CNS PRACTICAL 4

Aim: Design and Implement a product cipher using Substitution ciphers and Transposition Cipher.

Theory:
A product cipher is a type of encryption scheme that combines multiple encryption techniques, such as substitution and transposition ciphers, in order to enhance security. By applying multiple layers of encryption, product ciphers aim to provide a higher level of complexity and make it more difficult for attackers to break the cipher.

Substitution Cipher:
The substitution cipher is a method where each letter of the plaintext is replaced with another letter or symbol according to a fixed rule or key.
For example, a simple substitution cipher may replace each letter with the letter that appears three positions after it in the alphabet.

a. Substitution Encryption: Apply a substitution cipher to the plaintext to produce a modified plaintext (substituted characters).
b. Transposition Encryption: Rearrange the substituted characters from the previous step using a transposition cipher to create the ciphertext.

Transposition Cipher:
The transposition cipher is a method where the letters of the plaintext are rearranged or permuted based on a fixed rule or key.
For example, a simple transposition cipher may rearrange the letters in the plaintext in a specific pattern, such as reading them in columns instead of rows.

a. Transposition Decryption: Reverse the transposition cipher to rearrange the ciphertext into the substituted characters.
b. Substitution Decryption: Apply the inverse of the substitution cipher to obtain the original plaintext.

Review Questions

1. Explain the basic structure of a product cipher. How does it combine multiple encryption methods to enhance security?

Ans:

- A product cipher is an encryption method that combines two or more simple ciphers (such as substitution and transposition) in sequence.
- The idea is that while a single substitution or transposition alone may be weak, their combination multiplies the security and makes cryptanalysis harder.
- Structure:
  - Input plaintext → Apply first cipher (e.g., substitution) → Apply second cipher (e.g., transposition) → … → Final ciphertext.
- By mixing different operations, product ciphers create a more complex relationship between plaintext and ciphertext, enhancing security.

2. Explain product cipher and describe its components and encryption process, with example.

Ans:Components of a product cipher:

- **Substitution** → Replaces characters/blocks with others (adds confusion).
- **Transposition (Permutation)** → Rearranges positions of characters/blocks (adds diffusion).
- **Multiple Rounds** → Repeated application increases strength.

Encryption Process (Example):

- **Suppose plaintext = HELLO**
- **Step 1: Substitution (Caesar shift by +3):** HELLO → KHOOR
- **Step 2: Transposition (reverse order):** KHOOR → ROOHK
- **Ciphertext = ROOHK**

Here, neither substitution nor transposition alone would be very strong, but together they form a more secure product cipher.

3. Discuss how the security of a product cipher depends on the strength and secrecy of its component ciphers.

Ans:

- A product cipher is only as strong as its components.
- If one component is weak, cryptanalysts may exploit it to reduce the overall complexity.
- Secrecy of keys is critical — if attackers know the substitution or transposition rules, the cipher becomes vulnerable.
- Combination matters — for example, applying only substitution repeatedly does not add much strength, but mixing substitution and permutation in multiple rounds creates strong confusion and diffusion.
- This principle influenced modern block ciphers like DES, AES, which are essentially complex product ciphers.

In what scenarios might a product cipher be less effective or unnecessary compared to modern encryption methods?

4. In what scenarios might a product cipher be less effective or unnecessary compared to modern encryption methods?

Ans:

When strong modern algorithms exist: Algorithms like AES already provide robust security and are optimized — simple product ciphers are outdated.

Resource constraints: In lightweight systems (IoT devices), a full product cipher with many rounds may be too heavy. Instead, tailored lightweight ciphers are preferred.

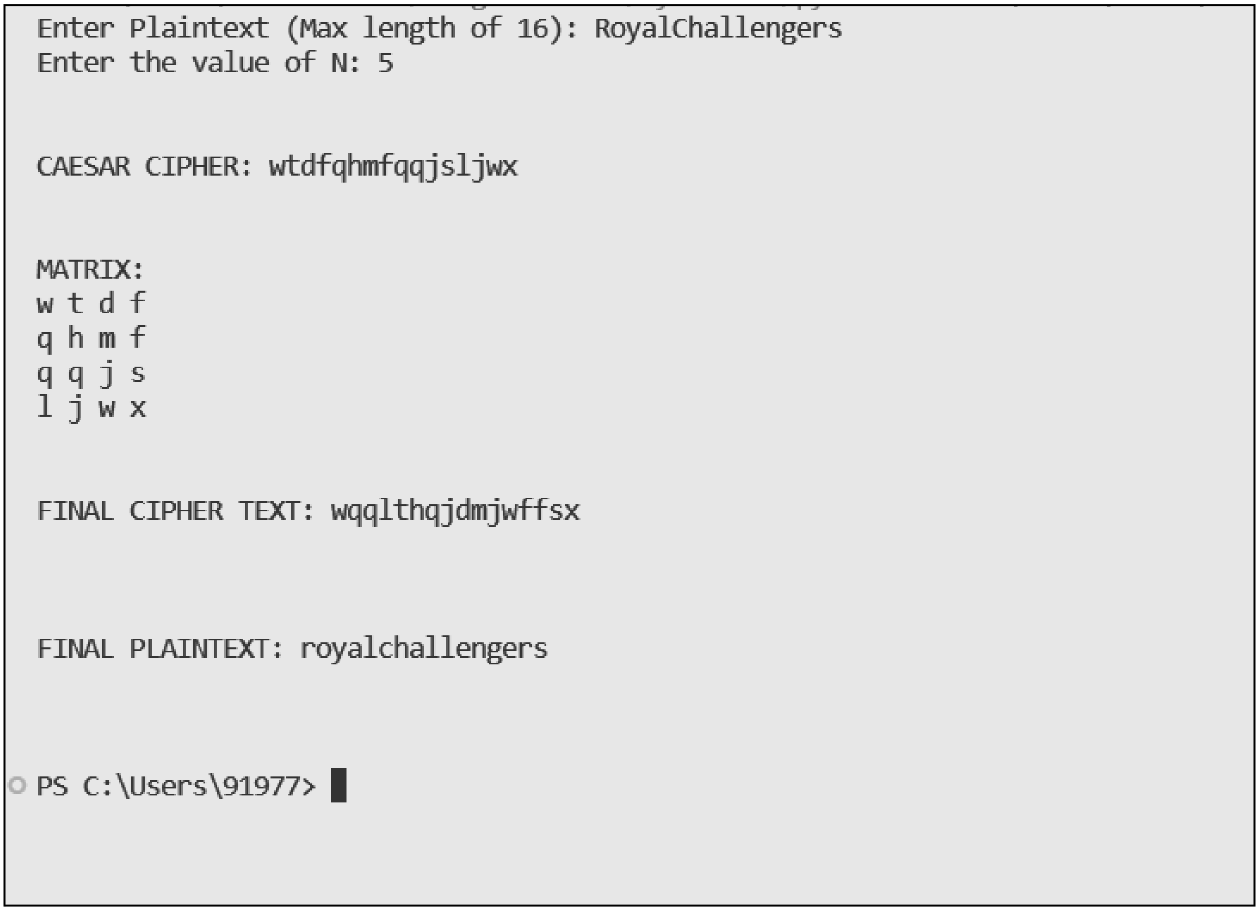
Short messages or low-security needs: If the data isn't sensitive (e.g., puzzles, games), product ciphers may be overkill.

Cryptanalysis advances: Classical product ciphers (like substitution + transposition) are vulnerable to frequency analysis and known-plaintext attacks, making them less effective for serious security applications.

Code:

```
plaintext = input("Enter Plaintext (Max length of 16): ")
plaintext = plaintext.lower().replace(" ", "")[:16]
n = int(input("Enter the value of N: "))
alphaToNum = {
'a': 0, 'b': 1, 'c': 2, 'd': 3, 'e': 4, 'f': 5,
'g': 6, 'h': 7, 'i': 8, 'j': 9, 'k': 10, 'l': 11,
'm': 12, 'n': 13, 'o': 14, 'p': 15, 'q': 16, 'r': 17,
's': 18, 't': 19, 'u': 20, 'v': 21, 'w': 22, 'x': 23,
'y': 24, 'z': 25
}
numToAlpha = {v: k for k, v in alphaToNum.items()}
while len(plaintext) < 16:
plaintext += "z"
ciphertext = ""
for i in plaintext:
ciphertext += numToAlpha[(alphaToNum[i] + n) % 26]
print("\n\nCAESAR CIPHER:", ciphertext)
matrix = [list(ciphertext[i:i+4]) for i in range(0, 16, 4)]
finalcipher = ""
for col in range(4):
for row in range(4):
finalcipher += matrix[row][col]
print("\n\nMATRIX:")
for row in matrix:
print(" ".join(row))
print("\n\nFINAL CIPHER TEXT:", finalcipher)
print("\n\n")
dec_matrix = [["" for _ in range(4)] for _ in range(4)]
k = 0
for col in range(4):
for row in range(4):
dec_matrix[row][col] = finalcipher[k]
k += 1
plaintext = ""
for row in dec_matrix:
plaintext += "".join(row)
finalplaintext = ""
for i in plaintext:
temp = alphaToNum[i] - n
if temp < 0:
temp += 26
finalplaintext += numToAlpha[temp % 26]
print("FINAL PLAINTEXT:", finalplaintext)
print("\n\n")
```

Output:



```
Enter Plaintext (Max length of 16): RoyalChallengers
Enter the value of N: 5


CAESAR CIPHER: wtdfqhmfqqjsljwx


MATRIX:
w t d f
q h m f
q q j s
l j w x


FINAL CIPHER TEXT: wqqlthqjdmjwffsx



FINAL PLAINTEXT: royalchallengers



PS C:\Users\91977> 
```