of substitution cipher.

In all of the above three cryptosystems; shift cipher, affine cipher, and substitution cipher, a single alphabet is replaced by a unique alphabet in encryption. These are called *mono-alphabetic substitution* and can be easily solved using *frequency analysis* (discussed in the next section). If a single alphabet of plaintext is replaced by more than one alphabet (*poly-alphabetic substitution*), then the cryptosystem may be more secure than mono-alphabetic cipher. Below, we discuss some substitution ciphers based on poly-alphabetic substitution.

6.2.1.4 Vigenere Cipher

The well-known Vigenere cipher is named after Blaise de Vigenere, a French diplomat and cryptographer who lived in the sixteenth century (1523–1596). It is a simple form of poly-alphabetic substitution.