

# Vigenere





This method needs a stream key and it must be the same length as the plain text and if it is less than 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.

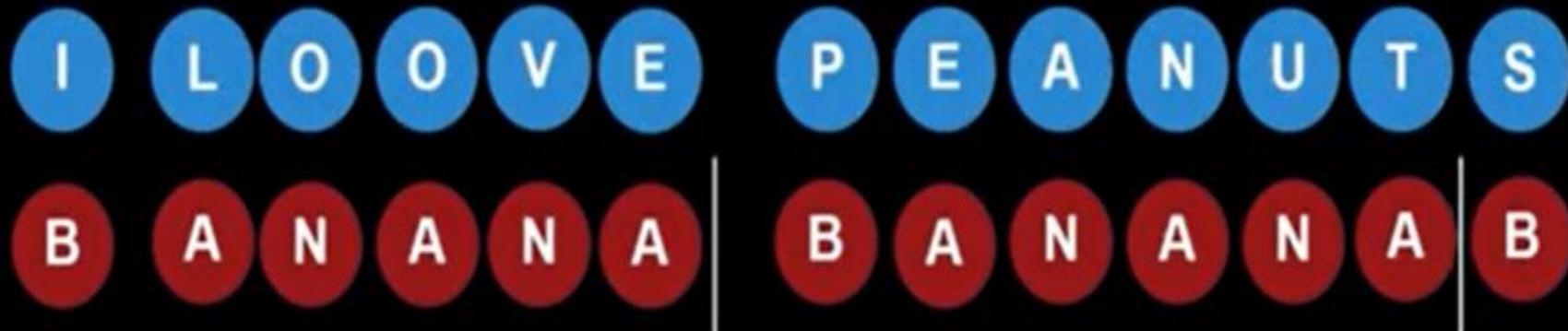
$$E_i = (P_i + K_i) \bmod 26$$

**Decryption**

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

# Vigenere

4



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

5

A diagram illustrating the Vigenere cipher process. At the top, there are two rows of numbers in blue and red circles, separated by a plus sign (+). The first row contains: 9, 12, 15, 15, 22, 6, 16, 5, 1, 14, 21, 20, 19. The second row contains: 2, 1, 14, 1, 14, 1, 2, 1, 14, 1, 14, 1, 2. Below these is a row of green circles containing the result of the addition: 11, 13, 3, 16, 10, 7, 18, 6, 15, 15, 9, 21, 21. Below the green row is a 2x13 grid mapping numbers to letters:

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 text "The encrypted message:" is followed by the red text "KMCPJGRFOOIUU".

# Vigenere

6

The diagram illustrates the decryption process of a Vigenere cipher. It shows two rows of numbers (ciphertext) being subtracted by another row (key), resulting in a third row (decrypted message). The numbers are represented in green, red, and blue circles.

Row 1 (Ciphertext):  
11 13 3 16 10 7 | 18 6 15 15 9 21 21  
2 1 14 1 14 1 | 2 1 14 1 14 1 | 2

Row 2 (Key):  
—  
9 12 15 15 22 6 | 16 5 1 14 21 20 19

Row 3 (Decrypted Message):  
16 5 1 14 21 20 19

Below the numbers are two tables mapping letters to numbers:

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 is:  
Ilovepeanuts

# Vigenere

7

Form1

Message

ilooovepeanuts

Normalization

Messnorm

ILOOVEPEANUTS

Vigener\_en

Key

BANANA

ciphertext

KMCPJFRFOOIUU

Vigener\_de

unciphertext

ILOOVEPEANUTS