VISUAL EXECUTIVE METHODS

NUR SYAFIQA BINTI ISMAIL

FACULTY OF COMPUTER SYSTEMS AND SOFTWARE ENGINEERING

2014

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF DIAGRAMS

LIST OF ABBREVIATION

VECCMIA - Visual Execution Of Caesar Cipher Methods And Its Application

OOMLCM - Object Oriented Methodology Life Cycle Model

AES - Advanced Encryption Standard

DES - Data Encryption Standard

3DES - Triple Data Encryption Standard

RC4 - Ron's Code 4

RSA - Rivest, Shamir, and Adelman

e.g - For example

ABSTRAK

Visual Pelaksanaan Kaedah Caesar Cipher Dan Perlaksanaan dibangunkan untuk pemula mempelajari proses asas penyulitan dan memeriksa apa yang sebenarnya berlaku semasa proses penyulitan dan penyahsulitan secara visualisasi. Kebanyakan alat kriptografi dibangunkan dan wejud dalam maya yang hanya dapat menyulitkan dan menyahsulit data tanpa menjelaskan bagaimana proses berlaku. Kaedah yang digunakan untuk melaksanakan projek ini adalah Berorientasikan Objek Model Cycle. Projek ini dapat menyumbang kepada pemahaman logik dan untuk memastikan pemula dapat menggunakan teori dalam persekitaran yang sebenar. Perkara utama yang dipertimbangkan dalam program ini adalah penjelasan sebagai pengenalan tentang Caesar Cipher terus ke pelajaran seterusnya. Program ini dibahagikan kepada tiga fasa yang berjujukan untuk setiap tulisan rahsia. Fasa pertama adalah penjelasan ringkas mengenai tulisan rahsia dan bagaimana ia berfungsi. Penjelasannya ialah menyampaikan dalam bentuk kata-kata penjelasan. Fasa kedua adalah demo bagaimana cipher disulitkan dan dinyahsulit. Fasa terakhir perlu sama sekali interaksi pengguna dengan aplikasi yang mana pengguna perlu memasukkan teks biasa, masukkan kunci, melaksana dan keluar. Proses ini dipersembahkan dengan menggunakan pelaksanaan visualisasi. Program ini juga menitikberatkan mengenai antara muka. Antara muka yang mudah difahami memegang dua panel khusus untuk menulis atau tampal teks untuk penyulitan atau penyahsulitan, dan panel yang lain untuk melihat konsep pelaksanaan adalah melaksanakan. Selain itu, butang untuk mula, berhenti, sebelum ini dan seterusnya juga disediakan untuk memastikan pengguna boleh menggunakan aplikasi dengan mudah. Hal ini dapat membantu pengguna dengan mudah melakukan memahami konsep dengan baik. Selain daripada itu, program ini juga menyediakan panel "brute force" untuk melihat senarai "brute force" bagi setiap kunci. Cipher yg digunakan untuk program ini adalah kaedah Caesar Cipher.

ABSTARCT

Visual Execution Of Caesar Cipher Methods And Its Application is developed for beginner to learn basic encryption process and inspect what is actually happen during encryption and decryption process in visualization approach. Most of cryptography tools developed and provide in the net is only able to encrypt and decrypt the data without explaining how do the process take place. The methodology used to implement this project is based on the Object Oriented Cycle Model. This project can contribute on logical understanding and to ensure beginner able to applied the theory in a real environment. The important things considered in this program is explanation as an introduction about the Cipher chosen before continue to next lesson. This program is divided into three sequential phase for each cipher. The first phase is briefly explanation about the cipher and how it work. The explanation is deliver in form of wording explanation. Second phase is demo on how the cipher is encrypted and decrypted. The last phase need totally user interaction with the application where the user need to enter the plaintext, enter the key, execute and exit. The process is presented by using visualization execution. This program also considered more about the interface. Simple interface which holds two panels dedicated to write or paste the text for encryption or decryption, and the other panel for viewing execution concept is implement. Besides that, button for play, pause, stop, next, previous and end also provided to ensure user can use the application easily. This can help user easily do understand the concept well. Other than that, this program also provide brute force attack panel to view brute force list for each keys. The cipher covered for this program is Caesar Cipher methods.

CHAPTER 1

INTRODUCTION

1.0 Introduction

Cryptography is message-utilizing an algorithms in order to keeps unnoticeable until the code is decrypted. To perform decrypt an encrypted message mostly involves a lot of specific code, or maybe in new age, the use of a special computer software. [1]. The project is carried out to develop visual tutorial of data encryption methods. The encryption is focus on one basic cipher called Caesar Cipher. As a student majoring in computer system and networking, it is important to have basic knowledge of encryption and decryption methods. Alternatively, encryption and decryption methods or as known as cryptography is widely used in computer network communication. Cryptography is especially important in wireless communications. Using collection of articles and journals, related to this project development and the strong concept of basic cryptography methods and algorithms which is Caesar Cipher, this project is carried out. This project also can be used for future enhancement of new cryptography methods. This project will guide from the preliminary study to the development this application until maintenance and testing.

1.1 Problem Statement

1.1.1 Issues for proposing the ideas

Confidential details needs to be protected and it is important to learn and understand how to encrypt any message or data. The easiest method to protect data on computer networks is by using encryption software. These programs provide full use of algorithms and methods to secure information. Password-protected data can merely be observed when it is decrypted[1]. But in order to use the software that already developed, it is important to understand first and be able to applied the theory and concept.

Most of cryptography tools developed and provide in the net is only able to encrypt and decrypt the data without explaining how do the process take place. Based on experience, beginner not able to understand well about the process and simply used the freeware software available to do encryption. This may lead them to not be able applied the theory on the real situation. At first they may not face any problem yet, but later to do physically and logically process of encrypt and decrypt the may have some. Even though there is simulator for encryption provided in internet, but most of them is very difficult to understand because of no explanations provided and need expertise to explain it very well before use it.

Besides that, most of the security subjects offered and provided in most universities only considering theories and concept. This may contribute on logical understanding and student not able to applied the theory in a real environment. Same goes to beginner in this field, they may face a problem on strongly understanding the process and algorithms used in cryptography. This project is carried out to develop a visual tutoring for data encryption and decryption of Caesar Cipher methods and algorithms to overcome this matter.

1.1.2 Importance of cryptography understanding

The importance of cryptography knowledge is about the message confidentiality which is prevent from message being disclosed to unauthorized users or parties. Message is disclosed to authorized and to the intended parties who have rights for that message only. Integrity also is important to provide no modification to the message being received. This is to ensure that message did not modify when sending from sender to receiver.

To secure data, encryption uses mathematic functions known as cryptography algorithms or known as ciphers, some example of well known and trusted cryptography algorithms are AES, Blowfish, Twofish and Serpent, these ciphers can be subcategorized with a number indicating its strength in bits[3]. The more mathematical strength the encryption algorithm has the more difficult it will be to crack it without access to the key but a strong cipher normally requires more computational power[3].

As a beginner, it is very important to have a strong understanding about each types of cryptography methods and analysis. As everyone know, when choosing an encryption algorithm in security, many factor need to be considered.

1.2 Objectives

The goals of this project is to develop an application for cryptography methods learning aids. The following objectives are set :

i. To develop a program about Caesar Cipher cryptography methods for beginner.
ii. To inspect what is actually happen during encryption and decryption of Caesar Cipher process for beginner understanding.
iii. To help beginner able to understand Caesar Cipher cryptography processes and algorithms using wording tutorial and visualization approaches.

1.3 Scopes

The scopes of this project are :

i. Focus Caesar Cipher encryption and decryption methods.
ii. Develop for beginners in security field.
iii. Design for windows user only.

1.4 Thesis Organization

This report consist of six (6) chapters. Chapter 1 will discuss on introduction to the whole idea of project including problem statement, objectives and scopes of the project. For Chapter 2 will explain about the literature review of this project. It will discuss about importance's of encryption and decryption in computer networking, type of cryptography in each asymmetric and symmetric methods and the theories and concepts of cryptography. The overall methods for the project will discuss and identify in Chapter 3. The analysis and ideas that needs to be include in the project are introduction on how the project has been conducted, project methodology, algorithms, methodology selection justification and software and hardware necessity. Project implementation and all the processes that involve in the development of the project will explained in Chapter 4. It is also explaining the method that involve in the development and how it is developed, either using source code or other tools should be included. Chapter 5 will explain about the results and the discussion. This chapter will explain the results and data analysis that had been acquired and this chapter must include result analysis, project limitation and suggestion and project enhancement. The conclusion of the developed project and summarization will stated in Chapter 6.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

This chapter is discussing about the literature review of the project that will be carried out which is visual execution for cryptography methods focused on Caesar Cipher. There are three subtopic involve in this chapter. First subtopic is basic vocabulary of encryption and decryption. Second is the comparison between several cryptography tools and simulation also will explained. Lastly, the overall project will discussed briefly. This project is carried out as a learning tools that may help beginner to understands the process of encryption and decryption of Caesar Cipher very well and enjoyable.

Block Cipher	Processes a block of input data at a time and produces a cipher text block of the same size.
Stream Cipher	A stream cipher encrypts data on the fly, usually one byte at time.
Cryptanalysis	Breaking the code.
Brute-Force Attack	Try every possible key on a piece of cipher text until an intelligible translation into plaintext is obtained.
Key Space	The total number of all possible keys that can be used in a cryptographic system.
Cryptology	Cryptography and cryptanalysis together constitute the area of cryptology.

Table 2.1 : Basic terminologies of encryption and decryption[6]

2.2 Existing Tools

2.2.1 Cryptographic Encryptor

Cryptographic Encryptor is a tools that used to simplifies the entire process of encrypting and decrypting text. The main window interface is dedicated to writing and pasting the text for encryption or decryption, and for viewing results.

Cryptographic Encryptor makes use of the most advanced encrypting algorithms, such as DES, Triple DES, AES-192, AES-128, RC2, RC4 and AES-256 and works on different version of Windows, including Vista and 7, Windows 2000 and 2003 Server, XP, 2008 Server, both 32 y 64 bit editions.

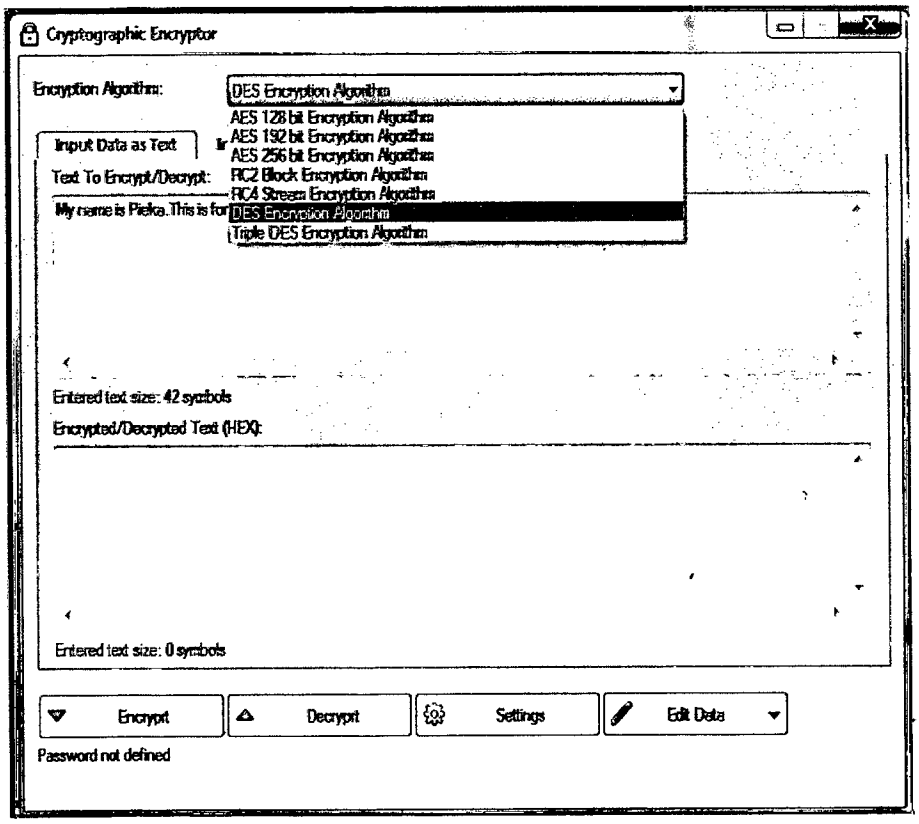

Figure 2.1 : Overall interface and list of algorithm provided in Cryptographic Encryptor

Cryptographic Encryptor contains a wide range of encryption algorithms to choose. It supports hotkeys for various commands for example swap files or text, clear entered data and can disable password confirmation.

In addition, users may pick the default algorithm and source or input data as text or file, UI language, visual style, style of tab sheet and tabs location, as well as establish a name pattern for encrypted and decrypted files. Options can be restored to their default values. User will prompted to enter key, which will be later required for decryption.

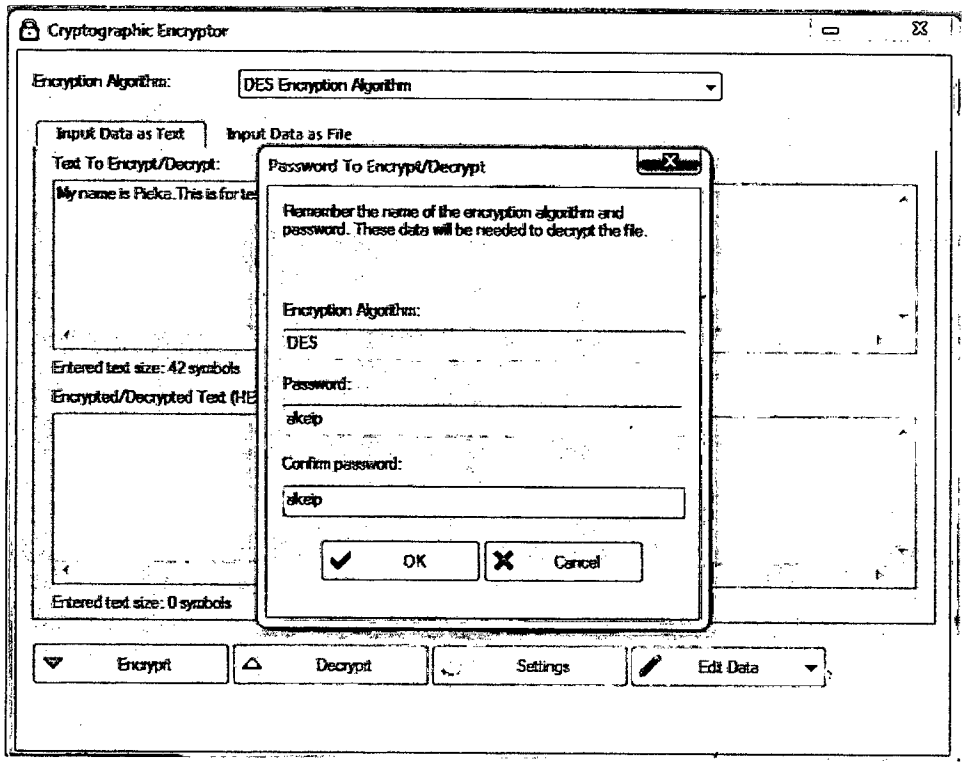

Figure 2.2 : Passkey is required to decryption process

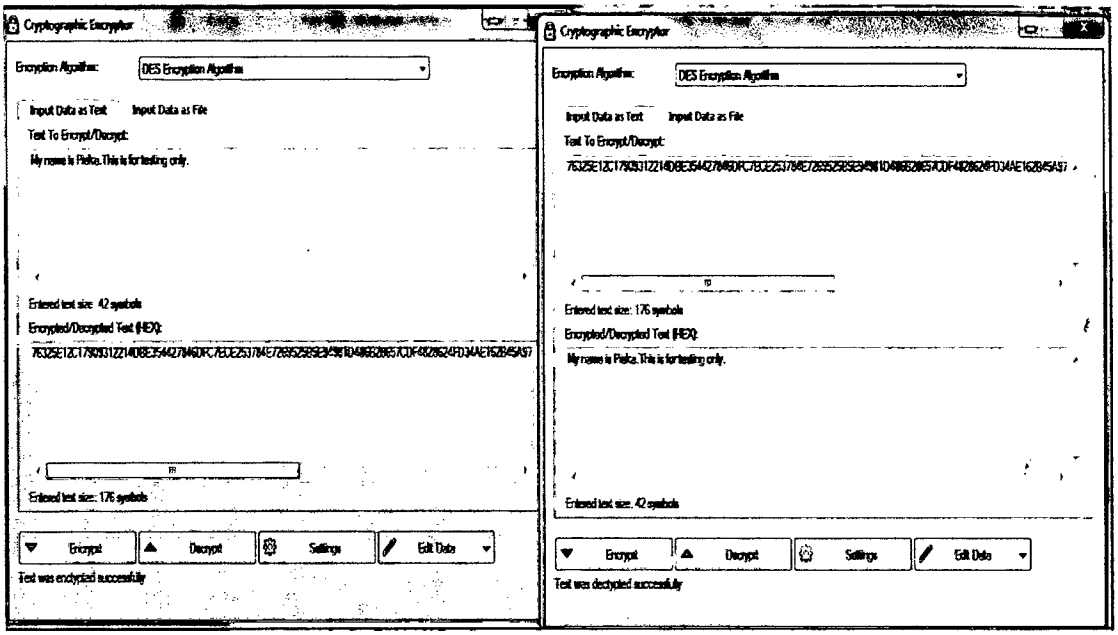

Figure 2.3 : The example of encryption and decryption process by using DES encryption algorithm

Characteristic :

- Easy to do encryption and decryption.
- Simple interface which holds two panels dedicated to write or paste the text for encryption or decryption, and for viewing results, respectively.
- Support for windows
- Provide DES, Triple DES, AES-192, AES-128, RC2, RC4 and AES-256 algorithms.
- Have two options, can enter text data or import file to be execute.
- Only focus on symmetric encryptions methods only.
- The process on how do the algorithm works do not stated.
- Easy to use but impossible to understand the concept for beginners.
- No simulation on encryption and decryption process.

2.2.2 CrypTool 1.4.31 Beta 6b

CrypTool is an open-source e-learning application which is used in the implementation and analysis of cryptographic algorithms. It supports both contemporary teaching methods at schools and universities as well as awareness training for employees and civil servants.[4]

This version requires a Win32 environment. The program contains some functions calling Java applications. To run these functions a Java runtime environment under Win32 (at least JRE 1.6) needs to be installed. CrypTool is available in English, German, Spanish, Polish and Serbian.

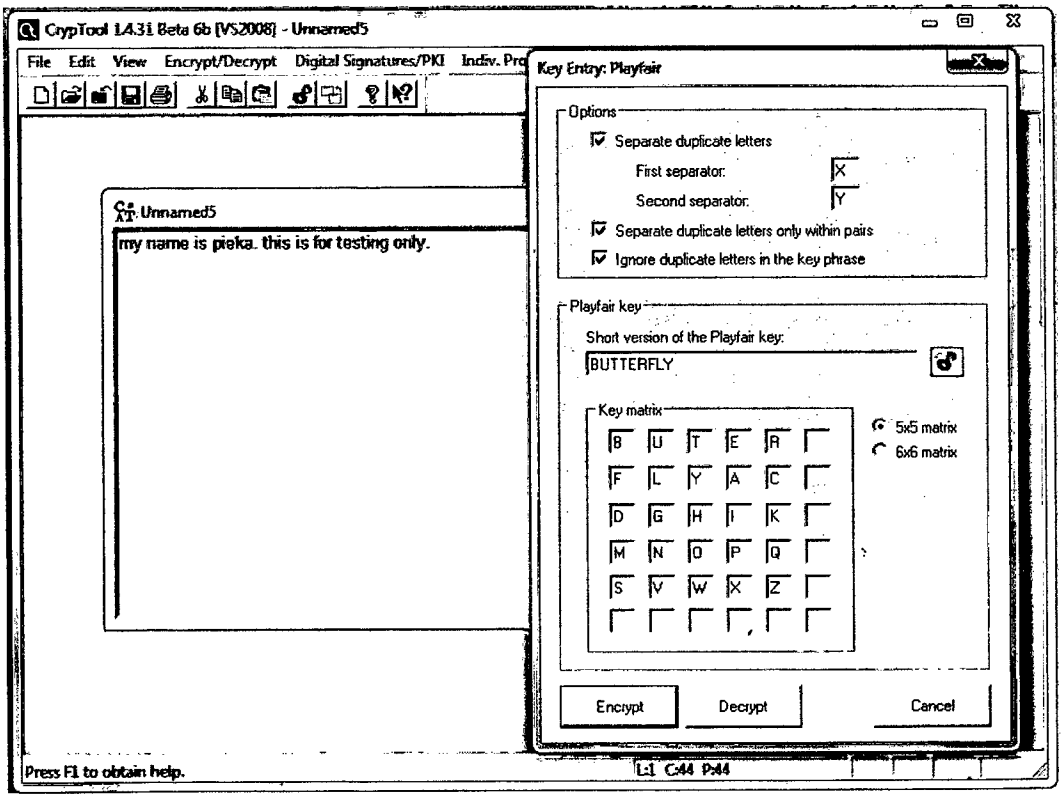

Figure 2.4 : The example of encryption using Playfair cipher.

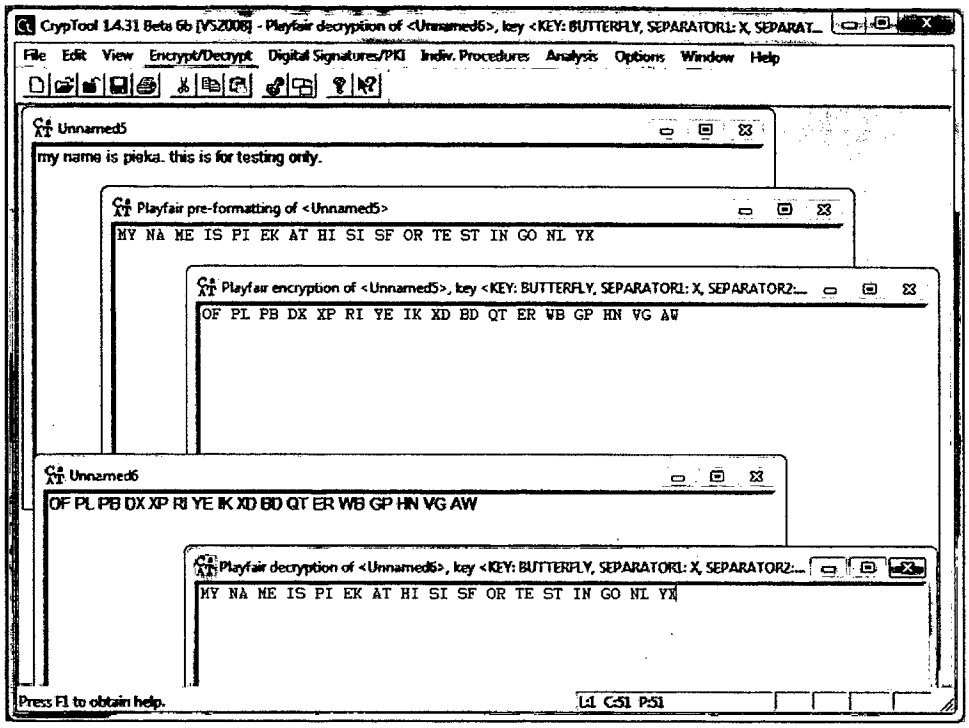

Figure 2.5 : The interface for successful encrypted and decrypted plaintext using Playfair cipher.

CrypTool offers classical cryptography algorithms and modern cryptographic algorithms which include encryption and decryption, secure passwords, key generation, secure protocols, authentication and other options.

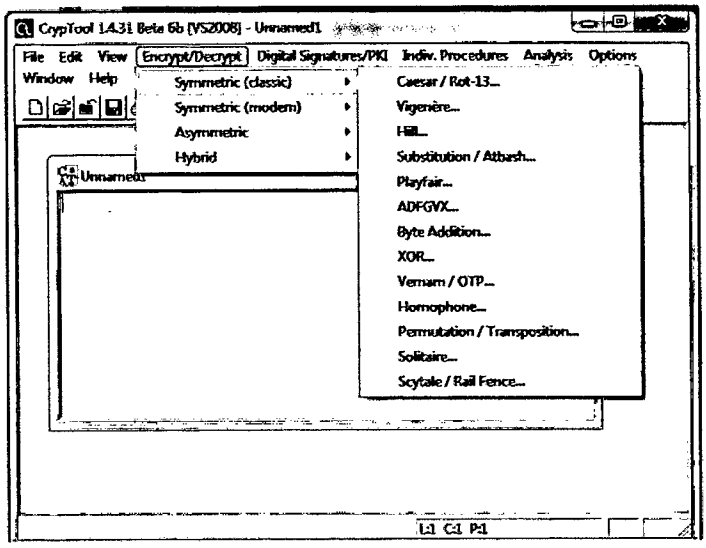

Figure 2.6 : List of classical symmetric encryption methods provided

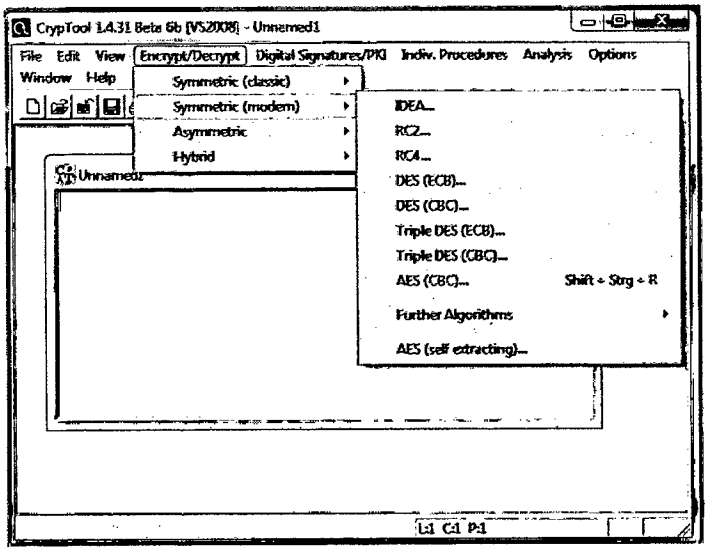

Figure 2.7 : List if modern symmetric encryption provided

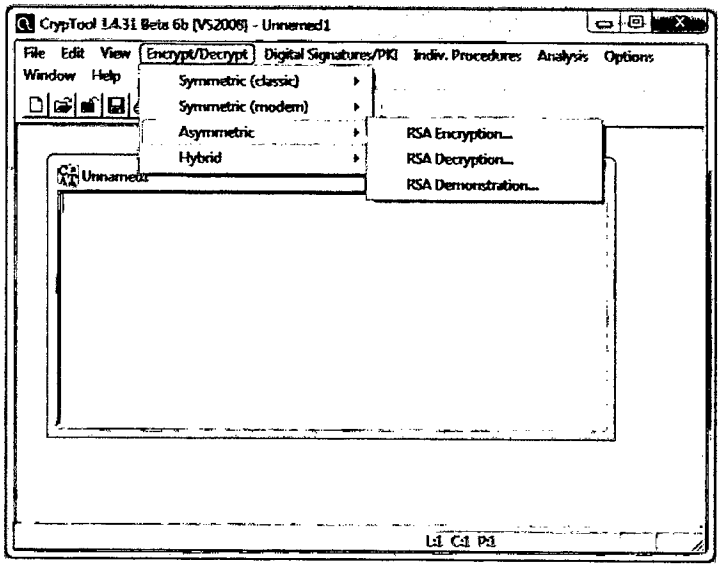

Figure 2.8 : List if asymmetric encryption provided

Basically, Cryptool provide many encryption cipher technique start from classical symmetric until hybrid encryption method. The encryption process only happen without visualization that may help beginner to understand about the algorithm currently used.

In other hand, Cryptool provides visualization of several algorithms for example Caesar, RSA, Enigma,Diffie-Hellman, AES and digital signatures. CrypTool also offers Cryptanalytical measurement methods and Cryptanalysis information for selected algorithms.

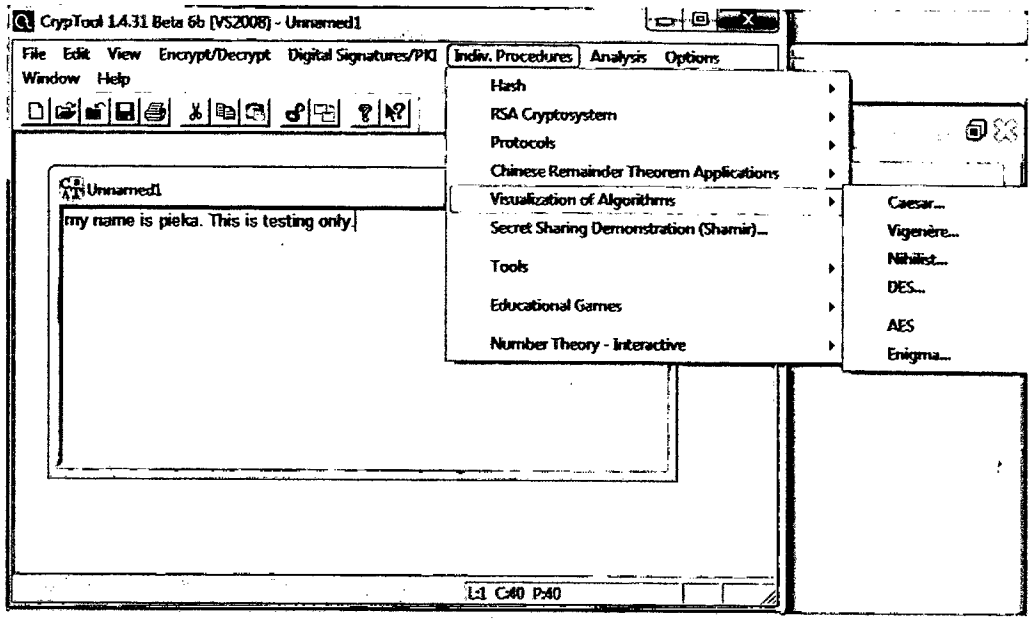

Figure 2.9 : The example of visualization of algorithms covered by Cryptool

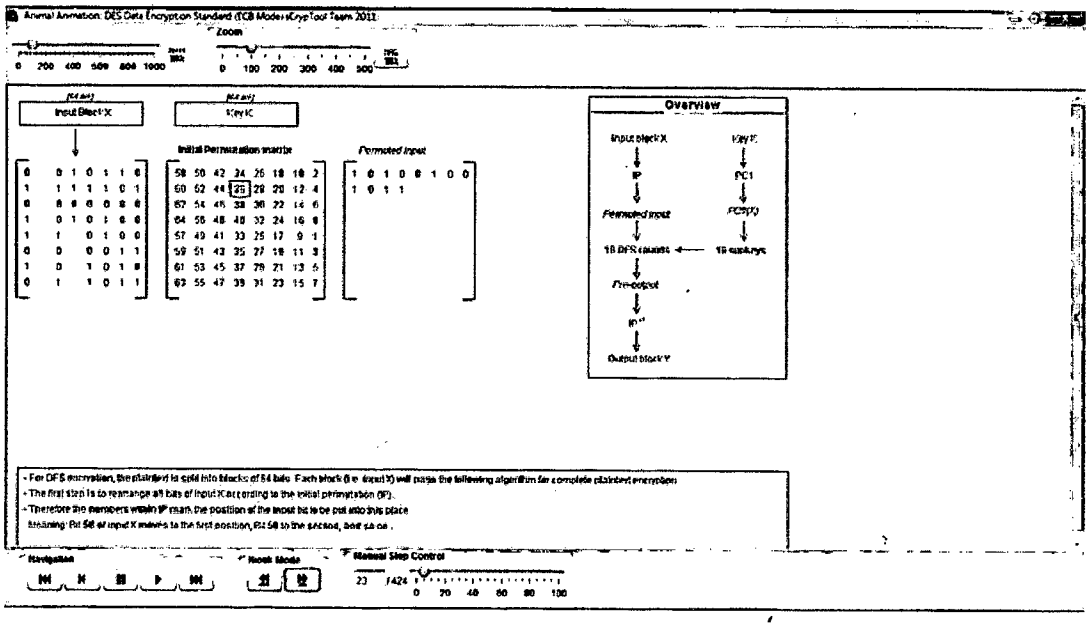

Figure 2.10 : Example of encryption process using DES algorithm