Divya Shah

2019130057

TE Comps

Batch C

Experiment 2: Traditional Crypto Methods

Aim:

To implement Diffie Hellman Key Exchange Algorithm.

1) **Diffie Hellman**

```
1 Substitution
2 ROT 13
3 Transpose
4 Double Transposition
5 Vernam Cipher
6 Diffie Hellman
Enter the Cryptogrpahy Method you want to choose:6
Enter the Public Keys
Enter Prime Number P: 1500450271
Enter Prime Number G: 3628273133
Private KeyA4093082899
Private KeyB3367900313
Secret key for the Alice is : 559050762
Secret Key for the Bob is : 559050762

Process finished with exit code 0
```

Conclusion:

Diffie Hellman is a safe key exchange algorithm for secret communication on public platform. It makes possible for two parties to agree on a secret key with giving away key information openly. Diffie Hellman is computation intensive for higher data in terms of resources and CPU Power.

Github Link:

https://github.com/Divya-127/CSS-Lab/tree/main/Exp2