Experiment 3

Shashwat Shah
60004220126
TYBtech Comps B

Aim : Study and implement Vernam Cipher

Theory : Vernam cipher is a method of encrypting alphabetic text. It is one of the substitution cipher techniques to converting plaintext into cipher text.

In this mechanism, we assign a number to each character of the plaintext, like (a=0, b=1, c=2, z=25). Method to take key : In the vernam cipher algorithm, we take a key to encrypt the plaintext whose length should be equal to the length of the plaintext.

Encryption Algorithm

1) Assign a number to each character of the plain text and key according to the alphabetic order.
2) Bitwise XOR both the numbers (corresponding plaintext character number and key character number).
3) Subtract the number from 26 if the resulting number is greater than or equal to 26. If it isnt then leave it.

Eg Plaintext 'OAK'
key ! 'SON'

key –	S	O	N
	18	14	13
Plaintext –	O	A	K
	18	0	10

ciphertext	C	O	H
	02	14	07

∴ cipher text : 'COH'

Conclusion : Both encryption and decryption algorithm are simple and involve a bitwise XOR operation . This simplicity can be an advantage in some situation . But the key must be atleast as long as the message, which can be inefficient for long messages.

Thus we studied and implemented vernam cipher

EXPERIMENT 3

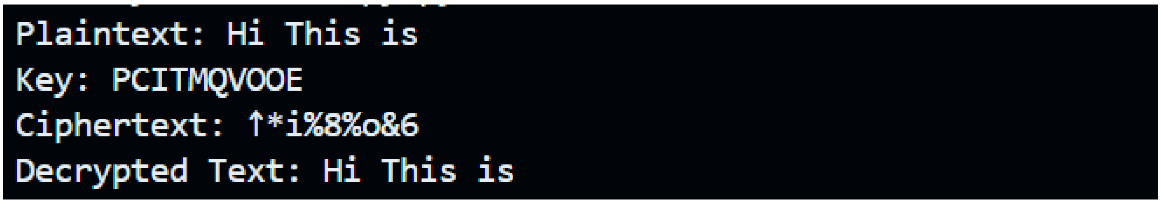
Shashwat Shah
TYBtech Comps B
C22
60004220126

AIM: Study and Implement Vernam Cipher.

CODE:

```
import random
def generate_key(plaintext_length):
    key = ''.join(random.choice('ABCDEFGHIJKLMNOPQRSTUVWXYZ') for _ in
range(plaintext_length))
    return key

def encrypt(plaintext, key):
    ciphertext = ''.join(chr(ord(p) ^ ord(k)) for p, k in zip(plaintext, key))
    return ciphertext
def decrypt(ciphertext, key):
    decrypted_text = ''.join(chr(ord(c) ^ ord(k)) for c, k in zip(ciphertext,
key))
    return decrypted_text

if __name__ == "__main__":
    plaintext = "Hi This is Prerna"
    key = generate_key(len(plaintext))

    print("Plaintext:", plaintext)
    print("Key:", key)

    ciphertext = encrypt(plaintext, key)
    print("Ciphertext:", ciphertext)

    decrypted_text = decrypt(ciphertext, key)
    print("Decrypted Text:", decrypted_text)
```

OUTPUT:



```
Plaintext: Hi This is
Key: PCITMQVOOE
Ciphertext: ↑*i%8%o&6
Decrypted Text: Hi This is
```