**Divya Shah**

**2019130057**

**TE Comps**

**Batch C**

## Experiment 1: Traditional Crypto Methods

## Aim:

**To implement Substitution, ROT 13, Transposition, Double Transposition and Vernam Cipher in Python.**

1) **Substitution Cipher**

```
1 Substitution
2 ROT 13
3 Transpose
4 Double Transposition
5 Vernam Cipher
6 Diffie Hellman
Enter the Cryptogrpahy Method you want to choose:1
Enter Plain Text to be encryptedDivya is my name
No of position to be shifted5
Encrypted Message Inadf%nx%rd%sfrj
Decrypted Message Divya is my name
```

2) **ROT 13**

```
1 Substitution
2 ROT 13
3 Transpose
4 Double Transposition
5 Vernam Cipher
6 Diffie Hellman
Enter the Cryptogrpahy Method you want to choose:2
Enter Plain Text to be encryptedDivya is my name
Encrypted Message Qviln-vf-zl-anzr
Decrypted Message Divya is my name

Process finished with exit code 0
```

**3) Transpose Cipher**

```
1 Substitution
2 ROT 13
3 Transpose
4 Double Transposition
5 Vernam Cipher
6 Diffie Hellman
Enter the Cryptogrpahy Method you want to choose:3
Enter Plain Text to be encryptedDivya is my name
Enter keyhash
Encrypted Message i maDa nys eviym
Decrypted Message Divya is my name

Process finished with exit code 0
```

**4) Double Transposition**

```
1 Substitution
2 ROT 13
3 Transpose
4 Double Transposition
5 Vernam Cipher
6 Diffie Hellman
Enter the Cryptogrpahy Method you want to choose:4
Enter Plain Text to be encryptedDivya is my name
Enter keyhash
 asiiDyvanemm  y
Divya is my name

Process finished with exit code 0
```

5) **Vernam Cipher**

```
1 Substitution
2 ROT 13
3 Transpose
4 Double Transposition
5 Vernam Cipher
6 Diffie Hellman
Enter the Cryptogrpahy Method you want to choose:5
Enter Plain Text to be encryptedDIVYAISMYNAME
Enter key textQWERTYUIOPASD
TEZPTGMUMCAEH
DIVYAISMYNAME

Process finished with exit code 0
```

**Conclusion:**

I feel substitution cipher and ROT 13 techniques are easier to decipher for an attacker using letter frequencies. To make substitution cipher safer and efficient we have to use polyalphabetic cipher technique. Substitution cipher can also be made complex by using permutations and combinations.

ROT 13 I feel is very easy to decrypt because the attacker knows that cipher ROT 13 is used then there is no other data necessary to decrypt the message.

Transpose Cipher has better mixing of letters than the rest of the ciphers so I feel this has much better security than rest of the methods. Cipher text generated by transpose cipher can be re encrypted to create a more secure encryption. This is called Double Transpose Cipher. I feel using transpose cipher and substitution cipher together would create a better and tougher encryption technique for the attacker to crack.

Vernam Cipher provides better encryption than many other techniques due to the presence of the secret key used for both encryption and decryption. The major disadvantage of vernam cipher is that the key length should be of the size of data. This renders this technique tiresome and requires high computational power for bigger data.