Caesar Method

A very simple monoalphabatic substitution cipher is the Julius Caesar's cipher or known as shift method. The transformation algorithm $E_K(i)$ is: "replace each letter in the plaintext by the third one following it in the standard alphabet", whereas the i is the letter index and k is the key simply the amount of "shift" between the original plaintext letters and the cipher text letters. It is called a shifted-alphabet cipher. Assume that k = 3, for instance.

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

Encryption Low

$$E(p) = C = (p + k) \bmod n$$

Decryption Low

$$D(C) = P = (C - k) \bmod n$$

note

* ***D(C)*** is the decryption process
* ***E(p)*** is the encryption process
* **C** is a ciphertext
* **p** is aplaintext
* ***k** is a key

Example 1 Encrypt the plaintext message "**brutus**" use Caesar cipher method.

Solution

Encryption process:

The encryption low is

$$E(p) = (p + k) \bmod n$$

Where k = 3 and n = 26.

Plaintext (P)	b	r	u	t	u	s
	1	17	20	19	20	18
k	3	3	3	3	3	3
P + k	4	20	23	22	23	21
Mod 26	**4**	**20**	**23**	**22**	**23**	**21**
Cipher text (C)	E	U	X	W	X	V

The cipher text is :

E (P) = C = "E U X W X V"

Example 2 Decrypt the cipher text message "**EUXWXV**" use Caesar cipher method.

Answer:

Decryption Algorithm:

The legitimate message recipient, having the encryption key **k** and knowing the encryption Transformation (i.e. shifted-alphabet cipher transformation) can perform the decryption of Cipher text C: "EU XW XV"

$$D(C) = P = (C - k) \bmod n$$

Ciphertext (C)	E	U	X	W	X	V
	4	20	23	22	23	21
k	3	3	3	3	3	3
C - k	1	17	20	19	20	18
Mod 26	**1**	**17**	**20**	**19**	**20**	**18**
Plaintext (P)	b	r	u	t	u	s

The plaintext is "**brutus**"

Example 3 Use Caesar cipher method to encrypt the plaintext message "**fire missile**". if the shift key is 11 step.

Answer

$$C = E(p) = (p + k) \bmod n$$

Plaintext (p)	f	i	r	e	m	i	s	s	i	l	e
	5	8	17	4	12	8	18	18	8	11	4
key	11	11	11	11	11	11	11	11	11	11	11
P+k	16	19	28	15	23	19	29	29	19	22	15
Mod 26	**16**	**19**	**2**	**15**	**23**	**19**	**3**	**3**	**19**	**22**	**15**
Ciphertext (C)	Q	T	C	P	X	T	D	D	T	W	P

The ciphertext is "QTCPXTDDTWP"

==========

Example 4

Decrypt the cipher text message "**QTCPXTDDTWP**" use Caesar cipher method. If the shift by 11 step**.**

Answer

$$D(C) = P = (C - k) \bmod n$$

Ciphertext (C)	Q	T	C	P	X	T	D	D	T	W	P
	16	**19**	**2**	**15**	**23**	**19**	**3**	**3**	**19**	**22**	**15**
key	11	11	11	11	11	11	11	11	11	11	11
C - k	5	8	-9	4	12	8	-8	-8	8	11	4
Mod 26	**5**	**8**	**17**	**4**	**12**	**8**	**18**	**18**	**8**	**11**	**4**
Plaintext (p)	f	i	r	e	m	i	s	s	i	l	e

The plaintext "fire missile"