**Name:** Karuna Bajirao Randive

**Prn:** 2020BTECS00024

**Batch:** B2

**Cryptography & Network Security Lab**

**Assignment No. 1**

**Theory:**

* Caesar Cipher, also known as the Shift Cipher, is one of the simplest and oldest encryption techniques used to secure information.
* It's a type of substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.
* The number of positions a letter is shifted is determined by a key.

**Encryption:**

**In Encryption, input is a Plain text and output is a Cipher text.**

Step 1: Choose a secret key (a positive integer).

Step 2: Take the plaintext message you want to encrypt.

Step 3: Shift each letter in the message forward in the alphabet by the key positions.

Step 4: Non-alphabetical characters remain unchanged.

Step 5: The result is the ciphertext, the encrypted message.

**Decryption:**

**In Decryption, input is a Cipher text and output is a Plain text.**

Step 1: Have the same key used for encryption.

Step 2: Take the ciphertext (the encrypted message).

Step 3: Shift each letter in the ciphertext backward in the alphabet by the key positions.

Step 4: Non-alphabetical characters remain unchanged.

Step 5: The result is the plaintext, the original message.

**Caesar Cipher:**

#include <iostream>

using namespace std;

string encrypt(string text, int s)

{

    string result = "";

    for (int i = 0; i < text.length(); i++) {

        if (isupper(text[i]))

            result += char(int(text[i] + s - 65) % 26 + 65);

        else

            result += char(int(text[i] + s - 97) % 26 + 97);

    }

    return result;

}

string decrypt(string text, int s)

{

    string result = "";

    for (int i = 0; i < text.length(); i++) {

        if (isupper(text[i]))

            result += char(int(text[i] - s - 65) % 26 + 65);

        else

            result += char(int(text[i] - s - 97) % 26 + 97);

    }

    return result;

}

int main()

{

    string text;

    cout << "Text : ";

    cin>>text;

    int s;

    cout << "\nShift: ";

    cin>>s;

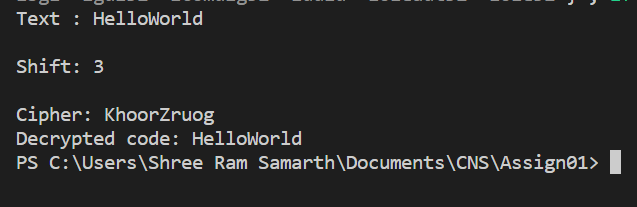
    string dec = encrypt(text, s);

    cout << "\nCipher: " << dec ;

    cout << "\nDecrypted code: " << decrypt(dec, s);

    return 0;

}

**Output:**

**Decryption of cipher text** **using nltk library:**

import nltk

nltk.download('words')

from nltk.corpus import words

def caesar\_decrypt(ciphertext, shift):

    decrypted\_text = ""

    for char in ciphertext:

        if char.isalpha():

            ascii\_offset = ord('a') if char.islower() else ord('A')

            decrypted\_char = chr((ord(char) - ascii\_offset - shift) % 26 + ascii\_offset)

            decrypted\_text += decrypted\_char

        else:

            decrypted\_text += char

    return decrypted\_text

def is\_meaningful\_word(word):

    return word.lower() in words.words()

def decrypt\_with\_meaningful\_text(ciphertext):

    for shift in range(26):

        decrypted\_text = caesar\_decrypt(ciphertext, shift)

        if all(is\_meaningful\_word(word) for word in decrypted\_text.split()):

            return decrypted\_text

encrypted\_text = "Ymjd hfs fyyfhp ymj uwjxnijsy"

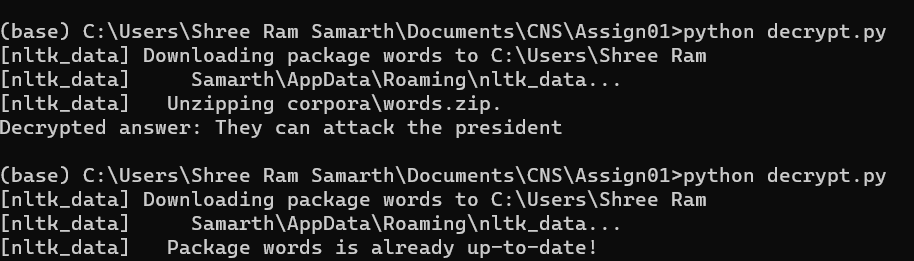
decrypted\_answer = decrypt\_with\_meaningful\_text(encrypted\_text)

if decrypted\_answer:

    print("Decrypted answer:", decrypted\_answer)

else:

    print("No valid decryption found.")

**Output:**