**Rivest Cipher (RC4)**

**CSE 459: Cryptography & Network Security**

Submitted by

Name : Pranav Mudigonda

Roll No: AP22110010765

Section: CSE Y

Lab Date: 10/02/2025

Submission Date: 10/02/2025

**A picture containing text

Description automatically generated**

**Department Computer Science and Engineering**

**School of Engineering and Sciences**

**SRM University–AP**

**Amaravati, Andhra Pradesh – 522240, India**

**Question**

Modify the client server program, use  RC4 to encrypt the communication, encrypt a file at the client end and send the data decrypt it at the servicer side and recreate the encrypted file and decrypt it.  
(You will have 2 file at server encrypted file and decrypted file)  
(You can use python library to implement this lab task)

**Solution :**

**from secrets import token\_bytes**

**def KSA(key):**

**S = [i for i in 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]**

**return S**

**def PRGA(S, text\_length):**

**i = j = 0**

**key\_stream = []**

**for \_ in range(text\_length):**

**i = (i + 1) % 256**

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

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

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

**key\_stream.append(S[t])**

**return key\_stream**

**def rc4\_encrypt\_decrypt(text, key):**

**S = KSA(key)**

**key\_stream = PRGA(S, len(text))**

**result = ''.join(chr(ord(text[i]) ^ key\_stream[i]) for i in range(len(text)))**

**return result**

**def encrypt\_text():**

**input\_text = input("Enter a string to encrypt: ")**

**key = token\_bytes(16)**

**key = list(key)**

**cipher\_text = rc4\_encrypt\_decrypt(input\_text, key)**

**with open("EncryptedText.txt", "w", encoding="utf-8") as enc\_file:**

**enc\_file.write(cipher\_text)**

**decrypted\_text = rc4\_encrypt\_decrypt(cipher\_text, key)**

**with open("DecryptedText.txt", "w", encoding="utf-8") as dec\_file:**

**dec\_file.write(decrypted\_text)**

**print("Encryption & Decryption completed! Check 'EncryptedText.txt' & 'DecryptedText.txt'.")**

**def encrypt\_file():**

**filename = input("Enter filename (with extension) to encrypt: ")**

**try:**

**with open(f'{filename}', "r", encoding="utf-8") as file:**

**file\_data = file.read()**

**key = token\_bytes(16)**

**key = list(key)**

**encrypted\_data = rc4\_encrypt\_decrypt(file\_data, key)**

**with open("EncryptedFile.txt", "w", encoding="utf-8") as enc\_file:**

**enc\_file.write(encrypted\_data)**

**decrypted\_data = rc4\_encrypt\_decrypt(encrypted\_data, key)**

**with open("DecryptedFile.txt", "w", encoding="utf-8") as dec\_file:**

**dec\_file.write(decrypted\_data)**

**print("Encryption & Decryption completed! Check 'EncryptedFile.txt' & 'DecryptedFile.txt'.")**

**except FileNotFoundError:**

**print("Error: File not found!")**

**print("1. Encrypt a text message")**

**print("2. Encrypt a file")**

**choice = input("Choose an option: ")**

**if choice == "1":**

**encrypt\_text()**

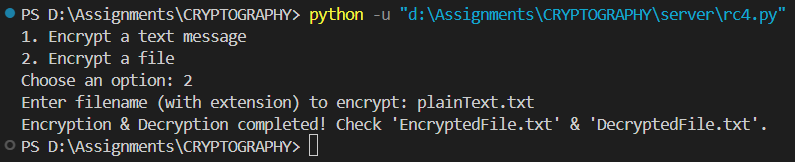
**elif choice == "2":**

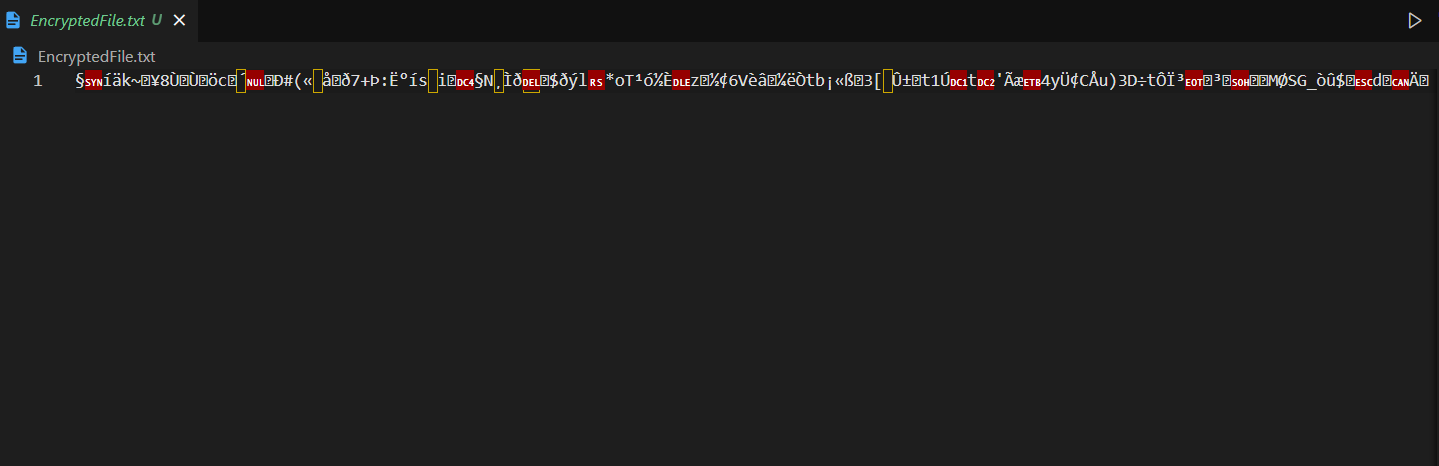
**encrypt\_file()**

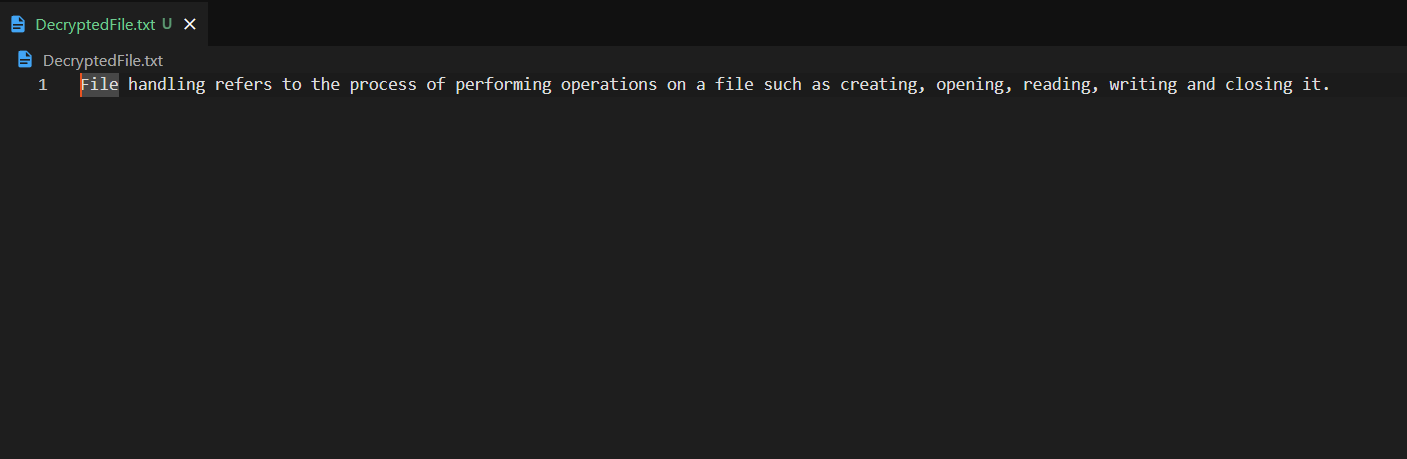
**else:**

**print("Invalid choice. Please select 1 or 2.")**

**Output:**

****

**EncryptedFile.txt:**

**DecryptedFile.txt:**

**Code Repository:**

[**https://github.com/pranav2885/crypto-lab**](https://github.com/pranav2885/crypto-lab)