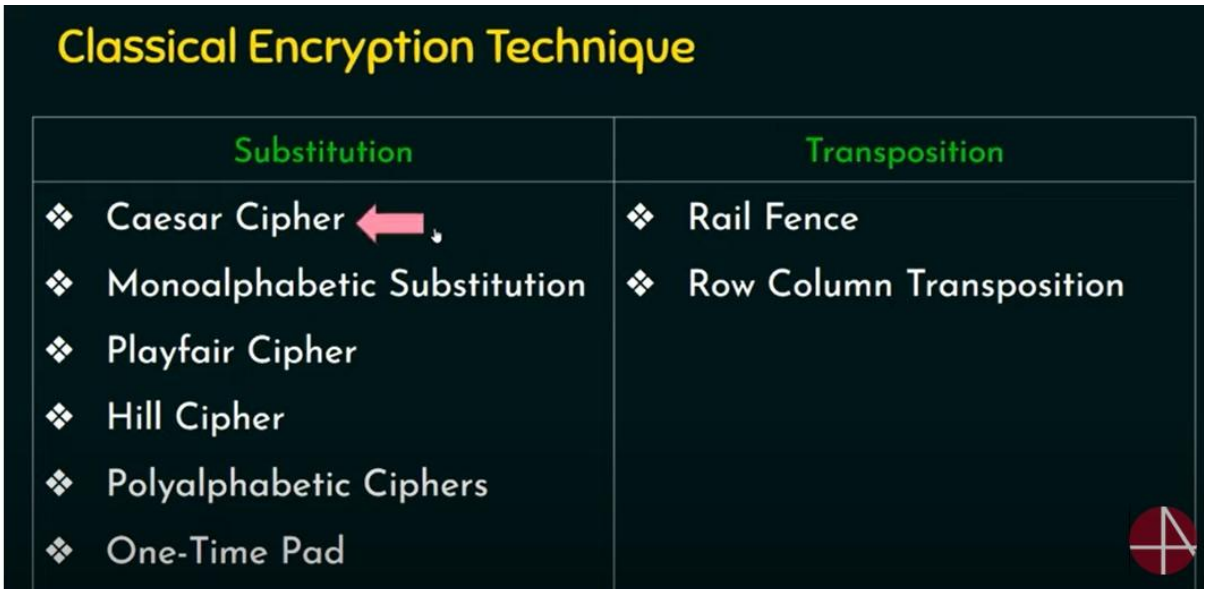
Chapter: Symmetric Cryptography

Classical Encryption Techniques are two types:

1. Substituion Technique
2. Transpositon Technique



Classical Encryption Technique

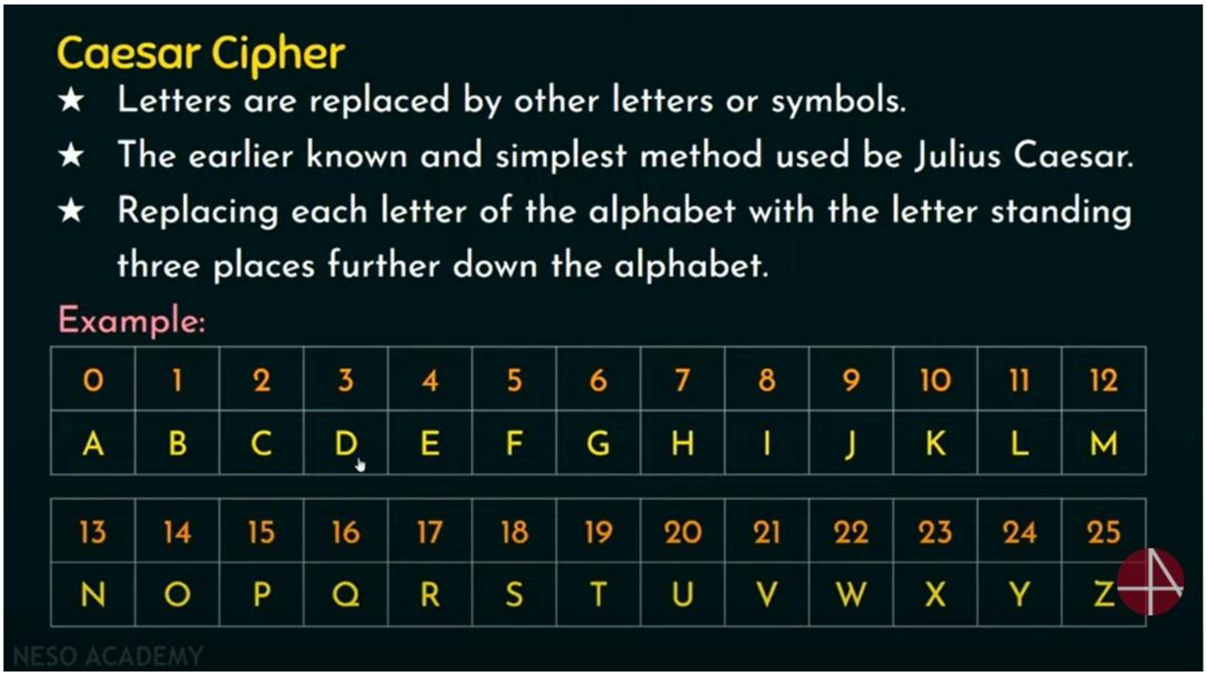
Substitution	Transposition
❖ Caesar Cipher	❖ Rail Fence
❖ Monoalphabetic Substitution	❖ Row Column Transposition
❖ Playfair Cipher	
❖ Hill Cipher	
❖ Polyalphabetic Ciphers	
❖ One-Time Pad	

Example of Symmetric cipher :

1. **Caesar cipher**
2. **Rot 13**
3. **Vigenere cipher**
4. **Morse code**
5. **Bacon Cipher**
6. **Alphabetical substitution**

Note: Every Cipher text will be in upper case letter.

1.Caesar cipher



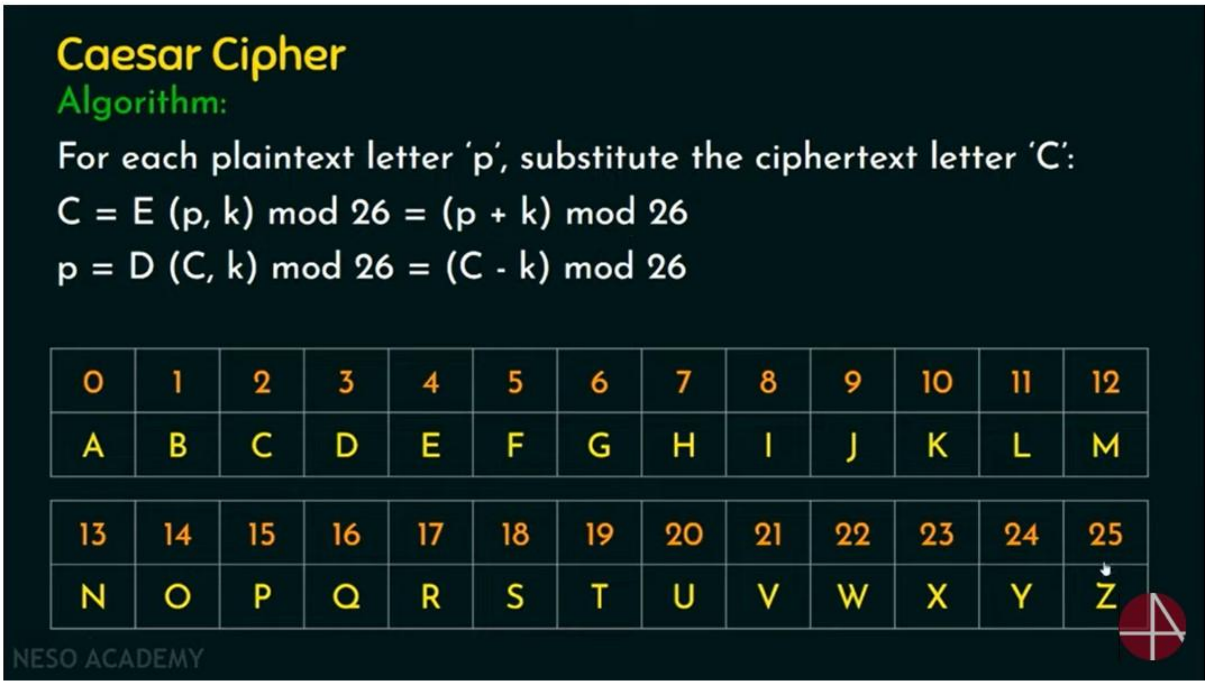
Caesar Cipher

- ★ Letters are replaced by other letters or symbols.
- ★ The earlier known and simplest method used be Julius Caesar.
- ★ Replacing each letter of the alphabet with the letter standing three places further down the alphabet.

Example:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z



Caesar Cipher

Algorithm:

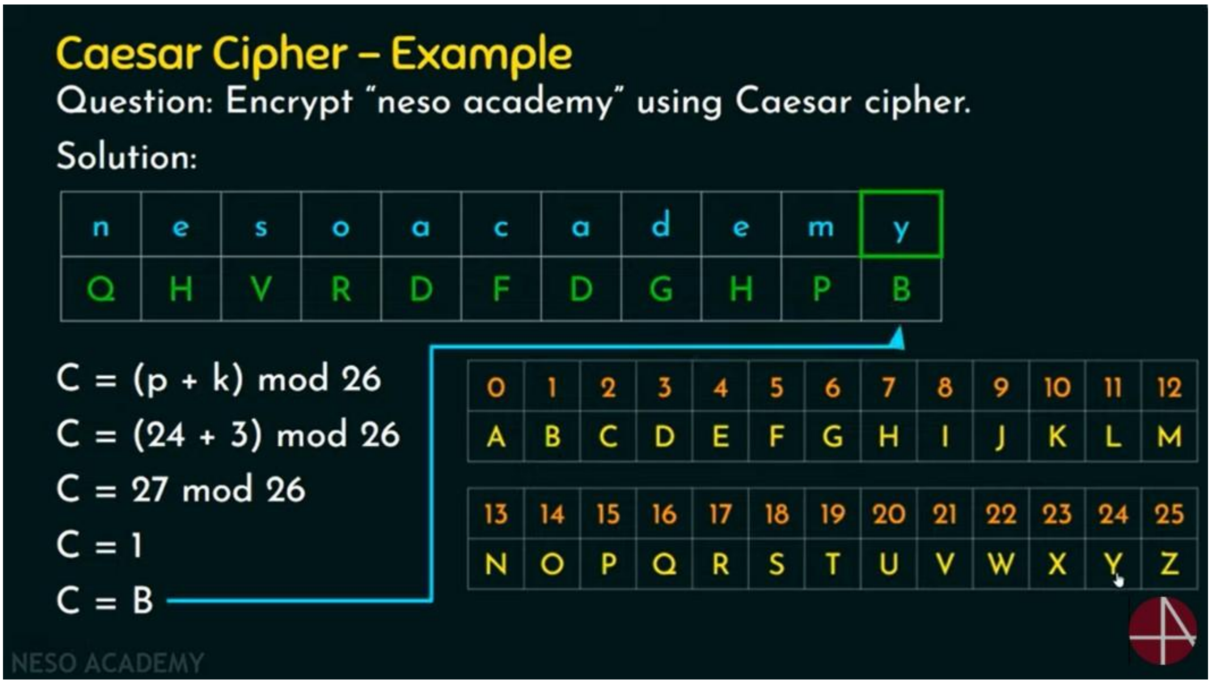
For each plaintext letter 'p', substitute the ciphertext letter 'C':

$C = E(p, k) \bmod 26 = (p + k) \bmod 26$

$p = D(C, k) \bmod 26 = (C - k) \bmod 26$

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z



Caesar Cipher – Example

Question: Encrypt "neso academy" using Caesar cipher.

Solution:

n	e	s	o	a	c	a	d	e	m	y
Q	H	V	R	D	F	D	G	H	P	B

C = (p + k) mod 26

C = (24 + 3) mod 26

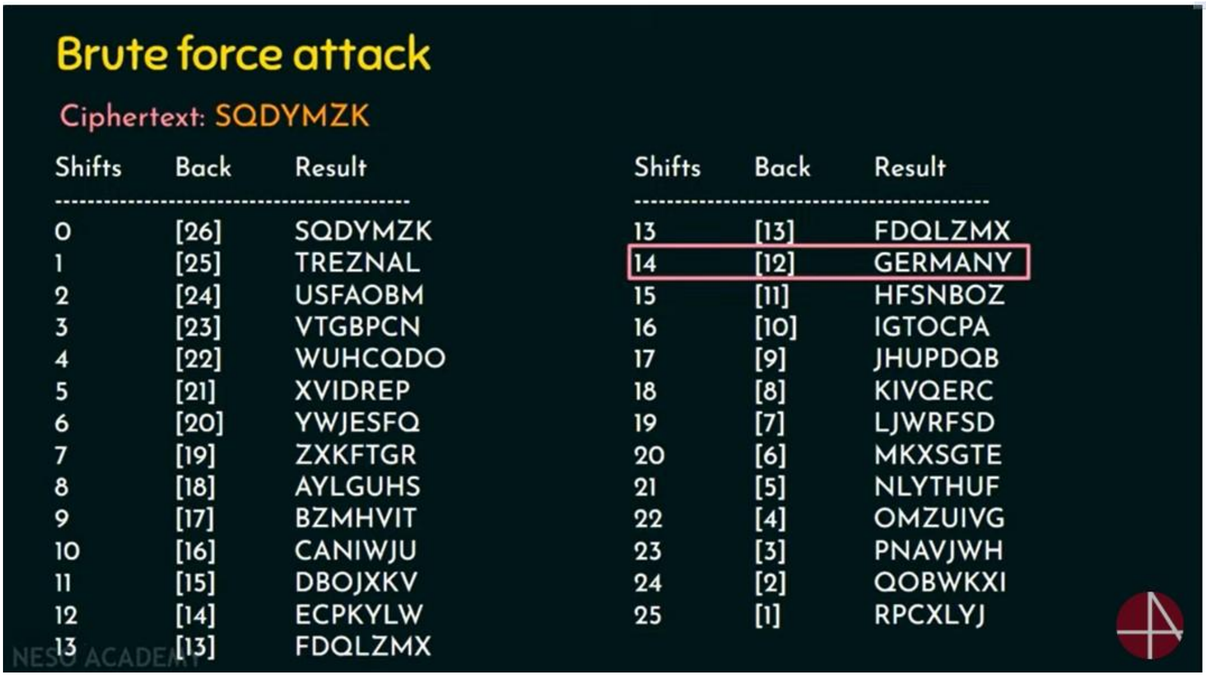
C = 27 mod 26

C = 1

C = B

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M

13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z



Brute force attack

Ciphertext: SQDYMZK

Shifts	Back	Result
0	[26]	SQDYMZK
1	[25]	TREZNAL
2	[24]	USFAOBM
3	[23]	VTGBPCN
4	[22]	WUHCQDO
5	[21]	XVIDREP
6	[20]	YWJESFQ
7	[19]	ZXKFTGR
8	[18]	AYLGUHS
9	[17]	BZMHVIT
10	[16]	CANIWJU
11	[15]	DBOJXKV
12	[14]	ECPKYLW
13	[13]	FDQLZMX
13	[13]	FDQLZMX
14	[12]	GERMANY
15	[11]	HFSNBOZ
16	[10]	IGTOCPA
17	[9]	JHUPDQB
18	[8]	KIVQERC
19	[7]	LJWRFSD
20	[6]	MKXSGTE
21	[5]	NLYTHUF
22	[4]	OMZUIVG
23	[3]	PNAVJWH
24	[2]	QOBWKXI
25	[1]	RPCXLYJ

2. ROT13 Cipher

The ROT13 cipher is a substitution cipher with a specific key where the letters of the alphabet are offset 13 places. I.e. all 'A's are replaced with 'N's, all 'B's are replaced with 'O's, and so on. It can also be thought of as a Caesar cipher with a shift of 13.

The ROT13 cipher offers almost no security, and can be broken very easily. Even if an adversary doesn't know a piece of ciphertext has been enciphered with the ROT13 cipher, they can still break it by assuming it is a substitution cipher and determining the key using hill-climbing. The ROT13 cipher is also an Caesar cipher with a key of 13, so breaking it as a Caesar cipher also works.

3. Vigenere Cipher

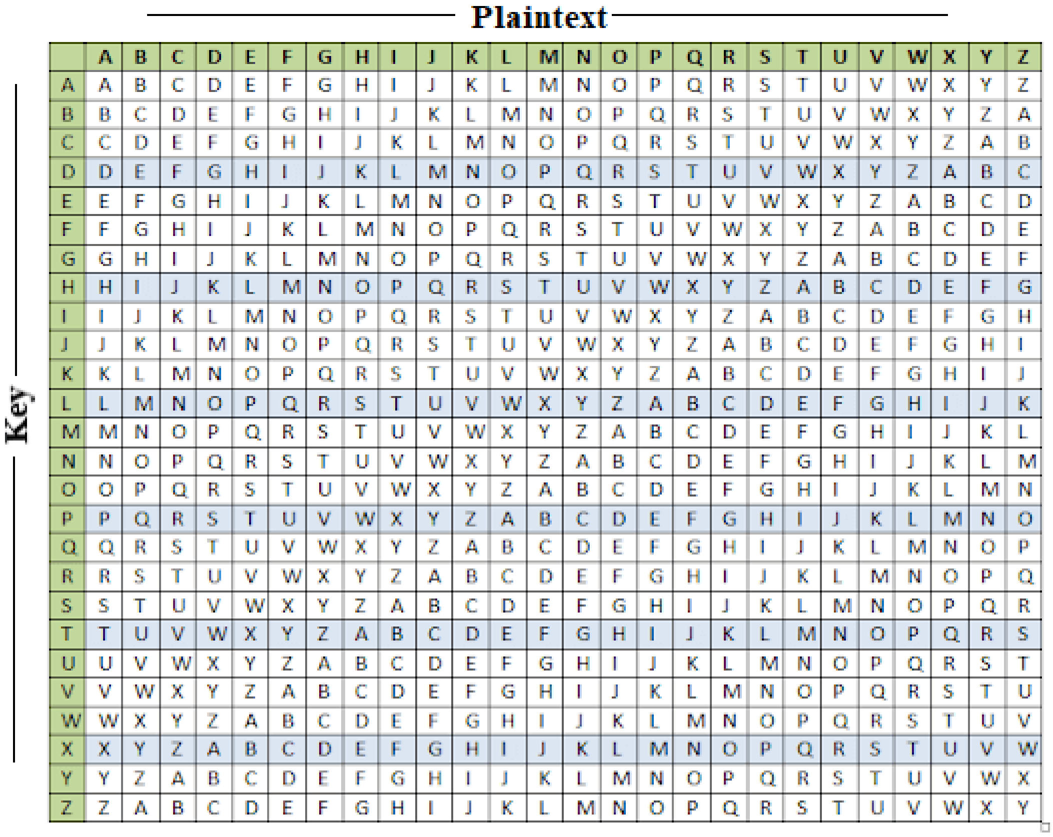
Introduction

The vigenere cipher is an algorithm that is used to encrypting and decrypting the text. The vigenere cipher is an algorithm of encrypting an alphabetic text that uses a series of interwoven caesar ciphers. It is based on a keyword's letters. It is an example of a polyalphabetic substitution cipher. This algorithm is easy to understand and implement. This algorithm was first described in 1553 by **Giovan Battista Bellaso**. It uses a Vigenere table or Vigenere square for encryption and decryption of the text. The vigenere table is also called the tabula recta.

Two methods perform the vigenere cipher.

Method 1

When the vigenere table is given, the encryption and decryption are done using the vigenere table (26 * 26 matrix) in this method.



Plaintext
Key

	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
A	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
B	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	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	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

Example: The plaintext is "JAVATPOINT", and the key is "BEST".

To generate a new key, the given key is repeated in a circular manner, as long as the length of the plain text does not equal to the new key.

J	A	V	A	T	P	O	I	N	T
B	E	S	T	B	E	S	T	B	E

Encryption

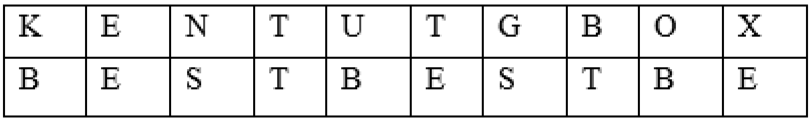
The first letter of the plaintext is combined with the first letter of the key. The column of plain text "J" and row of key "B" intersects the alphabet of "K" in the vigenere table, so the first letter of ciphertext is "K".Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text "A" and row of key "E" intersects the alphabet of "E" in the vigenere table, so the second letter of ciphertext is "E".

This process continues continuously until the plaintext is finished.

Ciphertext = KENTUTGBOX

Decryption

Decryption is done by the row of keys in the vigenere table. First, select the row of the key letter, find the ciphertext letter's position in that row, and then select the column label of the corresponding ciphertext as the plaintext.



K	E	N	T	U	T	G	B	O	X
B	E	S	T	B	E	S	T	B	E

For example, in the row of the key is "B" and the ciphertext is "K" and this ciphertext letter appears in the column "J", that means the first plaintext letter is "J".

Next, in the row of the key is "E" and the ciphertext is "E" and this ciphertext letter appears in the column "A", that means the second plaintext letter is "A".

This process continues continuously until the ciphertext is finished.

Plaintext = JAVATPOINT

Method 2

When the vigenere table is not given, the encryption and decryption are done by Vigenar algebraically formula in this method (convert the letters (A-Z) into the numbers (0-25)).

Formula of encryption is,

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

Formula of decryption is,

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

If any case (D_i) value becomes negative (-ve), in this case, we will add 26 in the negative value.

Where,

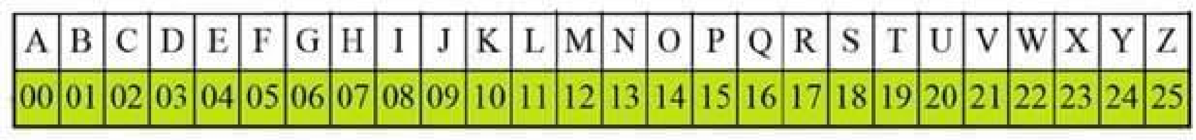
E denotes the encryption.

D denotes the decryption.

P denotes the plaintext.

K denotes the key.

> Note: "i" denotes the offset of the ith number of the letters, as shown in the table below.



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
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example: The plaintext is "JAVATPOINT", and the key is "BEST".

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

Plaintext	J	A	V	A	T	P	O	I	N	T
Plaintext value (P)	09	00	21	00	19	15	14	08	13	19
Key	B	E	S	T	B	E	S	T	B	E

Key value (K)	01	04	18	19	01	04	18	19	01	04
Ciphertext value (E)	10	04	13	19	20	19	06	01	14	23
Ciphertext	K	E	N	T	U	T	G	B	O	X

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

If any case (Di) value becomes negative (-ve), in this case, we will add 26 in the negative value. Like, the third letter of the ciphertext;

N = 13 and S = 18

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

$D_i = (13 - 18) \bmod 26$

$D_i = -5 \bmod 26$

$D_i = (-5 + 26) \bmod 26$

$D_i = 21$

Ciphertext	K	E	N	T	U	T	G	B	O	X
Ciphertext value (E)	10	04	13	19	20	19	06	01	14	23
Key	B	E	S	T	B	E	S	T	B	E

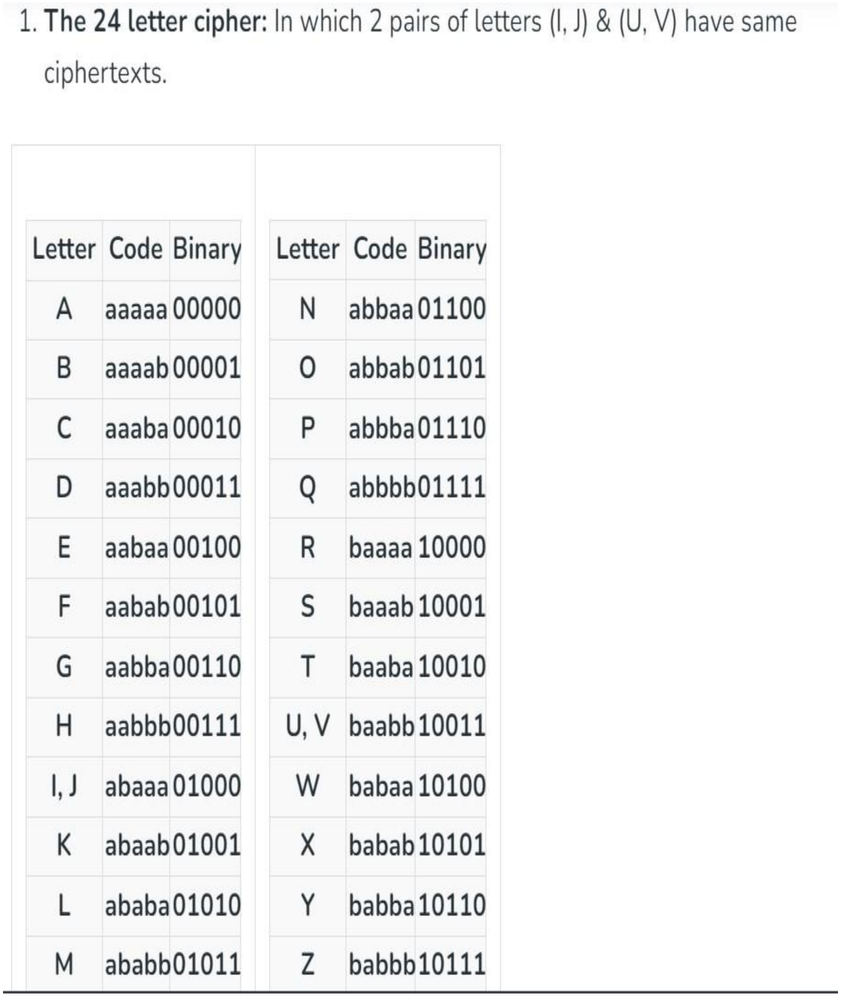
Key value (K)	01	04	18	19	01	04	18	19	01	04
Plaintext value (P)	09	00	21	00	19	15	14	08	13	19
Plaintext	J	A	V	A	T	P	O	I	N	T

4. Baconian Cipher

Bacon’s cipher or the Baconian cipher is a method of steganography (a method of hiding a secret message as opposed to just a cipher) devised by Francis Bacon in 1605. A message is concealed in the presentation of text, rather than its content. The Baconian cipher is a substitution cipher in which each letter is replaced by a sequence of 5 characters. In the original cipher, these were sequences of ‘A’s and ‘B’s e.g. the letter ‘D’ was replaced by ‘aaabb’, the letter ‘O’ was replaced by ‘abbab’ etc.

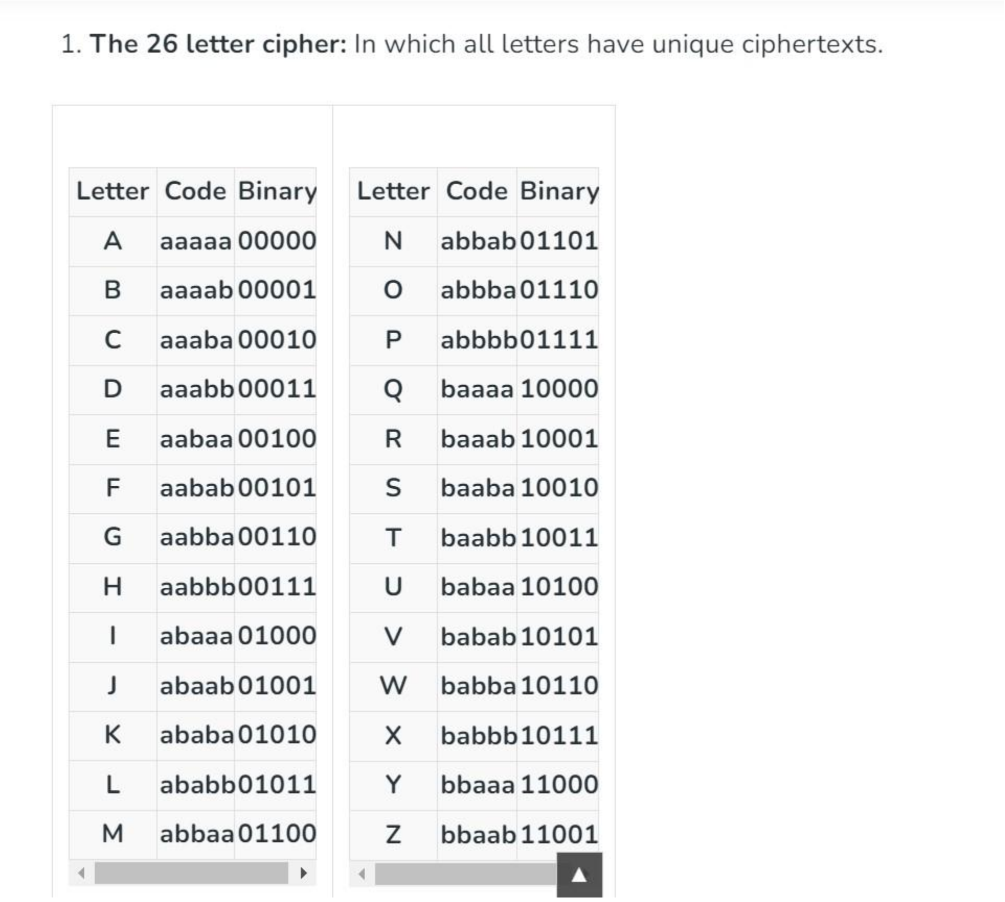
Each letter is assigned to a string of five binary digits. These could be the letters ‘A’ and ‘B’, the numbers 0 and 1 or whatever else you may desire.

There are 2 kinds of Baconian ciphers –



1. **The 24 letter cipher:** In which 2 pairs of letters (I, J) & (U, V) have same ciphertexts.

Letter	Code	Binary	Letter	Code	Binary
A	aaaaa	00000	N	abbaa	01100
B	aaaab	00001	O	abbab	01101
C	aaaba	00010	P	abbba	01110
D	aaabb	00011	Q	abbbb	01111
E	aabaa	00100	R	baaaa	10000
F	aabab	00101	S	baaab	10001
G	aabba	00110	T	baaba	10010
H	aabbb	00111	U, V	baabb	10011
I, J	abaaa	01000	W	babaa	10100
K	abaab	01001	X	babab	10101
L	ababa	01010	Y	babba	10110
M	ababb	01011	Z	babbb	10111

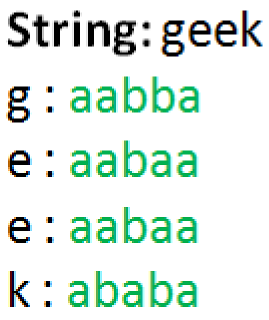


1. **The 26 letter cipher:** In which all letters have unique ciphertexts.

Letter	Code	Binary	Letter	Code	Binary
A	aaaaa	00000	N	abbab	01101
B	aaaab	00001	O	abbba	01110
C	aaaba	00010	P	abbbb	01111
D	aaabb	00011	Q	baaaa	10000
E	aabaa	00100	R	baaab	10001
F	aabab	00101	S	baaba	10010
G	aabba	00110	T	baabb	10011
H	aabbb	00111	U	babaa	10100
I	abaaa	01000	V	babab	10101
J	abaab	01001	W	babba	10110
K	ababa	01010	X	babbb	10111
L	ababb	01011	Y	bbaaa	11000
M	abbaa	01100	Z	bbaab	11001

Encryption

We will extract a single character from the string and if its not a space then we will replace it with its corresponding ciphertext according to the cipher we are using else we will add a space and repeat it until we reach the end of the string. For example 'A' is replaced with 'aaaaa'



String: geek

g : aabba

e : aabaa

e : aabaa

k : ababa