Name: Jigar Siddhpura **SAPID:** 60004200155

DIV: C/C2 **Branch:** Computer Engineering

IS - Experiment 3 - VERNAM CIPHER

Jigar Siddhpura
60004220155
C22

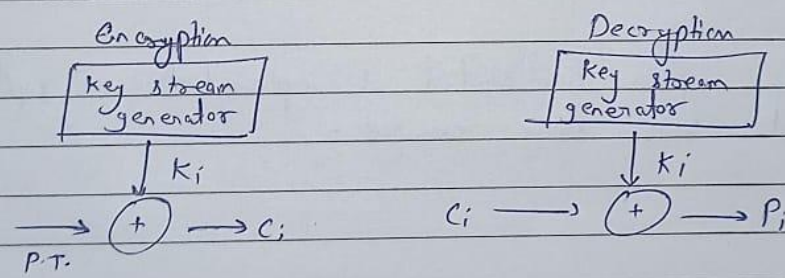
Exp 3 : Vernam Cipher

Aim: To Study & implement Vernam Cipher

Theory:

Vernam cipher is a symmetric encryption technique that offers perfect secrecy when implemented correctly. A random key bits are generated with same length as P.T. After this letters of key & P.T. are converted into ascii number or a no. is assigned (as a=0, b=1, c=2 ...) Then this binary equivalent is calculated. During encryption, XOR binary bits are calculated btw P.T. & key binary bits giving binary C.T. & finally converted back to text. For decryption, similar process, just XOR operation is done btw key & C.T. giving plaintext.

Diagrammatically:



Eg: P.T. : RAMSWARUPK
Key : RANCHOBABA

So operation happens:

P.T.	R	A	M	S	W	A	R	U	P	K
No.	17	0	12	18	22	0	17	20	15	10
Key	R	A	N	C	H	O	B	A	B	A
No.	17	0	13	2	7	14	1	0	1	0
XOR → C.T	0	0	1	16	17	14	16	20	14	10

Ciphertext : A A B Q R O Q U O K

Decryption:

	0	0	1	16	17	14	16	20	14	10
C.T. ⊕ Key no.	17	0	13	2	7	14	1	0	1	0
P.T. no. :	17	0	12	18	22	0	17	20	15	10
P.T. :	R	A	M	S	W	A	R	U	P	R

Conclusion:

So vernam cipher was studied & implemented on python & tested with above example.

CODE

```
def generate_key(plain_text, key):
    key_list = list(key)
    if len(plain_text) == len(key_list):
        return "".join(key_list)
    else:
        for i in range(len(plain_text) - len(key_list)):
            key_list.append(key_list[i % len(plain_text)])
        return "".join(key_list)

def encrypt(plain_text, key):
    cipher_text = []
    for i in range(len(plain_text)):
        x = (ord(plain_text[i]) - 65) ^ (ord(key[i]) - 65)
        x += ord("A")
        cipher_text.append(chr(x))
    return "".join(cipher_text)

def decrypt(cipher_text, key):
    decrypted_text = []
    for i in range(len(cipher_text)):
        x = (ord(cipher_text[i]) - 65) ^ (ord(key[i]) - 65)
        x += ord("A")
        decrypted_text.append(chr(x))
    return "".join(decrypted_text)

plaintext = input("Enter the plaintext : ").upper()
key = input("Enter the key : ").upper()

print(f"Plain Text: {plaintext}\nKey: {key}\n")

key = generate_key(plaintext, key)
print("Encrypted cipher text is:", encrypt(plaintext, key))

ciphered_text = encrypt(plaintext, key)
print("Decrypted text is:", decrypt(ciphered_text, key))
```

OUTPUT

```
PS D:\SEM-6\IS\EXPERIMENTS> python -u "d:\SEM-6\IS\EXPERIMENTS\vernam.py"
Enter the plaintext : GOODMORNING
Enter the key : ZEBRA
Plain Text: GOODMORNING
Key: ZEBRA

Encrypted cipher text is: `KPSMXVMZN`
Decrypted text is: GOODMORNING
PS D:\SEM-6\IS\EXPERIMENTS>
```