

## Project No. 4

Goal: To implement Vignere Cipher Substitution Technique.



Date :

### Practical No. 4

Aim: To implement Vignere Cipher Substitution Techniques.

Theory:

Vignere 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 Vignere square or Vignere table.

The table consist 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 cipher. 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 keywords.

The steps involved are as follows:

- ① Write the plaintext.
- ② Use the plaintext and the key letter to select a row and a column in the Vignere table.
- ③ The first letter of the plaintext is the first row and the key is the first column. For example, if the plaintext is INTELLPAT and the key is R, then the first row will be the one that starts with I, and the column will be the one that starts with R.
- ④ The first letter of ciphertext will be the letter where the first row and column intersect. In the case of our example that will be the letter Z.
- ⑤ Now, this process is continued till the entire plaintext is turned into a ciphertext. For INTELLPAT, that will be ZVHXPTXPAT.



Date :



Example :

sample input and output :

Main text	I	N	T	E	L	L	I	P	A	A	T
Key	R	I	N	T	E	L	L	I	P	A	A
Ciphertext	Z	V	U	X	P	W	T	X	P	A	T

Conclusion :

The concept of Vignere's cipher implemented successfully.

Viva Question :

① What is Vignere's cipher ?

→ Vignere cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. The encryption of the original text is done using the Vignere square or Vignere table.

② What are advantages of Vignere's cipher ?

- 
- ① It is more complex than the Caesar cipher.
  - ② It encrypts a message more securely than the Caesar cipher.
  - ③ It has large key space and it is largely ~~unbreakable~~ uncrackable without knowledge of method.

③ What are disadvantages of Vignere's cipher ?

- 
- ① Modern cryptanalysis techniques such as brute-force and other can efficiently break the Vignere cipher given enough ciphertext and computational power.
  - ② Key length and key repeating pattern.
  - ③ It lacks the sophisticated security feature found in modern cryptographic algorithms.