**Ques 11.** Implement a stream cipher technique.

Ans:-

# Bharat\_Sharma CSC/20/50 Univ\_Roll\_No: 20059570040

def rc4\_keystream(key):

"""Generate a pseudorandom keystream using the RC4 algorithm."""

S = list(range(256))

j = 0

for i in range(256):

j = (j + S[i] + key[i % len(key)]) % 256

S[i], S[j] = S[j], S[i]

i = 0

j = 0

while True:

i = (i + 1) % 256

j = (j + S[i]) % 256

S[i], S[j] = S[j], S[i]

yield S[(S[i] + S[j]) % 256]

def stream\_cipher(plaintext, key):

keystream = rc4\_keystream(key)

ciphertext = []

for byte in plaintext:

keystream\_byte = next(keystream)

ciphertext\_byte = byte ^ keystream\_byte

ciphertext.append(ciphertext\_byte)

return bytes(ciphertext)

if \_\_name\_\_ == "\_\_main\_\_":

plaintext = b"Hello, world!"

key = b"secretkey"

ciphertext = stream\_cipher(plaintext, key)

print("Cipher Text ==> ",ciphertext)

decrypted\_plaintext = stream\_cipher(ciphertext, key)

print("Deciphered Text ==> ",decrypted\_plaintext)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_OUTPUT:-

