$(13,4)$, 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.

In this cryptosystem, $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}^m$. For a key $K = (k_1, k_2, k_3, ...k_m) \in \mathcal{K}$ and a plaintext $x = (x_1, x_2, x_3 ...x_m) \in \mathcal{P}$, we define the encryption and decryption as follows:

- Encryption: $E_K(x_1, x_2, x_3, ...x_m) = (x_1 + k_1, x_2 + k_2, ..x_m + k_m) \mod 26$

- Decryption: $D_K(y_1, y_2, y_3, ...y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m) \mod 26$

In Vigenere cipher, we encrypt/decrypt a collection of m-alphabetic plaintext/ciphertext using a string of m-alphabetic key called "keyword". It is explained by the following simple examples.

Example 87 *Let the keyword be "CODE", number of alphabet in keyword is 4, so* $m = 4$. *Suppose Alice wants to send a plaintext "the germans are coming" to Bob. Before communicating, they first share the keyword. Using the correspondence* $A \leftrightarrow 0$, $B \leftrightarrow 1$, $C \leftrightarrow 2$ *...*$Z \leftrightarrow 25$ *as described earlier. She first obtains the numerical equivalent of keyword "CODE" and plaintext "the germans are coming". To encrypt the plaintext she does addition of the plaintext and key using residue modulo 26 as follows:*

Numeric value of the keyword is $(2, 14, 3, 4)$.

PT	*t*	*h*	*e*	*g*	*e*	*r*	*m*	*a*	*n*	*s*
numericalPT	19	7	4	6	4	17	12	0	13	18
Key	2	14	3	4	2	14	3	4	2	14
Encryption	21	21	7	10	6	5	15	4	15	6
CT	*V*	*V*	*H*	*K*	*G*	*F*	*P*	*E*	*P*	*G*
PT	*a*	*r*	*e*	*c*	*o*	*m*	*i*	*n*	*g*	–
numericalPT	0	17	4	2	14	12	8	13	6	–
Key	3	4	2	14	3	4	2	14	3	–
Encryption	3	21	6	16	17	16	10	1	9	–
CT	*D*	*V*	*G*	*Q*	*R*	*Q*	*K*	*B*	*J*	–

Thus, the ciphertext is "VVH KGFPEPG DVG QRQKBJ".
To decrypt the ciphertext, Bob does the above process in reverse order as below:

CT	*V*	*V*	*H*	*K*	*G*	*F*	*P*	*E*	*P*	*G*
NumericalCT	21	21	7	10	6	5	15	4	15	6
Key	2	14	3	4	2	14	3	4	2	14
Decryption	19	7	4	6	4	17	12	0	13	18
PT	*t*	*h*	*e*	*g*	*e*	*r*	*m*	*a*	*n*	*s*
CT	*D*	*V*	*G*	*Q*	*R*	*Q*	*K*	*B*	*J*	–
NumericalCT	3	21	6	16	17	16	10	1	9	–
Key	3	4	2	14	3	4	2	14	3	–
Decryption	0	17	4	2	14	12	8	13	6	–
PT	*a*	*r*	*e*	*c*	*o*	*m*	*i*	*n*	*g*	–

Thus, the plaintext is "the germans are coming".