Assignment 8—Cryptography

Due date

May 1, 2015 at 1pm

Objectives

- Create base classes and derived classes
- Allocate dynamic memory
- Work with pointers

Encryption

Encrypting messages is one of the ways people and organizations can exchange information without allowing a third party to intercept and interpret them.

Background

The cryptography algorithm we will use is called a Caesar cipher. The algorithm replaces each letter in a message with a letter further along in the alphabet. A Caesar cipher shifts the alphabet and is therefore also called a shift cipher. The encryption key is the number of letters you shift.

Caesar cipher is one of the oldest types of ciphers. It is named after Julius Caesar, who is said to have used it to send messages to his generals over 2,000 years ago.

So, cryptology has existed for more than 2000 years. But, what is cryptology? The word cryptology is derived from two Greek words: kryptos, which means “hidden or secret,” and logos, which means, “description.” Cryptology means secret speech or communication.

ROT13

The special case of the Caesar cipher we will use is called ROT13, or rotate by 13 places.

We can implement the letter shift with a lookup table of plain text characters to shifted characters. So when we find an `A` in the plain text, we replace it with an `N`. A plain text `B` is replaced with an `O` and so on.

Wikipedia has a full example of the lookup table.

Cipher

Create a base class called `Cipher` that contains two methods with the following signatures:

- `string encrypt(string text)`
- `string decrypt(string text)`

The method implementations for this class will not perform any actual encryption. They will simply pass through the plain text unaltered. This isn’t a very useful form of encryption!

Rot13

Create a class derived from `Cipher` called `Rot13`. Override `encrypt` and`decrypt` to implement the ROT13 algorithm described above.

Functions

Create two functions with the following signatures:

- `string decrypt_with(Cipher *cipher, string text)`
- `string encrypt_with(Cipher *cipher, string text)`

These functions accept a `Cipher` object to perform the encryption and a string of text to either encrypt or decrypt.

Main

The `main` function must:

- Allocate a `Rot13` object from the heap.
- Create a sample message text of “The quick brown fox jumped over the lazy dog”
- Call `encrypt_with` to encrypt the message.
- Call `decrypt_with` with the encrypted text to translate it back to plain text.
- Print both the encrypted and decrypted strings.

Output

The output of the program must match this text:

```
encrypted: Gur dhvpx oebja sbk whzcrq bire gur ynml qbt
decrypted: The quick brown fox jumped over the lazy dog
```

Extra credit

For 25 extra points, use AES, a real encryption algorithm, to encrypt and decrypt text. Write an `AES` class, derived from the `Cipher` base class, that accepts a secret encryption key in its constructor. The `encrypt` and`decrypt` method implementations will use the key and the AES algorithm to encrypt the message passed into the method.

The most popular C++ encryption library is OpenSSL. It’s likely already installed on your computer. Determine the best way to include the header files and call the library functions to perform the encryption.

Assignment details

- The name of the file must be called `Crypto.cc`.
- Comments at the top of your program
  - Your name
  - Date
  - Assignment #8
- Brief description of the assignment (one or two lines max).
- Comments throughout the program explaining what it is doing.
- The output must match exactly to the examples provided.
- The name and data types of the classes, methods, functions, parameters, and return values must be exactly as specified.
- Program must be written in C++ and submitted in Moodle.
- Code that does not compile will receive zero points for the assignment.
- Zip the Crypto.cc and submit to Moodle as Firstname_Lastname_HW8.zip.
-