**Cryptography and Network Security Lab**

**Assignment No. 2**

**PRN: 2020BTECS00092**

**Name: Vishal Shrirang Madle**

**Batch: B8**

**Title:** Caesar Cipher Decryption (Cryptanalysis)

**Aim:** To implement Caesar Cipher Decryption using Console and file input for cryptanalysis.

**Theory:** In cryptography, a Caesar cypher, also known as Caesar's cypher, the shift cypher, Caesar's code or Caesar shift, is one of the simplest and most widely known encryption-decryption techniques. It is a type of substitution cypher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on.

**Procedure:** Dn(x)=(x-n+26)% 26(Decryption Phase where x is the input character and n is the given key)

· Traverse the given text one character at a time.

· For each character, transform the given character as per the rule and encrypt plain text using key. Return the new string generated.

**Code:**

**#include <iostream>**

**#include <fstream>**

**#include <string>**

**using namespace std;**

**string CaesarCipherDecryption(string ciphertext, int key)**

**{**

**string plaintext = "";**

**for (int i = 0; i < ciphertext.length(); i++)**

**{**

**plaintext += char(int(ciphertext[i] - key - 65 + 26) % 26 + 65);**

**}**

**return plaintext;**

**}**

**int main()**

**{**

**int Choice, key;**

**string input\_text;**

**cout << "-----Caesar Cipher Decryption-----\n";**

**cout << "Enter Choice:\n1) Console\n2) File\n";**

**cin >> Choice;**

**cout << "Enter key: ";**

**cin >> key;**

**switch (Choice)**

**{**

**case 1:**

**cout << "Enter cipher text: ";**

**cin >> input\_text;**

**break;**

**case 2:**

**{**

**ifstream inputFile("input.txt");**

**if (!inputFile)**

**{**

**cerr << "Error opening input file." << endl;**

**return 1;**

**}**

**getline(inputFile, input\_text);**

**inputFile.close();**

**}**

**break;**

**default:**

**cerr << "Invalid choice." << endl;**

**return 1;**

**}**

**string plaintext = CaesarCipherDecryption(input\_text, key);**

**// Print the decrypted text to the console**

**cout << "Decrypted Text: " << plaintext << endl;**

**// Open the "output.txt" file for writing decrypted text**

**ofstream outputFile("output.txt");**

**if (!outputFile)**

**{**

**cerr << "Error opening output file." << endl;**

**return 1;**

**}**

**// Write the decrypted text to the output file**

**outputFile << "Decrypted Text: " << plaintext << endl;**

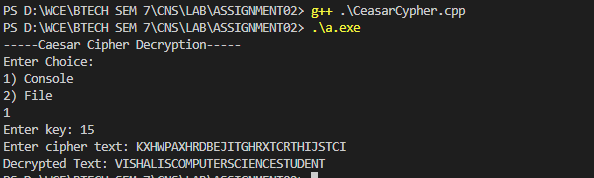
**// Close the output file**

**outputFile.close();**

**return 0;**

**}**

**Console Output**:



**Conclusion:** Caesar Cipher is simple substitution technique. It falls in category of monoalphabetic cipher where each character is substituted by addition of that character with given key. The key can be deciphered easily, thus makes it less secure.