Practical No. 4

Aim: To implement Vigenere Cipher Substitution Technique.

Date :

Practical No.4

Aim : To implement Vignere cipher Substitution Techniques.

Theory :

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.

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 vigenere 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 INTELLIPAAT 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 INTELLIPAAT, that will be ZVGXPWTXPAT.

Date :

Exampe :

Sampe Input and output:

Plaintext	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	G	X	P	W	T	X	P	A	T

Conclusion:

The concept of Vignere's cipher implemented successfully.

Viva Question:

① What is Vigner'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 vigenere square or vigenere table.

② What is advantages of vigner's cipher?

→ ① It is more complex than the caesar cipher.

② It encrypt a message more securely than the caesar cipher.

③ It has large key space and it is largely ~~[illegible]~~ uncrackable without knowledge of method.

③ What is disadvantages of vigner's cipher?

→ ① modern cryptanalysis techniques such as brute-force and other can efficiently break the vigenere cipher given enough ciphertext and computational power.

② Key length and key repeating pattern.

③ It lacks the sophisticated security feature found in moder cryptographic algorithm.