Course Project Documentation

CS101 Project

DES and AES

Team Id – 123

Anmol Yadav – 140010018

Puneet Mahajan – 140010013

Akhilesh Vyas – 14D110013

Sarthak Mittal – 14D170018

Table of Contents

1.Introduction :

In today’s world, data security has become a major concern. There are worldwide news about information being leaked from various sites and security systems.

The password based systems are the most commonly used system due to its simplicity and applicability. But these types of systems have higher sensitivity to cyber-attack. Most of the advanced methods for authentication based on password security encrypt the contents of password before storing or transmitting in the physical domain. But all conventional encryption methods are having its own limitations, either in terms of complexity or in terms of efficiency.

Apart from the passcodes, encryption can be used to store the entire files secret even if a person gets access to it. While Encrypting Cipher Cryptography converts plain text into cypher text using a key, and reverse while decrypting. Plain text is what input is given by user and the cipher text we get as output cannot be understood by any person, thus keeping the information secret. The cipher text can be re-converted into the same plain text as the input by using the same key that was given while giving input, which will be only known to the person responsible for encrypting the text/document/files/images.

2. Problem Statement:

The aim of the project is to make Cipher Encrypter and Decrypter.

In module one of the project we will be using DES (data encryption standard) algorithm.

In module two of the project we will be using AES (advanced encryption standard) algorithm.

Also we will make a user friendly interface.

3.Requirements:

Software requirements:
1. C++ / Codeblocks – To run the program.

2. Qt – For Graphics.

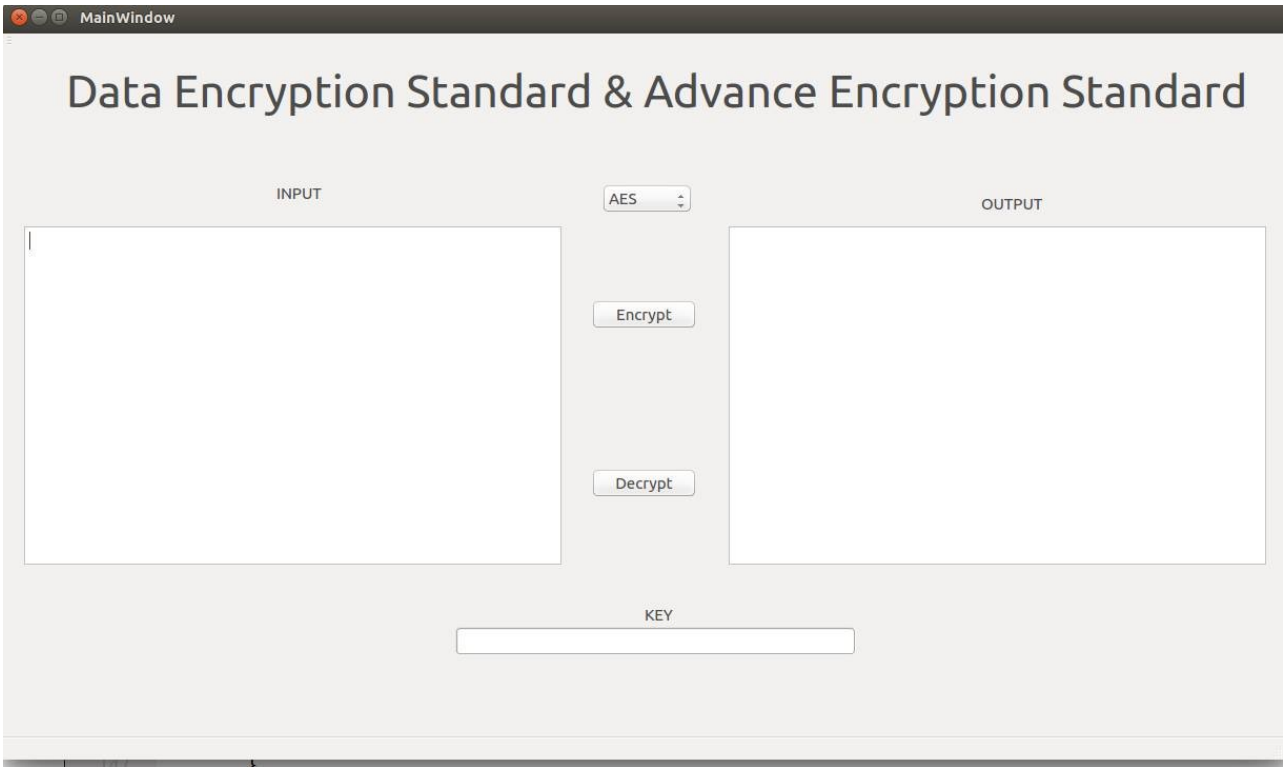
4.Implementation:

Functionality:

As we run the program a window appears which gives a dialogue box for entering Input, Key , a dialogue box for output and there is a dropdown window to choose whether they want to encrypt using DES or AES. There is a button for “Encrypt” which the user needs to press in order to get the cipher text in a dialogue box given where encrypted code is to be shown. The user may then copy paste and save the text in his system (saving the text is not the part of project) , while decrypting the user needs to put the encrypted text in the plain text box , enter the same key he/she used to encrypt the text and press the “Decrypt” button available on the window, and the plain text will b shown in the cipher text box.

It is upto the user that how many he wants to encrypt the text, whether to change the key everytime he/she encrypts the text and get the final output, but the user then has to remember all the keys and while decrypting use the keys in exact reverse order.

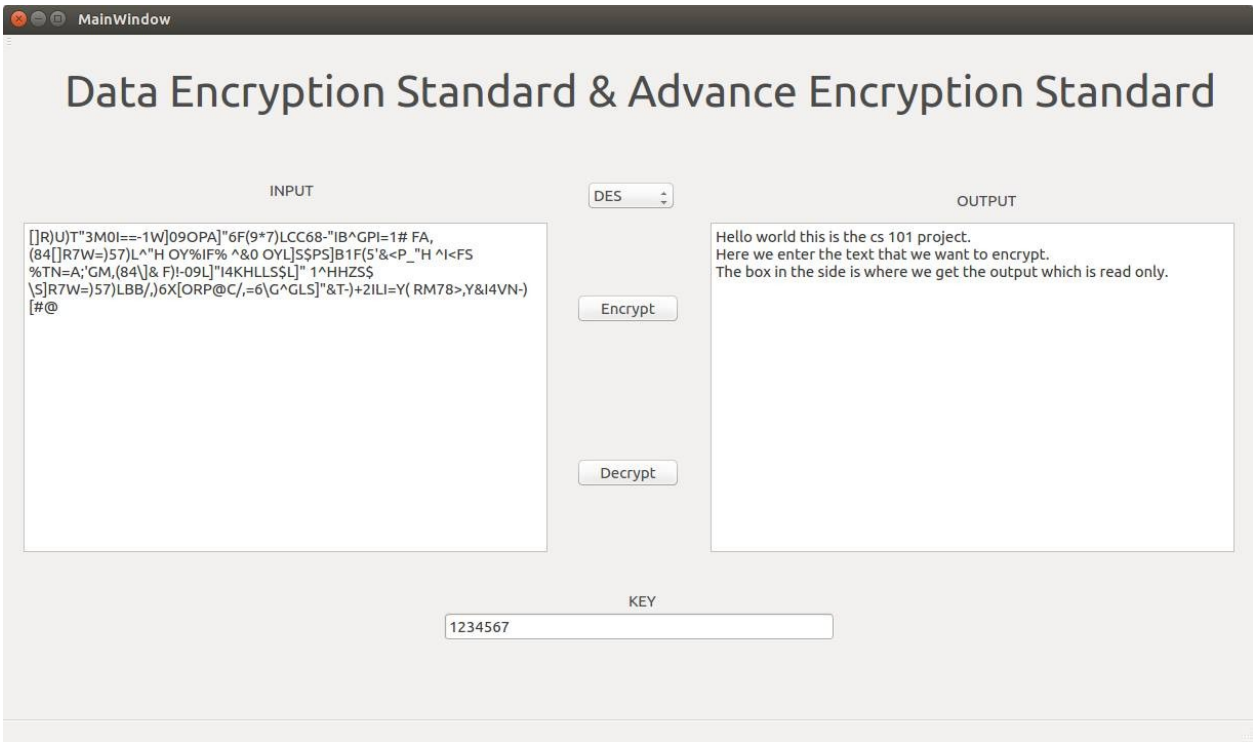
5.Testing Data and Strategy



This is the main input window from which the user interact...the message is to be given in the input window and the type of encryption is to be selected from the

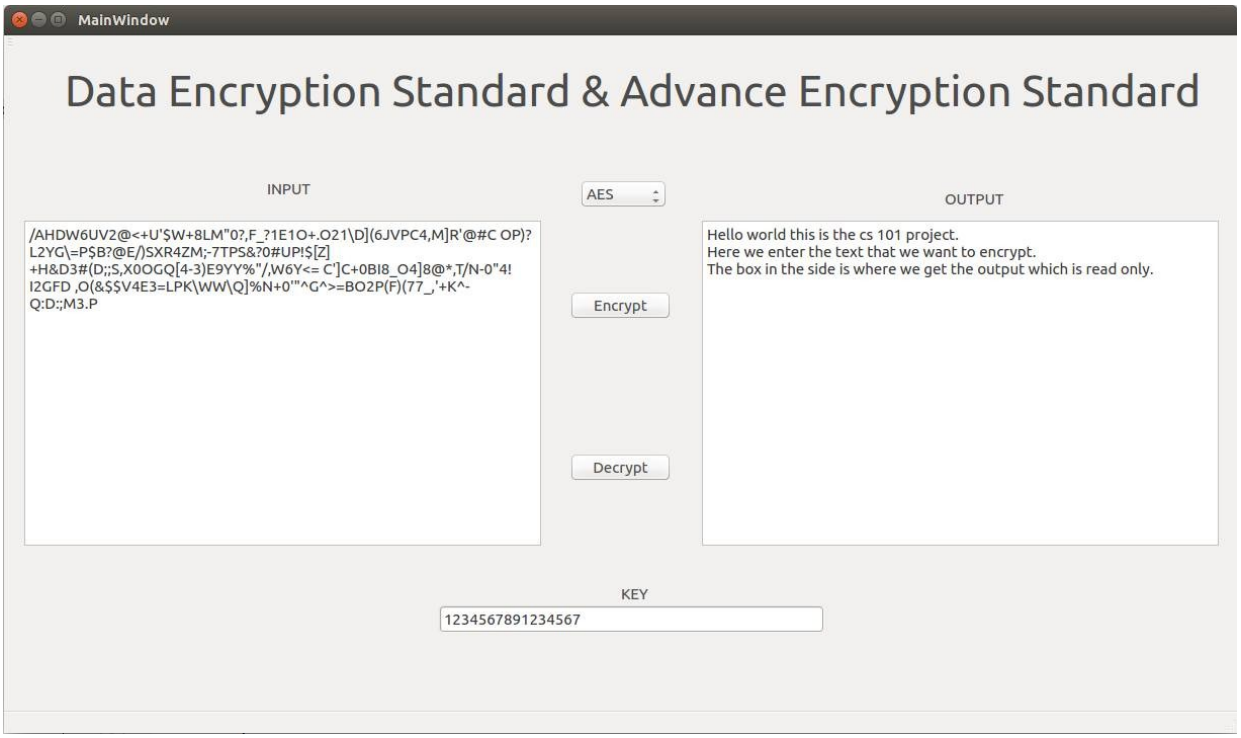
down menu as shown below.

The DES key input is of max 7 character. Input could be of any length after dese two things are given clicking on encrypt button gives the output which is the encrypted text



Now taking the same output as input with the same key using the decrypt button the original text could be retrieved

Now the same thing is done with the AES. Here the max key length is 16 characters. Giving the input with the key using encrypt key the output is obtained.



Copying the output and giving it as an input with the same key using decrypt key gives the original text back.

6. Discussion of Program:

A. What worked as per the plan?
DES (Data Encryption Standard) – The Encryption and Decryption algorithm of DES is standard, was taken from a reference mentioned below and was implemented exactly in the program. We used vectors to store the input and performed various functions as per algorithm with them.

AES (Advanced Encryption Standard) – The algorithm was taken from the source and implemented properly. We used matrices to store the input and performed the row/ column exchanges and other functions to implement the program.

B. What we added more than discussed in SRS?
As the project was based on just encryption and decryption of text, we were not thinking of adding graphics in the program and were going to use the terminal window to use the software. But to create user friendly interface and take the project as an opportunity to explore and use different compliers and libraries, we added graphics.

C. Changes made in the plan:
Adding graphics using Qt was the only change made in the plan.

.

7. Future Work:

As it was used for security purposes (keeping data secret, etc.), future applications just include making the algorithm more difficult to crack, currently both AES and DES are cracked. The user can input multiple keys making the code more strong. We can have multiple encryptions.

Like double DES, triple DES. We thought of a code that will permute the data in random number of times the value of which will be stored in the encrypted code(From both AES and DES) , and same number of times of permutation will be read and used to decrypt. We can do the step by step encryption (AES followed by DES, etc.).

In the project we have encrypted and decrypted texts, but this can also be used to encrypt and decrypt files/documents/images etc.

8.Conclusion:

In this project DES and AES has been presented. The key features of the program is that the user can use it to encrypt and decrypt a text as many number of times as he wishes making it more secure. With detailed study in this chapter we can increase the level of security and put our contributions to minimize cyber crime.

9. Reference:

1. Global Journal of Computer Science and Technology - Network, Web & Security, Volume 13 Issue 15 Version 1.0 Year 2013
2. A VHDL Implementation of the Advanced Encryption Standard-Rijndael Algorithm by Rajender Manteena
3. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
4. http://en.wikipedia.org/wiki/Data_Encryption_Standard
5. http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard
6. https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf
7. http://aesencryption.net/ - AES encryption