Vigenère Cipher

- Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.

- A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets .

- The encryption of the original text is done using the *Vigenère square or Vigenère table*.

Vigenere cipher

- The Vigenere cipher is the kind of polyalphabetic cipher.
- It was design by Blaise de Vigenere, a 16th century French mathematician.
- It was used in the American civil war and was once believed to be unbreakable.
- A Vigenere cipher uses a different strategy to create the key stream. The key stream is a repetition of an initial secret key stream of length m, where we have 1<=m<=26.
- The Vigenere cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.
- The Vigenere cipher uses multiple mixed alphabets, each is a shift cipher.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.
- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.
- The alphabet used at each point depends on a repeating keyword.

Vigenere Cipher

Plain text: $P = P_1 P_2 P_3 \ldots$

Cipher text: $C = C_1 C_2 C_3 \ldots$

Key stream: $K = [(k_1, k_2, \ldots, k_m), (k_1, k_2, \ldots, k_m), \ldots]$

Encryption: $C_i = P_i + k_i$

Decryption: $P_i = C_i - k_i$

Example

- Input :
- Plaintext : GEEKSFORGEEKS
- Keyword : AYUSH
- Output : Ciphertext : GCYCZFMLYLEIM
- For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.
- The keyword "AYUSH" generates the key "AYUSHAYUSHAYU"

Example

- We can encrypt the message **"She is listening"** using the 6-character keyword **"PASCAL"**. The initial key stream is **(15,0,18,2,0,11).** The key stream is the repetition of this initial key stream (as many times as needed) .

Use encryption algo: $C_i = P_i + k_i$

Plaintext:	s	h	e	i	s	l	i	s	t	e	n	i	n	g
P's values:	18	07	04	08	18	11	08	18	19	04	13	08	13	06
Key stream:	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*	*18*	*02*	*00*	*11*	*15*	*00*
C's values:	**07**	**07**	**22**	**10**	**18**	**22**	**23**	**18**	**11**	**6**	**13**	**19**	**02**	**06**
Ciphertext:	**H**	**H**	**W**	**K**	**S**	**W**	**X**	**S**	**L**	**G**	**N**	**T**	**C**	**G**

Vigenere Table

- Another way to look at Vigenere ciphers is through what is called a Vigenere Tableau, Vigenere Table or Vigenere Square.
- The first row of this table has the 26 English letters. Shows the plain text character to be encrypted.
- Starting with the second row, each row has the letters shifted to the left one position in a cyclic way. For example, when **B** is shifted to the first position on the second row, the letter **A** moves to the end.
- The first column contains the characters to be used by the 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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:-

- To find the cipher text for the plaintext **“she is listening ”** using the word **“PASCAL”** as the key

  - .we can find **“s”** in the first row**, “p”** in the first column, the cross section is the cross section is the cipher text character **“H”**

  - we can find **“h”** in the first row, **“A”** in the first column, the cross section is the cross section is the cipher text character **“H”**
  - And so on…..

Encryption example:

P.T "TO BE OR NOT TO BE THAT IS THE QUESTION"

Key : RELATIONS

Use Vigenere table method to encrypt plain text to cipher text.

Plaintext: TOBEO RNOTT OBETH ATIST HEQUE STION

Keyword: RELAT IONSR ELATI ONSRE LATIO NSREL

Ciphertext:KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Decrypt example:

“TO BE OR NOT TO BE THAT IS THE QUESTION”

Use Vigenere table method to decrypt cipher text to plain text.

Keyword: RELAT IONSR ELATI ONSRE LATIO NSREL

Ciphertext: KSMEH ZBBLK SMEMP OGAJX SEJCS FLZSY

Plaintext: TOBEO RNOTT OBETH ATIST HEQUE STION

Vigenere Cipher (Crypanalysis)

- This method was actually discovered earlier, in 1854 by Charles Babbage.

- Vigenere-like substitution ciphers were regarded by many as practically unbreakable for 300 years.

- In 1863, a Prussian major named **Kasiski** proposed a method for breaking a Vigenere cipher that consisted of finding the length of the keyword and then dividing the message into that many simple substitution cryptograms.