Information Security Practical Assignment

Submitted to : Ms Upasna

Name : Kanish

Roll Number : CSC/21/53

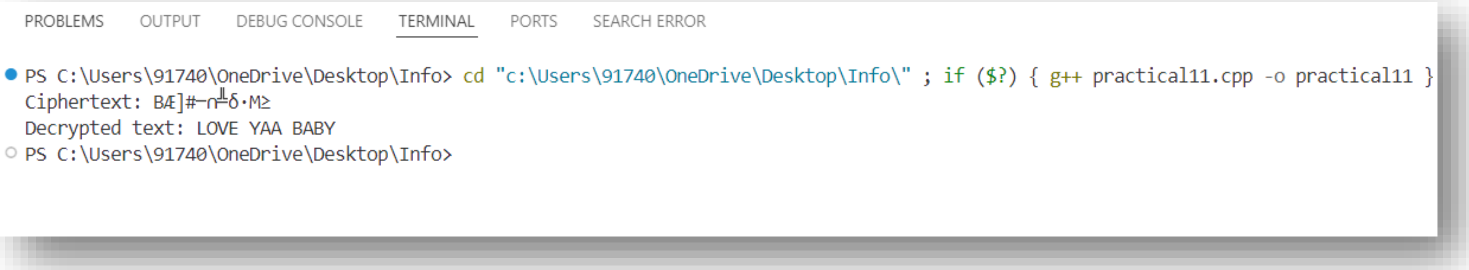
University Roll No: 21059570017

11. Implement a stream cipher technique.

Code:

```cpp
#include <iostream>
#include <vector>

// Initialize the RC4 state with a given key
void initializeRC4(std::vector<int>& S, const std::string& key) {
    int N = 256; // Size of the state vector
    for (int i = 0; i < N; ++i)
        S[i] = i;

    int j = 0;
    for (int i = 0; i < N; ++i) {
        j = (j + S[i] + key[i % key.length()]) % N;
        std::swap(S[i], S[j]);
    }
}

// Generate the next byte of the key stream
int generateKeyByte(std::vector<int>& S, int& i, int& j) {
    int N = 256;
    i = (i + 1) % N;
    j = (j + S[i]) % N;
    std::swap(S[i], S[j]);
    return S[(S[i] + S[j]) % N];
}

// Encrypt or decrypt data using the key stream
std::string streamCipher(const std::string& data, const std::string& key) {
    std::vector<int> S(256);
    initializeRC4(S, key);

    std::string result;
    int i = 0, j = 0;
    for (char c : data) {
        int keyByte = generateKeyByte(S, i, j);
        char encryptedChar = c ^ keyByte;
        result += encryptedChar;
    }
    return result;
}

int main() {
    std::string plaintext = "LOVE YAA BABY";
    std::string key = "MSINFOSECUPA"; // Replace with your own secret key

    std::string ciphertext = streamCipher(plaintext, key);
    std::cout << "Ciphertext: " << ciphertext << std::endl;

    // Decrypt the ciphertext (using the same key)
    std::string decryptedText = streamCipher(ciphertext, key);
    std::cout << "Decrypted text: " << decryptedText << std::endl;

    return 0;
}
```

Output:



```
● PS C:\Users\91740\OneDrive\Desktop\Info> cd "c:\Users\91740\OneDrive\Desktop\Info\" ; if ($?) { g++ practical11.cpp -o practical11 }
  Ciphertext: BÆ]#─n╨δ·M≥
  Decrypted text: LOVE YAA BABY
○ PS C:\Users\91740\OneDrive\Desktop\Info>
```