Multiplicative Method

Cipher based on multiply each character by Key, where k and 26 are relatively; so that the letters of the alphabet produce a complete set of residues, so that case the key must be an odd number and not equal to 13.

K_1	1	3	5	7	9	11	15	17	19	21	23	25
K_1^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

***Note*: Keep in your mine that**

k: the key is used for the encryption process

k^{-1}: the key is used for decryption process

Encryption process

A system of encryption in which each letter of message is replaced with another characters, to produce the cipher text according to this formula below:

$$C = (P * k) \bmod 26$$

Decryption process

A system of decryption in which each letter of ciphertext is replaced with another characters to produce the plaintext or the message according to this formula below:

$$P = (C * k^{-1}) \bmod 26$$

Example1

Use the multiplicative method to encrypt and decrypt the message "Computer" if the key is 5.

Solution

Encryption process:

By applying the encryption process formula: **C = (P * k) mod 26** on the plaintext

E (c)	**=**	**2 * 5**	**Mod 26**	**=>**	**10**	**Mod 26**	**10**	**=>**	**k**
E (o)	**=**	**14 * 5**	**Mod 26**	**=>**	**70**	**Mod 26**	**18**	**=>**	**s**
E (m)	**=**	**12 * 5**	**Mod 26**	**=>**	**60**	**Mod 26**	**8**	**=>**	**i**
E (p)	**=**	**15 * 5**	**Mod 26**	**=>**	**75**	**Mod 26**	**23**	**=>**	**x**
E (u)	**=**	**20 * 5**	**Mod 26**	**=>**	**100**	**Mod 26**	**22**	**=>**	**w**
E (t)	**=**	**19 * 5**	**Mod 26**	**=>**	**95**	**Mod 26**	**17**	**=>**	**r**
E (e)	**=**	**4 * 5**	**Mod 26**	**=>**	**20**	**Mod 26**	**20**	**=>**	**u**
E (r)	**=**	**17 * 5**	**Mod 26**	**=>**	**85**	**Mod 26**	**7**	**=>**	**h**

The ciphertext is "ksixwruh"

Decryption process:

By applying the Decryption process formula **$P = (C * k^{-1}) \bmod 26$** on the ciphertext "ksixwruh" to produce the original message

D (k)	**=**	**10 * 21**	**Mod 26**	**=>**	**210**	**Mod 26**	**2**	**=>**	**c**
D (s)	**=**	**18 * 21**	**Mod 26**	**=>**	**378**	**Mod 26**	**14**	**=>**	**o**
D (i)	**=**	**8 * 21**	**Mod 26**	**=>**	**168**	**Mod 26**	**12**	**=>**	**m**
D (x)	**=**	**23 * 21**	**Mod 26**	**=>**	**483**	**Mod 26**	**15**	**=>**	**p**
D (w)	**=**	**22 * 21**	**Mod 26**	**=>**	**462**	**Mod 26**	**20**	**=>**	**u**
D (r)	**=**	**17 * 21**	**Mod 26**	**=>**	**357**	**Mod 26**	**19**	**=>**	**t**
D (u)	**=**	**20 * 21**	**Mod 26**	**=>**	**420**	**Mod 26**	**4**	**=>**	**e**
D (h)	**=**	**7 * 21**	**Mod 26**	**=>**	**147**	**Mod 26**	**17**	**=>**	**r**

The plaintext is "computer"