cryptography

## Securing Communications

Taimoor Ul Islam (14031)

Dated: 06/02/2003

Fundamental of Programming (LAB)

Major Assignment By:

# CRYPTOGRAPHY

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The term is derived from the Greek word kryptos, which means hidden.

# PROGRAM

#include <iostream>

using namespace std;

## // Function to encrypt message

string encrypt(string key, string msg)

{

string code = "";

int i = 0, j = 0;

while (msg[i] != '\0')

{

code += char(int(msg[i]) + int(key[j]) - 62);

// Display operation in iteration for understanding

// cout << code << " = " << msg[i] << " + " << key[j] << " - 62" << endl;

i++;

j++;

if (key[j] == '\0')

{

j = 0;

}

}

return code;

}

## // Function to decrypt message

string decrypt(string key, string code)

{

string msg = "";

int i = 0, j = 0;

while (code[i] != '\0')

{

msg += char(int(code[i]) - int(key[j]) + 62);

// Display operation in iteration for understanding

// cout << msg << " = " << code[i] << " - " << key[j] << " + 62" << endl;

i++;

j++;

if (key[j] == '\0')

{

j = 0;

}

}

return msg;

}

## // Main function for testing encrypt and decrypt functions

main()

{

string Emsg, Ekey, code, Dkey, Dmsg;

cout << "Enter a message to encrypt: ";

getline(cin, Emsg);

cout << "Now enter an ecryption key: ";

getline(cin, Ekey);

code = encrypt(Ekey, Emsg);

cout << "Your message is encrypted sucessfully. \nYour encoded message is: " << code << endl;

cout << "Enter your secret key to decrypt: ";

getline(cin, Dkey);

Dmsg = decrypt(Dkey, code);

cout << "Your message is decrypted sucessfully. \nYour decoded message is: " << Dmsg << endl;

}

# EXPLANATION OF PROGRAM

In this program we will encrypt a message through a secret key to an encoded message or code which will make no sense when read. After that we will use the same key to decrypt that encoded message to a readable form.

In this program we will use and define two functions. One will be used for encryption of a readable message and the other will be use for the decryption of encoded message. After defining encryption and decryption we will use main function to call both encryption and decryption functions and test them by passing actual parameters.

# FUNCTION FOR ENCRYPTION

In our code first we declare the encryption function. In declaration we say that there is a function named encrypt which will take two string value as a parameter, one as a key and other as a message. After that it will perform some operation between them and return a third value with string data type which will be code (encoded message).

Now after declaration we have define the body of our function that what operation our function will perform between the key and msg (message) to return the string code (encoded message).

In the function body first we declare a string name code and initialize it to empty string. In this string we will store that encoded message.

Now to get the first character of the code we will add the first character of the string message with the first character of the string key and result will be add to our empty string code. Just like we do addition of the first characters of message and key to get the first character of our code we will add all of the characters of message with its corresponding character in string key to get all of the characters of our encoded message. The number of characters in code will be equal to the number of character of the message because our code is our message but with the addition of characters of key. Which means we can get or readable message simply by subtracting corresponding characters of key from our encoded message.

Now let move toward our actual code. We use while loop to perform the addition operation between key and message. We have declare two variables i and j. variable I is to control the loop and will represent the index position of the characters of string message. It means for in every iteration i will be incriminated and will represent the next character in the string message. On the last character of the string message, i will be incriminated and the character on that of that index position will be null mean empty and the loop will terminate because we have put the terminating condition to the while loop that terminate when the character at the i index position in the string message i becomes null. The variable j will represent the characters of the string key.

Inside while loop we are adding the integer values which represent the characters of the message and key in the asci table and subtracting 62 from it and then again converting it to the data type char and storing it in the string code.

In first iteration of the loop the variable I and j will be zero thus character in the string message at index position zero (its integer value) will be added with the character in the string key at the index position zero (its integer value) and 62 will be subtracted from it. The result will be again converted to char data type and will be added in the empty string code.

The number of characters in string message and string key may not be equal. Here we assume that the character of the key will be less than the characters in the string message so after addition and incrimination of I and j, we put an if condition that if character on index position j in string key I is null means if all of the character are added for so then again initialize j to zero means again start adding from the index position zero of the string key.

The while loop will iterate until all of the characters of the string message are finished and at the same time the empty string code will be full by the characters which will be the result of the addition of characters of message and key.

# FUNCTION FOR DECRYPTION

After defining encryption function we have define decryption function in the code.

In declaration of the decrypt function we have declare that our function has name decrypt while will take two parameters with string data type one as key and other as code or encoded message and will return a third string as a readable message.

In body we have declare a string msg and initialize it as empty string in which will we store the message.

All of the working of the decrypt function is same as that of the encrypt function. We use while loop to perform subtraction of key form encoded message and store it into the empty string message.

As we know that characters of code are characters of message but the addition of character of key and subtraction of 62.

So to get our readable message back we will reverse the process and in each iteration of the loop will subtract the character of the key and add 62 with the code and add it to the empty string message.

The process wil continue till we got our readable message back.

At the end we return the message.

# MAIN FUNCTION FOR TESTING

In main function we declare necessary variable and get them as input from user but rather that using simple cin we use another building function getline which will allow us to accept inputs with empty spaces.

Then we call encrypt function and store return value in variable code.

After that again we take key from user and pass the code and key to decrypt function and store value in message and them display that massage which was same as the message user enter for the first time for encryption and was passed through encrypt function.