Roll No: 2103163
Batch: C32
Name: Om Shete

Experiment No 2

Aim: Implementation of Ceaser Cipher.

Description:

- The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”.
- The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is named after Julius Caesar, who used it to communicate with his officials.
- Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.
- The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.
- For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.
- Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:

1. Write down the plaintext message: HELLO
2. Choose a shift value. In this case, we will use a shift of 3.
3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

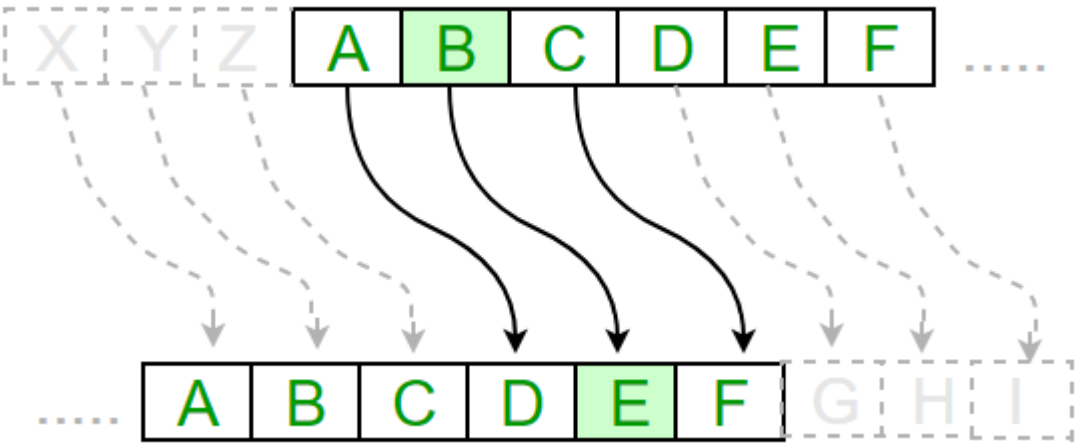
H becomes K (shift 3 from H)
E becomes H (shift 3 from E)
L becomes O (shift 3 from L)
L becomes O (shift 3 from L)
O becomes R (shift 3 from O)

4. The encrypted message is now “KHOOR”.

Roll No: 2103163
Batch: C32
Name: Om Shete
To decrypt the message, you simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “KHOOR” back by 3 positions to get the original message, “HELLO”.

$E_n(x)=(x+n) \mod 26$
(Encryption Phase with shift n)

$D_n(x)=(x-n) \mod 26$
(Decryption Phase with shift n)



Text: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Advantages:

1. Easy to implement and use thus, making suitable for beginners to learn about encryption.
2. Can be physically implemented, such as with a set of rotating disks or a set of cards, known as a scytale, which can be useful in certain situations.
3. Requires only a small set of pre-shared information.
4. Can be modified easily to create a more secure variant, such as by using multiple shift values or keywords.

Disadvantages:

1. It is not secure against modern decryption methods.
2. Vulnerable to known-plaintext attacks, where an attacker has access to both the encrypted and unencrypted versions of the same messages.

Roll No: 2103163
Batch: C32
Name: Om Shete

3. The small number of possible keys means that an attacker can easily try all possible keys until the correct one is found, making it vulnerable to a brute-force attack.

Code:

```
#include <cctype>
#include <iostream>
using namespace std;

string encrypt(const string &text, int shift) {
  string result = "";

  for (char ch : text) {
    if (isalpha(ch)) {
      char base = isupper(ch) ? 'A' : 'a';
      result += static_cast<char>((ch - base + shift) % 26 + base);
    } else {
      result += ch;
    }
  }
  return result;
}

int main() {
  string plaintext;
  int shift;

  cout << "Enter the text to encrypt: ";
  getline(cin, plaintext);

  cout << "Enter the shift value: ";
  cin >> shift;

  string ciphertext = encrypt(plaintext, shift);

  cout << "Encrypted text: " << ciphertext << endl;

  return 0;
}
```

Roll No: 2103163
Batch: C32
Name: Om Shete

Results:

```
Enter the text to encrypt: strength
Enter the shift value: 5
Encrypted text: xywjslym
```