

# Vigenere



////////////////////////////////////  
This method needs a stream key and it must be the same length as the plain text and if it is less then we repeat the characters of the stream key in succession.

Example: encrypt the plain text (I LOOVE PEANUTS) if you know that the stream key is (BANANA) using the Vigenere algorithm.

plain text : I LOOVE PEANUTS

stream key : BANANA

**Note** in the above example we doubled the stream key to be the length of the plaintext.

**Encryption** The plaintext(P) and key(K) are added modulo 26.

$$E_i = (P_i + K_i) \bmod 26$$

**Decryption**

$$D_i = (E_i - K_i) \bmod 26$$



Map each letter to a number (corresponding to its position in the alphabet).

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26



# Vigenere

The diagram illustrates the Vigenere cipher process. It shows a message (top row, blue circles) and a key (middle row, red circles) being added together (indicated by a '+' sign and a horizontal line) to produce an encrypted message (bottom row, green circles). The numbers are arranged in two groups of six, separated by a vertical line. The key is also arranged in two groups of six, with a vertical line after the second group. The encrypted message is arranged in two groups of six, with a vertical line after the second group.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

The encrypted message:  
**KMCPJGRFOOIUU**

# Vigenere

The diagram illustrates the decryption process of a Vigenere cipher. It features a grid of numbers on a black background, with a horizontal line separating the top two rows from the bottom row. The top row consists of green circles containing the numbers: 11, 13, 3, 16, 10, 7, 18, 6, 15, 15, 9, 21, 21. The second row consists of red circles containing the numbers: 2, 1, 14, 1, 14, 1, 2, 1, 14, 1, 14, 1, 2. The bottom row consists of blue circles containing the numbers: 9, 12, 15, 15, 22, 6, 16, 5, 1, 14, 21, 20, 19. Below the grid is a key table with two rows of letters and their corresponding numerical values.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

The decrypted message:  
Ilovepeanuts

# Vigenere

7



Form1

Message	<input type="text" value="ilovepeanuts"/>	Normalization
Messnorm	<input type="text" value="ILOOVEPEANUTS"/>	Vigener_en
Key	<input type="text" value="BANANA"/>	
ciphertext	<input type="text" value="KMCPJFRFOOIUU"/>	Vigener_de
unciphertext	<input type="text" value="ILOOVEPEANUTS"/>	