A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plaintext: CABLE

Number of alphabets to substitute is two: CA BL EA

The last single alphabet is padded.

For a two - alphabet substitution, the key is a 2 * 2 matrix of alphabets, meaning 4 characters.

KEY: DBGF ➔ $\begin{matrix} 3 & 1 \\ 6 & 5 \end{matrix}$

Plaintext matrix representation CA = $\begin{matrix} 2 \\ 0 \end{matrix}$ BL = $\begin{matrix} 1 \\ 11 \end{matrix}$ EA = $\begin{matrix} 4 \\ 0 \end{matrix}$

➔ Encryption

$C_i = K * P_i \bmod 26$

C is the cyphertext

K is the key

P is the plaintext

26 is the number of alphabets

$$C_1 = \begin{matrix} 3 & 1 \\ 6 & 5 \end{matrix} * \begin{matrix} 2 \\ 0 \end{matrix} \bmod 26 = \begin{matrix} 6 \\ 12 \end{matrix} \bmod 26 = \begin{matrix} 6 \\ 12 \end{matrix} \rightarrow \begin{matrix} G \\ M \end{matrix}$$

$$C_2 = \begin{matrix} 3 & 1 \\ 6 & 5 \end{matrix} * \begin{matrix} 1 \\ 11 \end{matrix} \bmod 26 = \begin{matrix} 4 \\ 61 \end{matrix} \bmod 26 = \begin{matrix} 4 \\ 9 \end{matrix} \rightarrow \begin{matrix} O \\ J \end{matrix}$$

$$C_3 = \begin{matrix} 3 & 1 \\ 6 & 5 \end{matrix} * \begin{matrix} 4 \\ 0 \end{matrix} \bmod 26 = \begin{matrix} 12 \\ 24 \end{matrix} \bmod 26 = \begin{matrix} 12 \\ 24 \end{matrix} \rightarrow \begin{matrix} M \\ Y \end{matrix}$$

Cyphertext = GMOJMY

➔ Decryption

$P_i = (K^{-1} * C_i) \bmod 26$

$$K^{-1} = \frac{1}{|K|} \text{adj}(K)$$

$|K|$ is the absolute vale of K

$$|K| = 3 * 5 - 6 * 1 = 9$$

$\frac{1}{|K|}$ is the multiplicative inverse of the absolute vale of K

N.B: For there to be a multiplicative inverse of the absolute vale of K, the absolute value and 26 must have a gdc = 1.

$$\frac{1}{|K|} = \frac{1}{9} = 3$$

$$\text{adj}(K) = \begin{matrix} 5 & -1 \\ -6 & 3 \end{matrix}$$

$$K^{-1} = 3 * \begin{matrix} 5 & -1 \\ -6 & 3 \end{matrix} = \begin{matrix} 15 & -3 \\ -18 & 9 \end{matrix} \rightarrow \begin{matrix} 15 & -3 + 26 \\ -18 + 26 & 9 \end{matrix} = \begin{matrix} 15 & 23 \\ 8 & 9 \end{matrix}$$

$$P_1 = \begin{matrix} 15 & 23 \\ 8 & 9 \end{matrix} * \begin{matrix} 6 \\ 12 \end{matrix} \text{ mod } 26 = \begin{matrix} 366 \\ 156 \end{matrix} \text{ mod } 26 \quad \begin{matrix} 2 \\ 0 \end{matrix} \rightarrow \begin{matrix} C \\ A \end{matrix}$$

$$P_2 = \begin{matrix} 15 & 23 \\ 8 & 9 \end{matrix} * \begin{matrix} 14 \\ 9 \end{matrix} \text{ mod } 26 = \begin{matrix} 417 \\ 193 \end{matrix} \text{ mod } 26 \quad \begin{matrix} 1 \\ 11 \end{matrix} \rightarrow \begin{matrix} B \\ L \end{matrix}$$

$$P_3 = \begin{matrix} 15 & 23 \\ 8 & 9 \end{matrix} * \begin{matrix} 12 \\ 24 \end{matrix} \text{ mod } 26 = \begin{matrix} 732 \\ 312 \end{matrix} \text{ mod } 26 \quad \begin{matrix} 4 \\ 0 \end{matrix} \rightarrow \begin{matrix} E \\ A \end{matrix}$$

Output: CA BL EA

But the last single alphabet was padded with A. therefore,

Plaintext: CABLE