VIGENERE CIPHER

The best known, and one of the simplest, polyalphabetic ciphers is the Vigenère cipher. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter, which is the ciphertext letter that substitutes for the plaintext letter a. Thus, a Caesar cipher with a shift of 3 is denoted by the key value d.

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

Thus, the first letter of the key is added to the first letter of the plaintext, mod 26, the second letters are added, and so on through the first *m* letters of the plaintext. For the next *m* letters of the plaintext, the key letters are repeated. This process continues until all of the plaintext sequence is encrypted.

$$C = (M + K) \bmod 26$$

The Decryption process

Similarly, decryption is a generalization of Equation To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword.

$$P = (C - K) \bmod 26$$

Example 1

If the keyword is "***deceptive"*** and the message is "***we are discovered save yourself***" encrypt the message use vigenere cipher method.

Answer

Note that the key length is samller than the length of the plaintext therefore we are repeat the key to be tha e same length. And apply the encryption low

C = (M + K) mod 26

Plaintext	w	e	*a*	*r*	*e*	d	i	s	c	o	v	e	r	e	d	*s*	*a*	*v*	*e*	y	o	u	r	s	e	l	f
(P)	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	11	5
Key	d	e	c	e	p	t	i	v	e	**d**	**e**	**c**	**e**	**p**	**t**	**i**	**v**	**e**	d	e	c	e	p	t	i	v	e
(K)	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
C + K	25	8	2	21	19	22	16	39	6	17	25	6	21	19	22	26	21	25	7	28	16	24	32	37	12	32	9
Mod 26	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22	0	21	25	7	2	16	24	6	11	12	6	9
Ciphertext (C)	z	i	c	v	t	w	q	n	g	r	z	g	v	t	w	a	v	z	h	c	q	y	g	l	m	g	j

Cipher text is "zicvtwqngrzgvtwavzhcqyglmgj"

Example 2

If the keyword is "***deceptive"*** and the ciphertext is **"zicvtwqngrzgvtwavzhcqyglmgj** "

Decrypt the message use vigenere cipher method.

Answer

P = (C - K) mod 26

Ciphertext	Z	I	C	V	T	W	Q	N	G	R	Z	G	V	T	W	A	V	Z	H	C	Q	Y	G	L	M	G	J
(C)	25	8	2	21	19	22	16	13	6	17	25	6	21	19	22	0	21	25	7	2	16	24	6	11	12	6	9
Key	d	e	c	e	p	t	i	v	e	**d**	**e**	**c**	**e**	**p**	**t**	**i**	**v**	**e**	d	e	c	e	p	t	i	v	e
(k)	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4	3	4	2	4	15	19	8	21	4
C - K	22	4	0	17	4	3	8	-8	2	14	21	4	17	4	3	-8	0	21	4	-2	14	20	-9	-8	4	-15	5
Mod 26	22	4	0	17	4	3	8	18	2	14	21	4	17	4	3	18	0	21	4	24	14	20	17	18	4	9	5
Plaintext (p)	**w**	**e**	a	r	e	**d**	**i**	**s**	**c**	**o**	**v**	**e**	**r**	**e**	**d**	s	a	v	e	**y**	**o**	**u**	**r**	s	e	l	f

Plaintext is " we are discovered save your self "