**Department of Computer Engineering**

**Name of the Student: Parth Das Roll Number: C-111**

**SAP ID: 60004220185 Class: Comps Division: C-2 Batch: 2**

**Subject: Information Security**

**DATE OF PERFORMANCE: 08/03/2025 DATE OF SUBMISION: 08/03/2025**

**EXPERIMENT NO: 6**

**AIM:** Design and Implement your "own" cipher combining "Substitution" and "Transposition" techniques.

**Theory:**

**SOURCE CODE WITH OUTPUTS:**

def substitute(text, key):

shift = sum(ord(c) for c in key) % 256

substituted = [(ord(c) + shift) % 256 for c in text]

# Convert to 3-digit numbers (000-255)

return ''.join(f"{b:03d}" for b in substituted)

def transpose(numeric\_str, key):

chunk\_size = max(len(key), 1)

# Split into 3-digit number groups

groups = [numeric\_str[i:i+3] for i in range(0, len(numeric\_str), 3)]

# Split into chunks based on key length

chunks = [groups[i:i+chunk\_size] for i in range(0, len(groups), chunk\_size)]

# Reverse order of chunks and join

transposed = ''.join(''.join(chunk[::-1]) for chunk in chunks)

return transposed

def encrypt(plaintext, key):

"""Combined substitution + transposition encryption"""

substituted = substitute(plaintext, key)

return transpose(substituted, key)

def unsubstitute(numeric\_str, key):

"""Reverse the substitution cipher"""

shift = sum(ord(c) for c in key) % 256

# Split into 3-digit numbers

groups = [numeric\_str[i:i+3] for i in range(0, len(numeric\_str), 3)]

# Convert back to bytes and unshift

original = [(int(g) - shift) % 256 for g in groups]

return ''.join(chr(b) for b in original)

def decrypt(ciphertext, key):

"""Decryption: reverse transposition then substitution"""

transposed = transpose(ciphertext, key) # Transpose is self-inverse

return unsubstitute(transposed, key)

key = "power"

plaintext = "hello world!"

encrypted = encrypt(plaintext, key)

print(f"Encrypted: {encrypted}")

decrypted = decrypt(encrypted, key)

print(f"Decrypted: {decrypted}")

**Output:-**



**CONCLUSION:**

The experiment showed that This cipher combines substitution (character shifting) and transposition (chunk reversal) for layered encryption.The key dynamically determines the shift value and chunk size, making each encryption unique. Ciphertext is represented as numeric strings (3 digits per character) to obscure patterns.The process is fully reversible, ensuring accurate decryption with the correct key.