**CRYPTOGRAPHY PROJECT**

**ENCRYPTION FOR PERSONAL DIARY**

**ANIKETH S HEGDE PES1201700104**

**MITHUN PES1201700197**

**SHAMITHA K PES1201700973**

This project uses both Vernam cipher and playfair cipher for encrypting a personal diary.

**Vernam cipher -**

Vernam Cipher is a method of encrypting alphabetic text. Here, we take a key to encrypt the plain text which length should be equal to the length of the plain text. The Vernam Cipher is based on the principle that each plaintext character from a message is 'mixed' with one character from a key stream. If a truly random key stream is used, the result will be a truly 'random' ciphertext which bears no relation to the original plaintext. In that case the cipher is similar to the unbreakable One-Time Pad.

**Vernam Cipher Encryption algorithm :**

1. Assign a number to each character of the plain-text and the key according to alphabetical order.
2. Add both the number (Corresponding plain-text character number and Key character number).
3. Subtract the number from 26 if the added number is greater than 26, if it isn’t then leave it.

**Playfair cipher –**

The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but was named after Lord Playfair who promoted the use of the cipher. The technique encrypts pairs of letters (digraphs), instead of single letters as in the simple substitution cipher. The Playfair is significantly harder to break since the frequency analysis used for simple substitution ciphers does not work with it. Frequency analysis can still be undertaken, but on the 25\*25=625 possible digraphs rather than the 25 possible monographs.

**The Playfair Cipher Encryption Algorithm:**

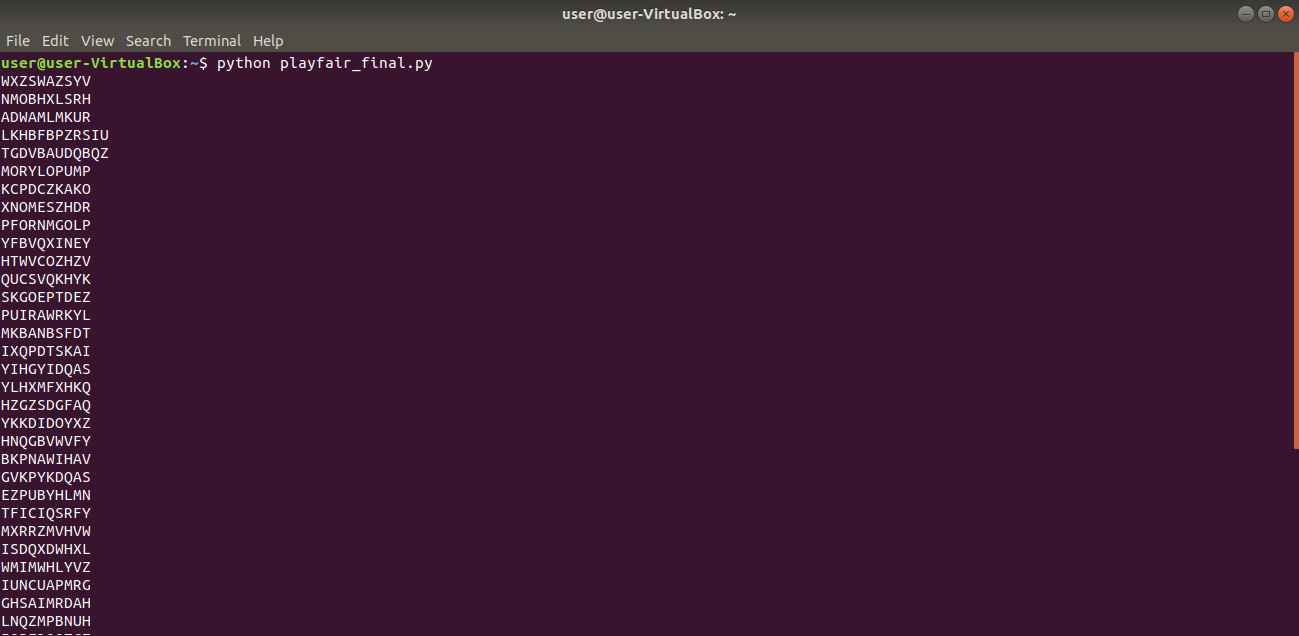
The Algorithm consists of 2 steps:

1. **Generate the key Square(5×5):**
   * The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I.
   * The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.
2. **Algorithm to encrypt the plain text:** The plaintext is split into pairs of two letters (digraphs). If there is an odd number of letters, a Z is added to the last letter.

Rules for Encryption:

* **If both the letters are in the same column**: Take the letter below each one (going back to the top if at the bottom).
* **If both the letters are in the same row**: Take the letter to the right of each one (going back to the leftmost if at the rightmost position).
* **If neither of the above rules is true**: Form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

**Output of the program :**

****