**Objective:**

- To understand the concept of polymorphism in C++.

**Challenge** - **1:** Encryptor App                                        **(**15**)**

Imagine you are working as a cybersecurity engineer at a leading technology company, tasked with developing a secure messaging feature for a new communication platform. The platform aims to provide end-to-end encryption for messages exchanged between users to ensure confidentiality and privacy.

Your task is to design and implement a program that can encrypt and decrypt messages using various encryption algorithms. The program should include the following classes:

**Encryptor:** This is an abstract base class representing a generic encryption algorithm.

- virtual String encrypt(const String& message) const = 0;
- virtual String decrypt(const String& cipher) const = 0;

We are going to Discuss/Implement two Different cipher techniques named Cease Cipher and Vignere Cipher and going to develop a class for each of them.

| | |
|---|---|
| **CaesarCipher** | This class inherits from the Encryptor class. The Caesar cipher shifts each letter in the message by a fixed number of positions in the alphabet. |
| **Encryption Process:** | Each letter in the message will be replaced by the letter located a fixed number of positions forward in the alphabet. |
| | If the shift is 3, 'A' will be replaced by 'D', 'B' will be replaced by 'E',  if 'Z' it will round off to 'C', and so on. |
| **Example:** | "HELLO" encrypted with a Caesar Cipher with a shift of 3 becomes "KHOOR".<br>H Shifts to K   → H,I,J then K. H after shift of 3 becomes K. and so on. |
| **Decryption Process:** | To decrypt the message, we'll reverse the process by replacing each letter in the ciphertext with the letter located a fixed number of positions backward in the alphabet. |
| **Example:** | "KHOOR" decrypted with a Caesar Cipher with a shift of 3 becomes |

| | "HELLO".<br>K Shifts back to H → K,J,I then H. K after shift of 3 becomes H. and so on. |
|---|---|

| **VigenereCipher** | This class inherits from the Encryptor class. |
|---|---|
| **Encryption Process:** | Vigenere Cipher is a method of encrypting alphabetic text by using a keyword and a repeating sequence of different Caesar ciphers. |
| **Example:** | Let's say we have the keyword "KEY" and the plaintext "HELLO". We align the keyword with the plaintext: |

| **Plaintext:** | H | E | L | L | O |
|---|---|---|---|---|---|

| **Keyword:** | K | E | Y | K | E |
|---|---|---|---|---|---|
| **Shift Value:** | 10 | 4 | 24 | 10 | 4 |

e.g. A has a shift value of 0. B has a shift value of 1 and so on.
If a keyword is shorter than the plain text it will repeat itself.

| H | is shifted by 10 positions (K) | R |
|---|---|---|
| E | is shifted by 4 positions (E) | I |
| L | is shifted by 24 positions (Y) | J |
| L | is shifted by 10 positions (K) | V |
| O | is shifted by 4 positions (E) | S |

So, the resulting ciphertext is "RIJVS".

| **Decryption Process:** | Decryption in Vigenere Cipher involves using the same keyword to reverse the encryption process. Each letter in the ciphertext is shifted back according to the corresponding letter in the keyword to reveal the original plaintext. |
|---|---|

| **Example:** | Now we have the keyword "KEY" we'll decrypt the word "RIJVS" |
|---|---|

| **Encrypted Text:** | R | I | J | V | S |
|---|---|---|---|---|---|

| **Keyword:** | K | E | Y | K | E |
|---|---|---|---|---|---|
| **Shift Value:** | 10 | 4 | 24 | 10 | 4 |

If a keyword is shorter than the plain text it will repeat itself.

| R | is shifted back by 10 positions (K) | H |
|---|---|---|
| I | is shifted back by 4 positions (E) | E |
| J | is shifted back by 24 positions (Y) | L |
| V | is shifted back by 10 positions (K) | L |
| S | is shifted back by 4 positions (E) | O |

So, the resulting decrypted text is "HELLO".

| **Encryptor** |
|---|
| ```
class Encryptor
{
public:
    virtual String encrypt(const String& message) const = 0;
    virtual String decrypt(const String& cipher) const = 0;
};
``` |

| **CaesarCipher** | **VigenereCipher** |
|---|---|
| ```
class CaesarCipher : public Encryptor
{
private:
``` | ```
class VigenereCipher : public Encryptor
{
private:
``` |

```
    int shift;

public:
CaesarCipher(int shift);
    void setShift(int newShift);
    String encrypt(const String& message)
const override;
    String decrypt(const String& message)
const override;
};
```

```
    String keyword;

public:
VigenereCipher(const String& keyword);
    void setKeyword(const String&newKeyword);
    String encrypt(const String& message) const
override;
    String decrypt(const String& message) const
override;
};
```