Shri Vile Parle Kelavani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC Accredited with "A" Grade (CGPA : 3.18)

Experiment 4

Date of Performance : 4 March 2023 **Date of Submission:** 4 March 2023

SAP Id: 60004200132 **Name :** Ayush Jain

Div: B **Batch :** B3

Aim of Experiment

Design and Implement Electronic Code Book(ECB) algorithmic mode. Plaintext is given as paragraph. First convert given paragraph into ASCII values and then Binary. Use 128 bits of block as input to ECB and encrypt using "t" bits shifter(Left/Right). Display encrypted paragraph.

Theory / Algorithm / Conceptual Description:

Electronic Codebook (ECB) is a mode of operation in symmetric-key encryption that encrypts each plaintext block independently of the other blocks. In ECB mode, the encryption algorithm takes a fixed-size block of plaintext and produces a fixed-size block of ciphertext. The plaintext is divided into these fixed-size blocks, and each block is encrypted using the same key and encryption algorithm.

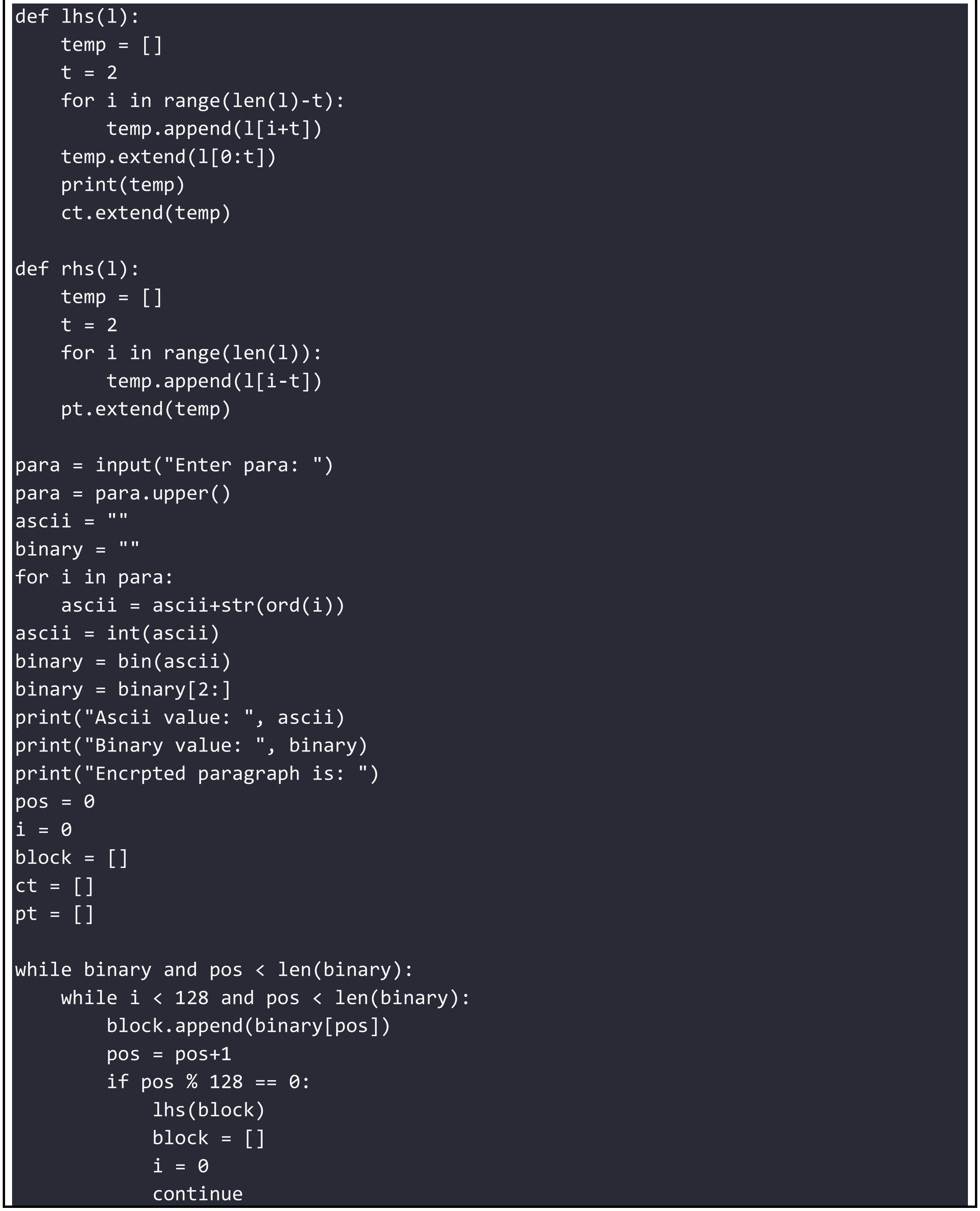
ECB is a straightforward and efficient mode of operation, but it has some significant limitations. One of the main problems with ECB is that identical plaintext blocks result in identical ciphertext blocks, which can reveal patterns in the plaintext. This makes it vulnerable to some attacks, such as frequency analysis or known-plaintext attacks.

Another limitation of ECB is that it doesn't provide any integrity or authentication of the message. An attacker can modify the ciphertext blocks, and the receiver will not be able to detect the modification.

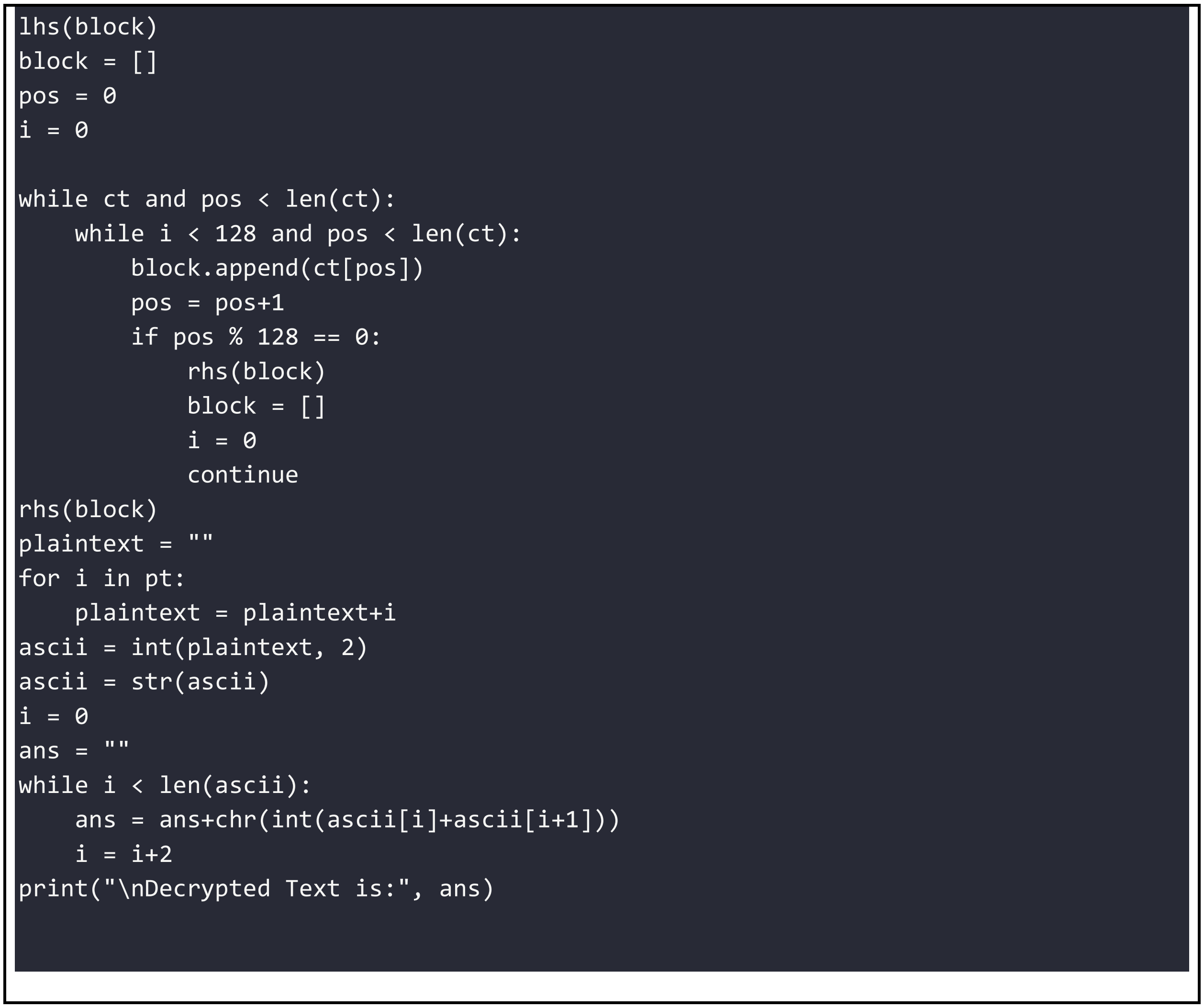
Despite these limitations, ECB is still used in some applications where security is not a primary concern, or the data being encrypted is of low sensitivity. ECB is also useful in some applications where individual blocks must be encrypted or decrypted independently, such as storing large files on a disk.

In summary, while ECB is simple and efficient, it is not considered a secure mode of operation for modern cryptographic applications.

Program

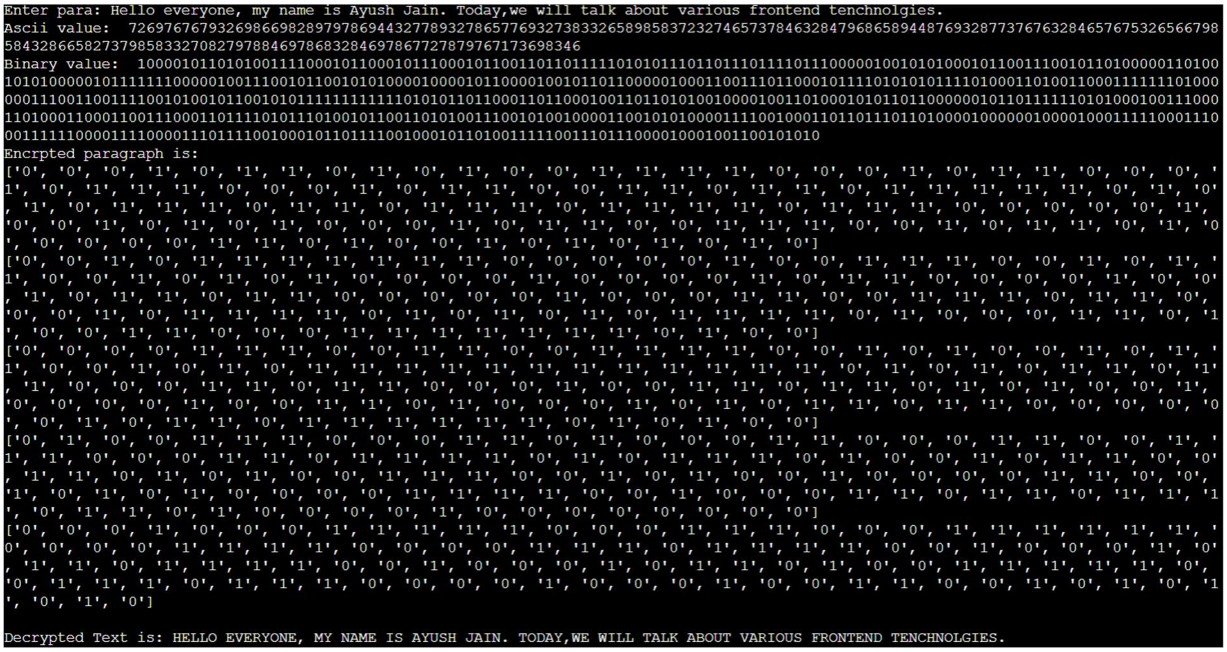


```python
def lhs(l):
    temp = []
    t = 2
    for i in range(len(l)-t):
        temp.append(l[i+t])
    temp.extend(l[0:t])
    print(temp)
    ct.extend(temp)

def rhs(l):
    temp = []
    t = 2
    for i in range(len(l)):
        temp.append(l[i-t])
    pt.extend(temp)

para = input("Enter para: ")
para = para.upper()
ascii = ""
binary = ""
for i in para:
    ascii = ascii+str(ord(i))
ascii = int(ascii)
binary = bin(ascii)
binary = binary[2:]
print("Ascii value: ", ascii)
print("Binary value: ", binary)
print("Encrpted paragraph is: ")
pos = 0
i = 0
block = []
ct = []
pt = []

while binary and pos < len(binary):
    while i < 128 and pos < len(binary):
        block.append(binary[pos])
        pos = pos+1
        if pos % 128 == 0:
            lhs(block)
            block = []
            i = 0
            continue
```



```
lhs(block)
block = []
pos = 0
i = 0

while ct and pos < len(ct):
    while i < 128 and pos < len(ct):
        block.append(ct[pos])
        pos = pos+1
        if pos % 128 == 0:
            rhs(block)
            block = []
            i = 0
            continue
rhs(block)
plaintext = ""
for i in pt:
    plaintext = plaintext+i
ascii = int(plaintext, 2)
ascii = str(ascii)
i = 0
ans = ""
while i < len(ascii):
    ans = ans+chr(int(ascii[i]+ascii[i+1]))
    i = i+2
print("\nDecrypted Text is:", ans)
```

Output



```
Enter para: Hello everyone, my name is Ayush Jain. Today,we will talk about various frontend tenchnolgies.
Ascii value:  72697676793269866982897978694432778932786577693273833265898583723274657378463284796865894487693287737676328465767532656679858432866582737985833270827978846978683284697867727879767173698346
Binary value:  10000101101010011110001011000101110001011001101101111101010111011011101111011100000100101010001011001110010110100000110100
1010100000101111111100000100111001011001010100001000010110000100101101100000100011001110110001011110101010111101000110100110001111111101000
000111001100111100101001011001010111111111111101010110110001101100010011011010100100001001101000101011011000000101101111110101000100111000
1101000110001100111000110111101011101001011001101010011100101001000011001010100001111001000110110111011010000100000001000010001111110001110
00111111000011110000111011110010001011011110010001011010011111001110111000010001001100101010
Encrpted paragraph is:
['0', '0', '0', '1', '0', '1', '1', '0', '1', '0', '1', '0', '0', '1', '1', '1', '1', '0', '0', '0', '1', '0', '1', '1', '0', '0', '0', '
1', '0', '1', '1', '1', '0', '0', '0', '1', '0', '1', '1', '0', '0', '1', '1', '0', '1', '1', '0', '1', '1', '1', '1', '1', '0', '1', '0'
, '1', '0', '1', '1', '1', '0', '1', '1', '0', '1', '1', '1', '0', '1', '1', '1', '1', '0', '1', '1', '1', '0', '0', '0', '0', '0', '1',
'0', '0', '1', '0', '1', '0', '1', '0', '0', '0', '1', '0', '1', '1', '0', '0', '1', '1', '1', '0', '0', '1', '0', '1', '1', '0', '1', '0
', '0', '0', '0', '0', '1', '1', '0', '1', '0', '0', '1', '0', '1', '0', '1', '0', '1', '0']
['0', '0', '1', '0', '1', '1', '1', '1', '1', '1', '1', '0', '0', '0', '0', '0', '1', '0', '0', '1', '1', '1', '0', '0', '1', '0', '1', '
1', '0', '0', '1', '0', '1', '0', '1', '0', '0', '0', '0', '1', '0', '0', '0', '0', '1', '0', '1', '1', '0', '0', '0', '0', '1', '0', '0'
, '1', '0', '1', '1', '0', '1', '1', '0', '0', '0', '0', '0', '1', '0', '0', '0', '1', '1', '0', '0', '1', '1', '1', '0', '1', '1', '0',
'0', '0', '1', '0', '1', '1', '1', '1', '0', '1', '0', '1', '0', '1', '0', '1', '1', '1', '1', '0', '1', '0', '0', '0', '1', '1', '0', '1
', '0', '0', '1', '1', '0', '0', '0', '1', '1', '1', '1', '1', '1', '1', '0', '1', '0', '0']
['0', '0', '0', '0', '1', '1', '1', '0', '0', '1', '1', '0', '0', '1', '1', '1', '1', '0', '0', '1', '0', '1', '0', '0', '1', '0', '1', '
1', '0', '0', '1', '0', '1', '0', '1', '1', '1', '1', '1', '1', '1', '1', '1', '1', '1', '1', '0', '1', '0', '1', '0', '1', '1', '0', '1'
, '1', '0', '0', '0', '1', '1', '0', '1', '1', '0', '0', '0', '1', '0', '0', '1', '1', '0', '1', '1', '0', '1', '0', '1', '0', '0', '1',
'0', '0', '0', '0', '1', '0', '0', '1', '1', '0', '1', '0', '0', '0', '1', '0', '1', '0', '1', '1', '0', '1', '1', '0', '0', '0', '0', '0
', '0', '1', '0', '1', '1', '0', '1', '1', '1', '1', '1', '1', '0', '1', '0', '1', '0', '0']
['0', '1', '0', '0', '1', '1', '1', '0', '0', '0', '1', '1', '0', '1', '0', '0', '0', '1', '1', '0', '0', '0', '1', '1', '0', '0', '1', '
1', '1', '0', '0', '0', '1', '1', '0', '1', '1', '1', '1', '0', '1', '0', '1', '1', '1', '0', '1', '0', '0', '1', '0', '1', '1', '0', '0'
, '1', '1', '0', '1', '0', '1', '0', '0', '1', '1', '1', '0', '0', '1', '0', '1', '0', '0', '1', '0', '0', '0', '0', '1', '1', '0', '0',
'1', '0', '1', '0', '1', '0', '0', '0', '0', '1', '1', '1', '1', '0', '0', '1', '0', '0', '0', '1', '1', '0', '1', '1', '0', '1', '1', '1
', '0', '1', '1', '0', '1', '0', '0', '0', '0', '1', '0', '0', '0', '0', '0', '0', '0', '0']
['0', '0', '0', '1', '0', '0', '0', '1', '1', '1', '1', '1', '0', '0', '0', '1', '1', '1', '0', '0', '0', '1', '1', '1', '1', '1', '1', '
0', '0', '0', '0', '1', '1', '1', '1', '0', '0', '0', '0', '1', '1', '1', '0', '1', '1', '1', '1', '0', '0', '1', '0', '0', '0', '1', '0'
, '1', '1', '0', '1', '1', '1', '1', '0', '0', '1', '0', '0', '0', '1', '0', '1', '1', '0', '1', '0', '0', '1', '1', '1', '1', '1', '0',
'0', '1', '1', '1', '0', '1', '1', '1', '0', '0', '0', '0', '1', '0', '0', '0', '1', '0', '0', '1', '1', '0', '0', '1', '0', '1', '0', '1
', '0', '1', '0']

Decrypted Text is: HELLO EVERYONE, MY NAME IS AYUSH JAIN. TODAY,WE WILL TALK ABOUT VARIOUS FRONTEND TENCHNOLGIES.
```

CONCLUSION: We have successfully implemented the electronic code book (ECB) where the plain text is a paragraph.