The International Journal of Multi-Disciplinary Research

ISSN: 3471-7102

Asymmetric Cryptography (AsymmCrypto)

(Conference ID: CFP/274/2017)

Author: Mwashi Matela **(SIN**: 1310110633)
Dept. of Information Security and Computer Forensics
School of Enginneering,
Information and Communications University
P. O. Box 30226, Lusaka, Zambia

Supervisor: Dr Richard Silumbe
ICU Programs Coordinator
School of Enginneering,
Information and Communications University
P. O. Box 30226, Lusaka, Zambia

This Paper was Submitted in Partial fulfillment of a Bachelors Degree in Information Security and Computer Forensics

August 2017

DECLARATION

I Mwashi Matela, hereby declare that the work which is being presented in the project entitled "**Asymmetric Cryptography "**is in partial fulfillment for a Bachelors Degree in Information Security and Computer Forensics, and submitted to the Department of Computer Forensics, Information and Communications University is a record of my own work carried out under the Guidance of Dr. Richard Silumbe, ICU Programs Coordinator.

(Signature of Candidate)

MWASHI MATELA (1310110633)

DEDICATION

This piece of work is dedicated to my wife, Elina Chumbu Mwashi, who has not only been my wife but close and dependable friend. You offered unconditional love, thereby making the burden of writing this project report lessen substantially.

It is also dedicated to my parents Mr Boaz Soyala Mwashi and Mrs Inness Mambwe Mwashi who taught me to be hardworking, disciplined and respectful and above all to be God fearing.

Last but not the least, my friend Kay Kan for always putting a smile on my face even in the presence of undertaking this project.

ACKNOWLEDGEMENT

Acknowledgements are given to the following persons who were instrumental in this research. My supervisor, Dr Richard Silumbe for his valuable insight into the topic that helped me focus this research for valuable output. Much appreciation goes to the various institutions and companies that took time to answer my questions and gave me the required feedback to the objectives. Zambia Research and Development Center (ZRDC) for their support and efforts in seeing this project a success.

I would like to thank and appreciate my family and friends for their continued encouragement and support towards attaining greater heights in life.

To save the best for the last, I would like to thank God almighty for the strength and the wisdom.

TABLE OF CONTENTS

Declaration
Dedication
Acknowledgement
Abstract

Chapter One: Introduction
1.0 History of Cryptography
1.1 Objective
1.2 Scope
1.3 Algorithm
1.4 Use of the Project

Chapter Two: Theoretical Background
2.0 What is Cryptography?
2.1 Cryptography
2.2 Existing System and Problem Statement
2.3 Proposed System
2.4 Advantage of a Proposed System

Chapter Three: System Analysis and Planning
3.0 Modules and Their Description
3.0.1 GUI (Graphical User Interface)
3.0.2 Key Generation
3.0.3 Encryption
3.0.4 Decryption
3.1 Design
3.2 Activity Diagram
3.2.0 Sequence Diagram

3.2.1 Sequence Diagram Guide
3.3 Types of cryptographic algorithms
3.4 Public/Private key Cryptography
3.5 Attacks of cryptography

Chapter Four: System Implementation Details
4.0 **Hardware** and Software Requirements
4.0.1 Hardware Requirements
4.0.2 Software Requirements

Chapter Five: Source Code
5.0 Encryption
5.1 Decryption

Chapter Six: Output
6.0 How AsymmCrypto works
6.0.1 Encryption
6.0.2 Decryption

Chapter Seven: Recommendation and Conclusion

References

Abstract

Many organizations are working hard to secure themselves from the growing threats of message hacking through various trends in cryptography. Yet the headlines are dominated with the latest news of message passing disaster more frequently than any time before.

This document intends to review this problem and propose several possible solutions. The cryptographic industry has been responding to these threats with ever-quicker responses to the rapid onslaught of malicious techniques, while corporations establish strict cryptographic techniques.

Placing organization's cryptographic techniques at the desktop level is like closing all the doors in a house while leaving windows and other entry points open. The present document discusses various cryptographic techniques of all times such as the three basic algorithms namely private key algorithm, public key algorithm and the hash functions.

The need for having three encryption techniques has also been encrypted.

A detailed discussion has been done on the classical cryptography and the drawbacks of the classical cryptography to ensure the need for going to new trends in cryptography like quantum cryptography, elliptic curve cryptography.

These new techniques that have emerged out of various exploitations in the field of cryptography rises a fair amount of hope that we can overcome the problems we are facing in a head hoc way. These proven technologies can meet the needs of the most demanding of environments while their respective focus on manageability has automated many tasks and simplified administrative functions through easy-to-use interfaces developed through years of customer feedback. And at the end of the document we can conclude that soon we can save secrecy involved in message passing from the dangerous clutches of message hackers.

INTRODUCTION

The Internet is the internationally connected network of computer networks with addresses that are administrated by IANA (Internet address and Naming Authority). It grew dramatically because anyone can connect to it and anyone connected to it can connect others to it as well. Each site that is connected to it, can become an Internet Service provider to other sites

Does increased security provide comfort to paranoid people? Or does security provide some very basic protections that we are naive to believe that we don't need? During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with.

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. This paper has two major purposes. The first is to define some of the terms and concepts behind basic cryptographic methods, and to offer a way to compare the myriad cryptographic schemes in use today. The second is to provide some real examples of cryptography and new trends in use today.

CHAPTER 1

INTRODUCTION

1.0 History of Cryptography

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography is writing dates back to circa 1900 B.C. when an
Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans.

It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any UN trusted medium, which includes just about any network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- **Authentication**: The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- **Privacy/confidentiality**: Ensuring that no one can read the message except the intended receiver.
- **Integrity**: Assuring the receiver that the received message has not been altered in any way from the original.
- **Non-repudiation**: A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below.

In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

1.1 Objective

Security measures must be incorporated into computer systems whenever they are potential targets for malicious or mischievous attacks. This is especially for systems which handle financial transactions or confidential, classified or other information whose secrecy and integrity are critical. With the need to protect the integrity and privacy of information belonging to individuals and organizations, we have developed this system. The objective of encryption algorithms is to allow the encryption of a message by one person and the decryption of the message by another person

1.2 Scope

This project aims at converting the plaintext into a form unreadable by unauthorized people and hence can be readily transferred across the web and decrypted at the recipient side only by authorized people. It provides an interactive environment to encrypt, decrypt or transfer encrypted files without compromising with the integrity and privacy of critical information .In the era of wide area , open distributed systems , this system will help resolve various security issues.

1.3 Algorithm

- A large prime number p and a random number g which is prime and less than the initially

  Chosen prime number is chosen.
- Then after from {0,…,p-1} there are chosen the elements x1,x2,…,x2n+1, preferably distinct .
- Calculate y1=gx1 mod p,y2=g x2 mod p,…, y2n+1=g x2n+1 mod p.
- The public key is {p,g,y1,y2,…….,y2n+1} and the private key consists of {x1,x2,…,x2n+1}.

- The sender encrypts message m knowing the public key as : choose a random element k from {0 ,…, p-1} and calculates c1=g k mod p,c21=m.x1 k mod p, c22=m.x2 k mod p,… , c22n+1=m.x2n+1 k mod p, c2= c21. c23. c25. c27…./c22. c24. c26…. then sends the encrypted message (c1, c2) to the recipient.

- To decrypt the message (c1, c2), calculate c2. c1x2 . c1x4 . c1x6 …/ c1x1 . c1x3 . c1x5 . c1x7 …= (c21. c23. c25. c27…/ c22. c24. c26…)(c1x2 . c1x4 . c1x6…/ c1x1 . c1x3 . c1x5 . c1x7…) = (m . y 1 k . m . y 3 k . m . y 5 k . m . y 7 k…/ m . y 2 k . m . y 4 k . m . y 6 k…)(c1x2 . c1x4 . c1x6…/ c1x1 . c1x3 . c1x5 . c1x7…) = m.

1.4 Use of the Project

It can be used by the government of a country so that the task of various national policy formulation and international trade may proceed smoothly. It can also be used by banks so that the task of amount transfer, amount withdrawal or balance enquiry, etc. can be done without the fear of losing the password. It can even be used by various websites so as to keep the password and other private entities of the user secure .It can be used by credit card companies so as to safely send the credit card numbers on the net and avoid it‟s misuse and thus take proper care of the customer’s wealth.

CHAPTER 2

THEORETICAL BACKGROUND

2.0 What is Cryptography?

Cryptography derived its name from a Greek word called "krypto's" which means "Hidden Secrets".
Cryptography is the practice and study of hiding information. It is the Art or Science of converting a plain intelligible data into an unintelligible data and again retransforming that message into its original form.
It provides Confidentiality, Integrity, and Accuracy

2.1 Cryptography

Cryptography is probably the most important aspect of communication's security and is becoming increasingly important as a basic building block for computer security. The increased use of computer and communication systems by the industry has increased the risk of theft of proprietary information although these threats may require a variety of counter measures. Encryption is a primary method of protecting valuable electronic information. Encryption is the process of encoding a message in such a way as to hide its contents. Modern cryptography includes several secure algorithms for encrypting and decrypting messages. They are all based on the use of secrets called keys. A cryptographic key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without the knowledge of the key. Terms used in cryptography are as follows:

- **Plain text**: original message is known as plain text.
- **Cipher text**: coded message is known as cipher text.
- **Encryption**: the process of converting the plain text to cipher text is known as encryption.
- **Decryption**: the process of restoring the plain text from the cipher text is known as decryption.

Cryptographic systems are characterized along three independent dimensions

- ➢ The type of operation used for transforming plain text to cipher text:

  Substitution Technique: A substitution technique is one in which letters of plain text are replaced by other letters or by numbers or by symbols.

  Transposition Technique: In this we perform some sort of permutation on the plaintext letters.

- The number of keys used:

  Symmetric encryption: When both the sender and receiver use the same key for encrypting the plaintext and decrypting the cipher text to plain text, it is called symmetric encryption.

  Asymmetric encryption: When the sender use the public key of the receiver that has already been published by the recipient to encrypt the plaintext to cipher text and the receiver uses its private key to decrypt the cipher text to plaintext, it is called asymmetric encryption.

- The way in which plain text is processed :

  Lock Cipher: It is one in which a block of plaintext is treated as a whole and is used to produce a cipher block of equal length.
  Stream Cipher: It is the one that encrypts a digital data stream a bit or one byte at a time.

2.2 Existing System and Problem Statement

At present, the Elgamal encryption algorithm works by sending data to the receiver who has just one private key to decrypt the data .The entire process is as follows :

Key generation : The receiver who wishes to get message, chooses a large prime number p, a random number g which is also prime and less than the prime number initially chosen and a random integer x from 0 to (p-1). He then calculates

$$y=gx \bmod p$$

The public key of the sender is (p , g , y) and his private key is x.

Encryption by the sender : The sender generates an integer k lying between 0 to (p-1). He then calculates

$$r = g\ k \bmod p$$

and t = (yk . M) mod p and transmits (r , t) as the encrypted message .

Decryption of the cipher text:

The receiver with his private key calculates t. r-x which gives the plaintext .But in this algorithm, as there is just one private key, it can be gessed by any intruder and is thus not reliable.

2.3 Proposed System

In this project, the encryption algorithm called the public key and assigning them to 2n+1 authorized receivers individually. The persons will be able to decrypt the message received from the sender only if they are together, separately this operation being impossible for them.

It has the following operations:

Key generation : A large prime number p and a random number g which is prime and less than the initially chosen prime number is chosen. Then after from {0,…,p-1} there are chosen the elements x1,x2,…,x2n+1, preferably distinct , then there are being calculated y1=g x1 mod p,y2=g x2 mod p,…, y2n+1=g x2n+1 mod p .The public key is {p,g,y1,y2,…….,y2n+1} and the private key consists of {x1,x2,…,x2n+1}.

Encryption of a message: The sender encrypts message m knowing the public key as follows: He chooses a random element k from {0 ,…, p-1} and calculates c1=g k mod p,c21=m.x1 k mod p, c22=m.x2 k mod p,… , c22n+1=m.x2n+1 k mod p, c2= c21. c23. c25. c27…./c22. c24. c26…. then sends the encrypted message (c1, c2) to the recipient.

Decryption of the message: In order to decrypt the message (c1, c2),the receiver use p and the private keys {x1}, {x2},…..,{x2n+1} respectively, computing together c2. c1 x2 . c1 x4 . c1 x6 …/ c1 x1 . c1 x3. c1 x5. c1 x7…= (c21. c23. c25. c27…/ c22. c24. c26…)(c1 x2 . c1 x4 . c1 x6…/ c1 x1. c1 x3.c1 x5. c1 x7…) = (m .y1 k . m . y3 k . m . y5 k . m . y7 k…/ m .y2 k . m . y4 k . m . y6 k…)(c1 x2. c1 x4 . c1 x6…/ c1 x1 . c1 x3 . c1 x5 . c1 x7…) = m.

2.4 Advantage of a Proposed System

The encrypted message can be decrypted only if all the 2n+1 parts of the private key is known. Thus the intruder is unable to identify the message even if he succeeds in calculating one or some of the parts of the private key because the calculation of all 2n+1 parts of the private key is a difficult task and thus it is more secure.

CHAPTER 3

SYSTEM DESIGN

3.0 Modules and Their Description

There are five modules in this project

- GUI(Graphical User Interface)
- Key generation
- Encryption
- Decryption
- Data transfer

Now a description of each of the modules :

3.0.1 GUI (Graphical User Interface):

GUI provides an efficient way through which user can interact with the system and works accordingly to fulfill the task. Through GUI user can select the file that is to be encrypted or decrypted. User can generate keys randomly or enter manually. At every window a “back” button is provided to let the user to go back to the previous window. Thus, it provides a user-friendly environment.

3.0.2 Key Generation:

This module generates keys. The keys can be generated randomly or it can be specified by the user. If the keys are being generated randomly, the user does not need to check if the number is prime or not. But if the keys are entered manually, the user needs to be sure of the number to be prime otherwise an error message will be displayed every time the user enters a wrong value. When the keys are entered manually, the test for prime number is done by Millar Rabin algorithm.

3.0.3 Encryption:

The sender chooses a random element k from {0,…,p-1} and calculates c1=g k mod p, c21=m.x1 k mod p, c22=m.x2 k mod p,…, c22n+1=m.x2n+1 k mod p, c2= c21. c23. c25. c27…./ c22. c24. c26…. then sends the encrypted message (c1, c2) to the recipient.Thus the size of the encrypted message is double of the plaintext as each charater is represented by two values.

3.0.4 Decryption

In order to decrypt the message (c1, c2), receiver1 , receiver2 ,…, receiver2n+1 are using q and the private keys {x1}, {x2},…..,{x2n+1} respectively, computing together c2. c1 x2. c1 x4. c1 x6 …/ c1 x1. c1 x3. c1 x5. c1 x7… 4.1.5 Data Transfer: This module will be used to transfer encrypted files from one system to the other. The other system should keep waiting for the file if it wants to receive a file or else a connection failure occurs. The IP address of the destination needs to be mentioned correctly.

3.1 Design

Software design is a process of problem solving and planning for a software solution. After the purpose and specifications of software are determined, software developers will design or employ designers to develop a plan for a solution. It includes low-level component and algorithm implementation issues as well as the architectural view. Software design can be considered as putting solution to the problem(s) in hand using the available capabilities. Hence the main difference between Software analysis and design is that the output of the analysis of a software problem will be smaller problems to solve and it should not deviate so much even if it is conducted by different team members or even by entirely different groups. But since design depends on the capabilities, we can have different designs for the same problem depending on the capabilities of the environment that will host the solution (whether it is some OS, web, mobile or even the new cloud computing paradigm). The solution will depend also on the used development environment (Whether you build a solution from scratch or using reliable frameworks or at least implement some suitable design patterns).

3.2 Activity Diagram

Activity diagrams are a loosely defined diagram technique for showing workflows of stepwise activities and actions, with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control. In Sys ML the activity diagram has been extended to indicate flows among steps that convey physical element (e.g., gasoline) or energy (e.g., torque, pressure). In UML 1.x, an activity diagram is a variation of the UML State diagram in which the "states" represent activities, and the transitions represent the completion of those activities. Activity diagrams are typically used for business process modeling. They consist of initial node, activity final node, activities. The starting point of the diagram is the initial node, and the activity final node is the ending.

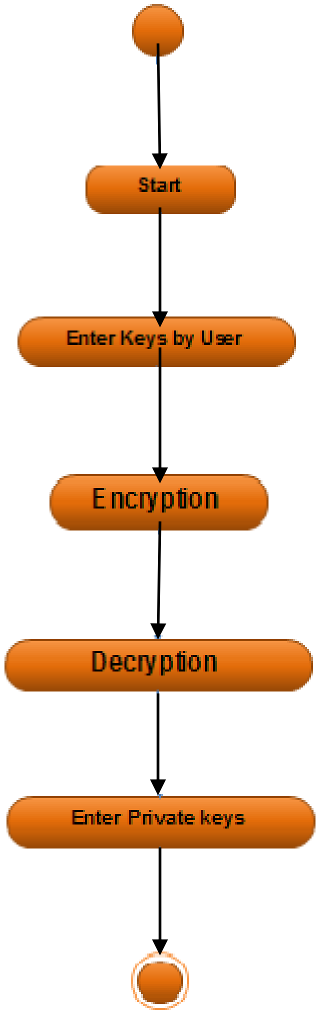


Figure 3.1: Activity Diagram

3.2.1 Sequence Diagram

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called Event-trace diagrams, event scenarios, and timing diagrams. A sequence diagram shows, as parallel vertical lines ("lifelines"), different processes or objects that live simultaneously, and, as horizontal arrows, the messages exchanged between them, in the order in which they occur. This allows the specification of simple runtime scenarios in a graphical manner.

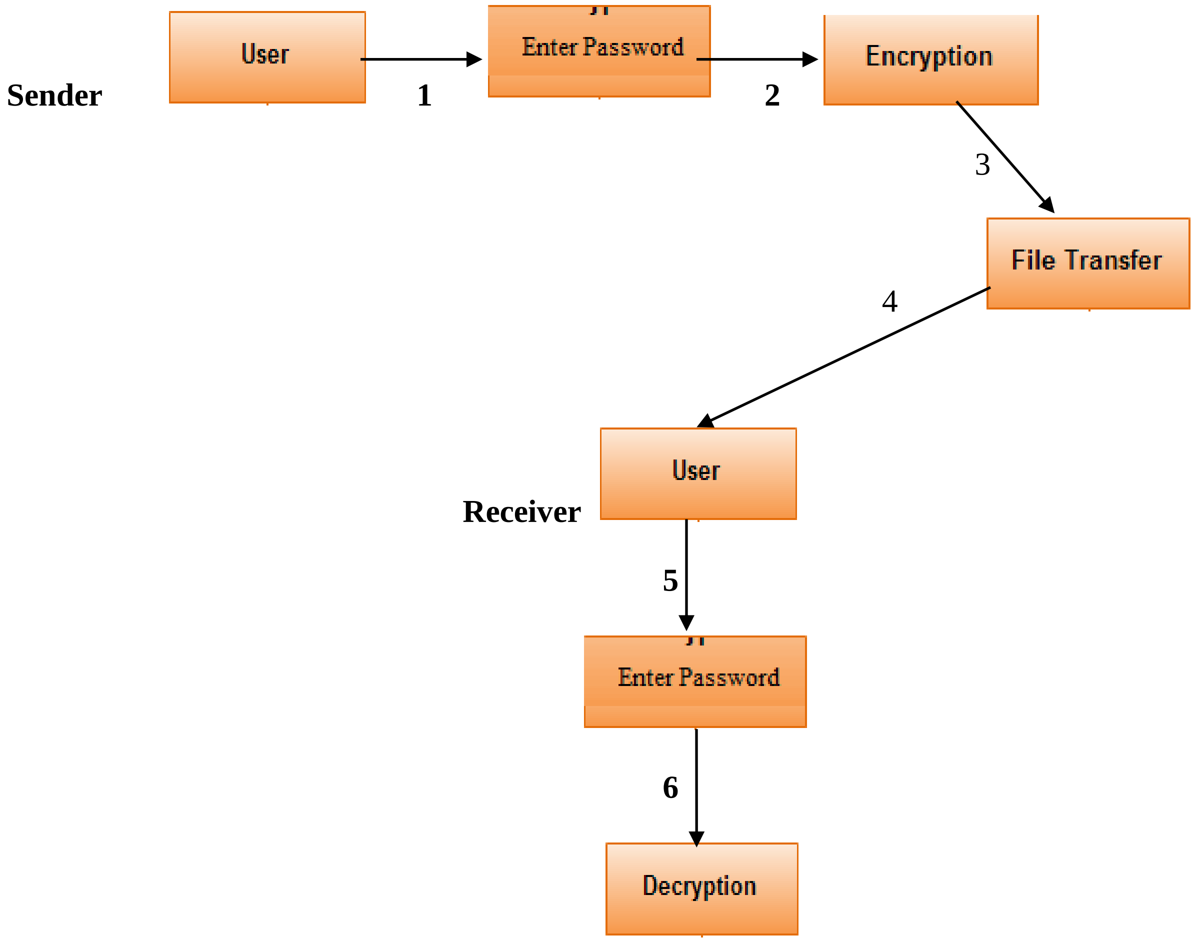


Figure 3.2: Sequence Diagram

3.2.1 Sequence Diagram Guide

1) User (sender) Opens AsymmCrypto
2) Enters the Encryption key (Public Key) password
3) Types the message(plain text),Encrypts it (cipher text), saves it and then sends it.
4) User (receiver) receives the file, Opens AsymmCrypto
5) Enters the Decryption key (Private key) password
6) Cipher text is Decrypted to plain text and then saved or discarded

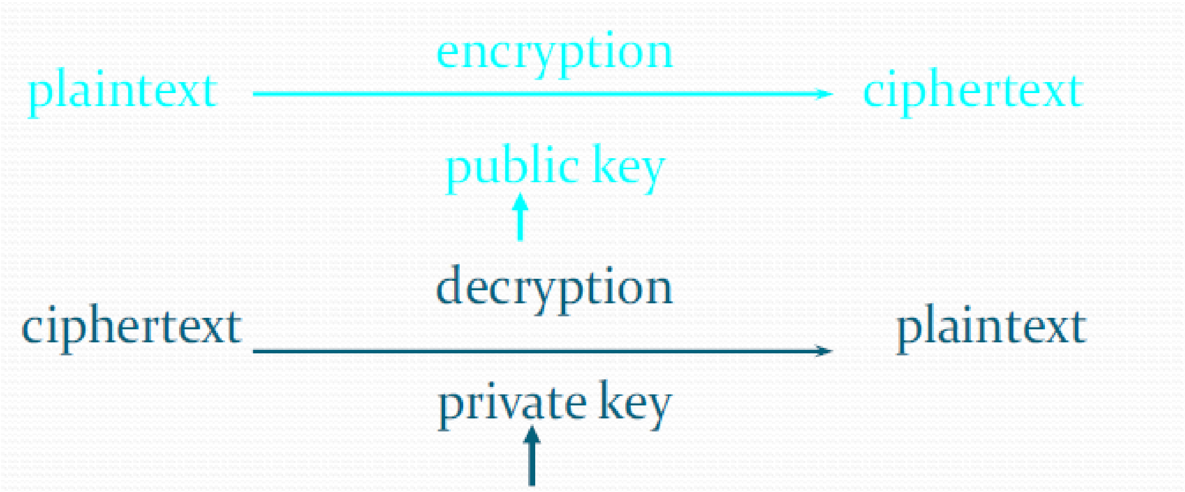


Figure 3.3: Process of Asymmetric cryptography

3.3 Types of cryptographic algorithms

There are several ways of classifying cryptographic algorithms. For purposes of this project, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are

· Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption

· Public Key Cryptography (PKC): Uses one key for encryption and another for decryption

· Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

a) Secret key (asymmetric) cryptography. SKC uses a single key for both encryption and decryption.

b) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption

c) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the cipher text.

3.4 Public/Private Key Cryptography

Asymmetric key cryptography overcomes the key management problem by using different encryption and decryption key pairs. Having knowledge of one key, say the encryption key, is not sufficient enough to determine the other key - the decryption key.

Therefore, the encryption key can be made public, provided the decryption key is held only by the party wishing to receive encrypted messages (hence the name public/private key cryptography). Anyone can use the public key to encrypt a message, but only the recipient can decrypt it.

RSA is a widely used public/private key algorithm is, named after the initials of its inventors, Ronald L. Rivets, Adi Shamir, and Leonard M. Adelman [RSA 91]. It depends on the difficulty of factoring the product of two very large prime numbers. Although used for encrypting whole messages, RSA is much less efficient than symmetric key algorithms such as DES. El Gamal is another public/private key algorithm [El Gamal 85]. This uses a different arithmetic algorithm than RSA, called the discrete logarithm problem.

The mathematical relationship between the public/private key pair permits a general rule: any message encrypted with one key of the pair can be successfully decrypted only with that key's counterpart. To encrypt with the public key means you can decrypt only with the private key. The converse is also true - to encrypt with the private key means you can decrypt only with the public key.

3.5 Attacks of cryptography

1. Cipher text only attack
   The only data available is a target cipher text
2. Known plaintext attack
   A target cipher text
   Pairs of other cipher text and plaintext (say, previously broken or guessing)
3. Chosen plaintext attacks
   A target cipher text
   Can feed encryption algorithm with plaintexts and obtain the matching cipher texts
4. Chosen cipher text attack
   A target cipher text
   Can feed decryption algorithm with cipher texts and obtain the matching plaintexts

CHAPTER 4

SYSTEM IMPLEMENTATION DETAILS

4.0 Hardware and Software Requirements

This project has been coded in Visual Basic and the system requirements are as follows:

4.0.1 Hardware Requirements

- Intel Pentium III Processor
- RAM size 256MB
- Hard Disk 10GB

4.0.2 Software Requirements

- Windows XP
- Visual Basic 6.0

CHAPTER 5
SOURCE CODE

5.0 Encryption key

```
set x = WScript.CreateObject("WScript.Shell")

mySecret= inputbox("enter text to be encoded")

mySecret= StrReverse(mySecret)

x.Run "%windir%\notepad"

wscript.sleep 1000

x.sendkeys encode(mySecret)


function encode(s)

For i = 1 To Len(s)

newtxt = Mid(s,i,1)

newtxt = Chr(Asc(newtxt)+3)

coded = coded & newtxt

Next

encode = coded

End function
```

5.1 Decryptor

```
set x = WScript.CreateObject("WScript.Shell")
mySecret= inputbox("enter text to be encoded")
mySecret= StrReverse(mySecret)
x.Run "%windir%\notepad"
wscript.sleep 1000
x.sendkeys encode(mySecret)

function encode(s)
For i = 1 To Len(s)
newtxt = Mid(s,i,1)
newtxt = Chr(Asc(newtxt)-3)
coded = coded & newtxt
Next
encode = coded
End function
```

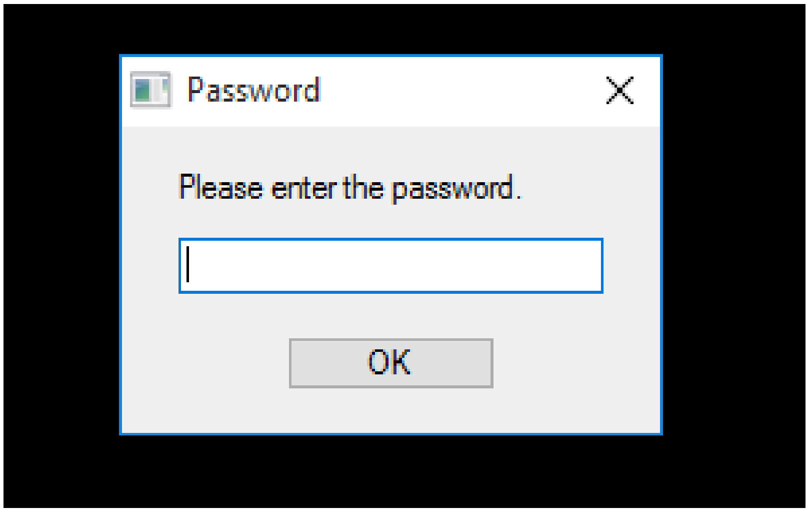
CHAPTER 6

OUTPUT

6.0 How AsymmCrypto works

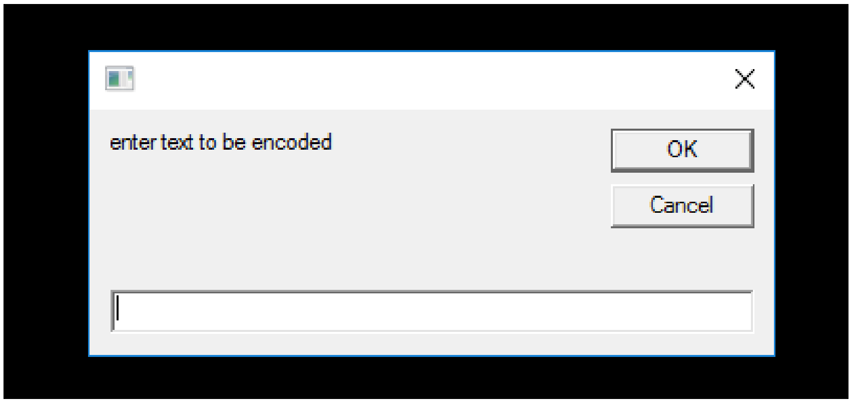
6.0.1 Encrypting:

- Double Click the Encryption Key and the following window will pop up then enter the password (zrdcicu)



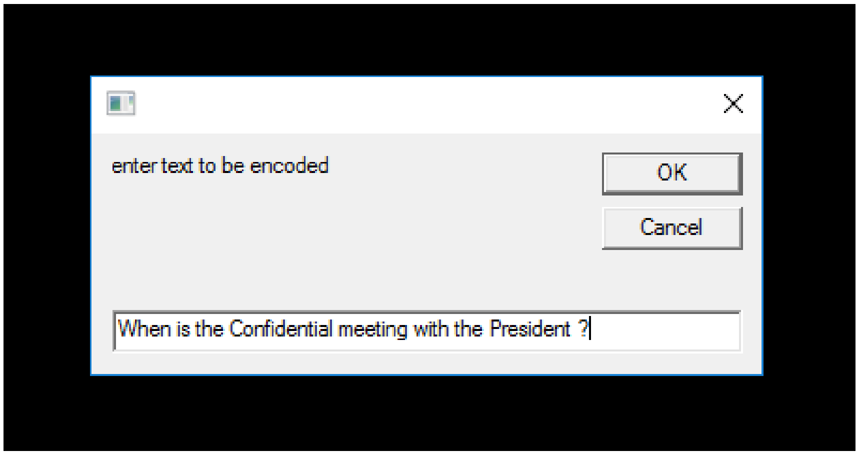
Please enter the password.

- When u enter a wrong password the following window will pop up
- When u enter a correct password the following window will pop up



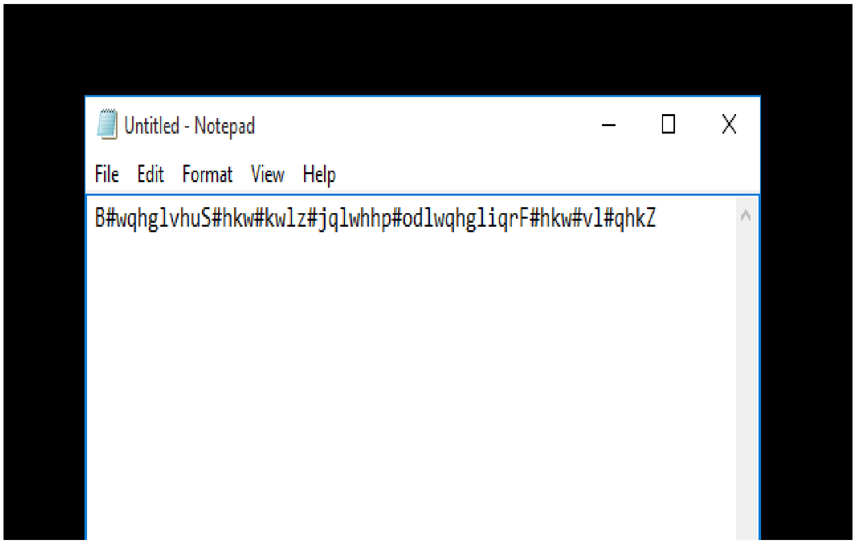
enter text to be encoded

- Type the message u would like to Encrypt.



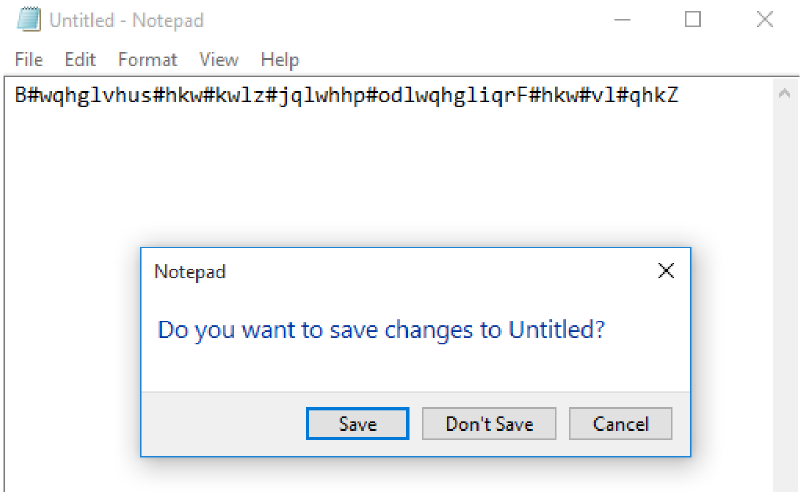
enter text to be encoded

When is the Confidential meeting with the President ?



```
B#wqhglvhuS#hkw#kwlz#jqlwhhp#odlwqhgliqrF#hkw#vl#qhkZ
```

- After typing,click on ok if u want to encrypt the message or cancel to discard.
- When u click on OK button Notepad opens.
- Save your message in text format with a (.txt) extension.



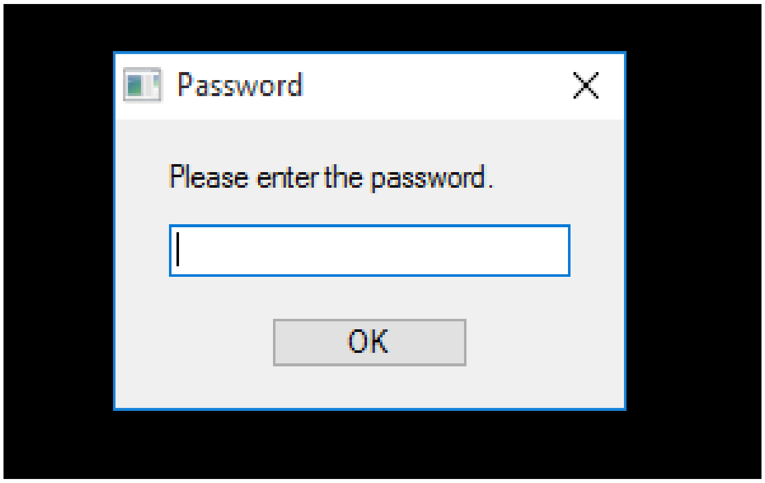
```
B#wqhglvhus#hkw#kwlz#jqlwhhp#odlwqhgliqrF#hkw#vl#qhkZ
```

Do you want to save changes to Untitled?

- If u try to close Notepad without saving, it will prompt u with "Do you want to save changes to untitled?" .At this point u can either save or discard, but remember that when saving u save it with a (.txt) extension.

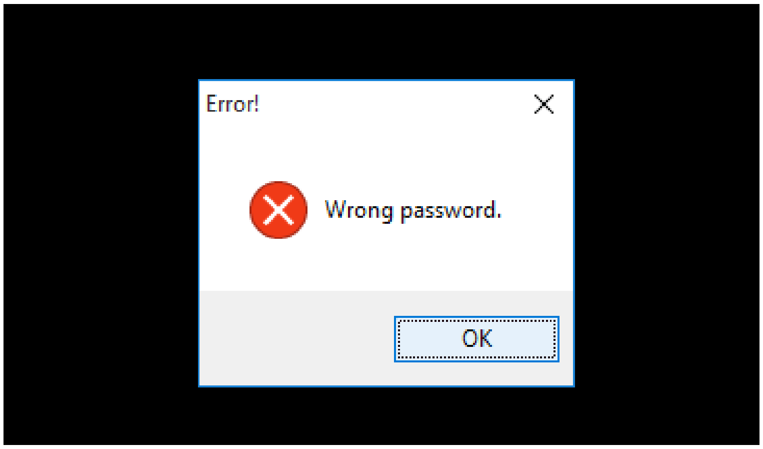
6.1 Decrypting:

- Double Click the Decryption Key and the following window will pop up.
- Enter the password (icu)



Please enter the password.

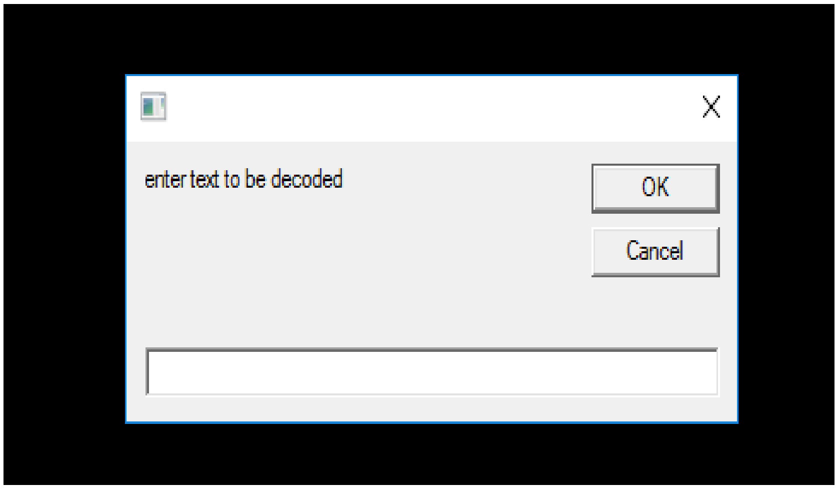
- When you enter a wrong password, the following window will pop up



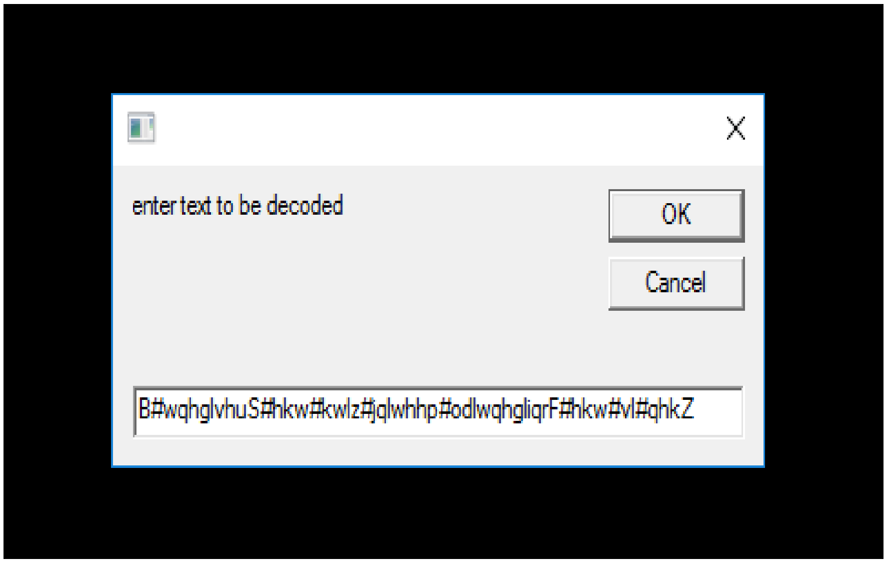
Error!

Wrong password.

- When u enter a correct password, the following window will pop up, paste the message you would like to Decrypt.



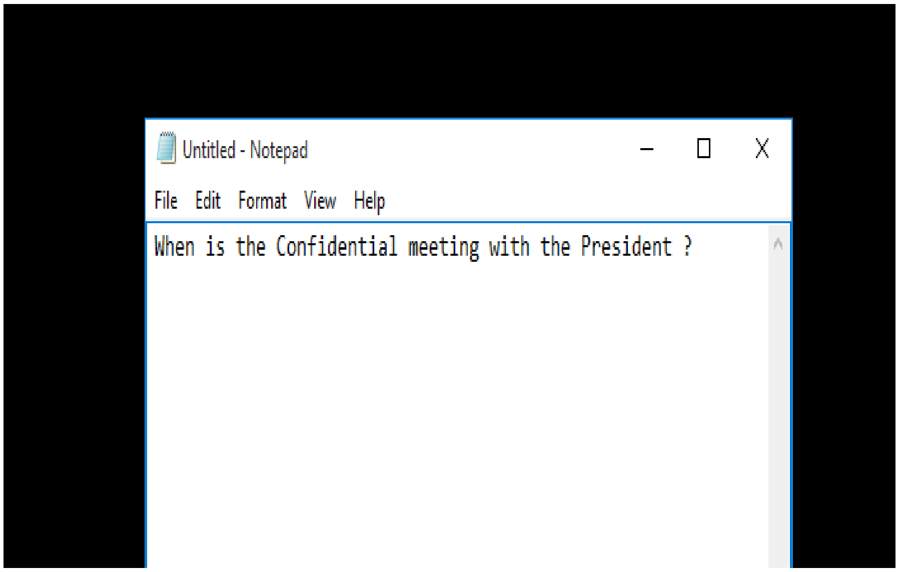
enter text to be decoded



enter text to be decoded

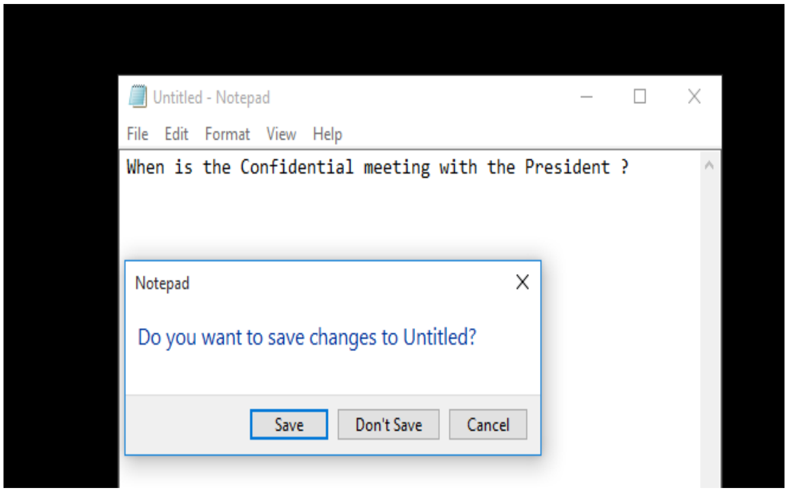
B#wqhglvhuS#hkw#kwlz#jqlwhhp#odlwqhgliqrF#hkw#vl#qhkZ

- After Pasting, click on ok to Decrypt the message or cancel to discard.
- When u click on OK button Notepad opens.



When is the Confidential meeting with the President ?

- Save your message in text format with a (.txt) extension.



When is the Confidential meeting with the President ?

Do you want to save changes to Untitled?

- If u try to close Notepad without saving, it will prompt u with “Do you want to save changes to untitled?”. At this point u can either save or discard, but remember that when saving u save it with a (.txt) extension.

CHAPTER SEVEN

RECOMMENDATION AND CONCLUSION

We use different types of algorithms to establish security services in different service mechanisms. We use either private key cryptography or public key cryptography according to requirements. If we want to send message quickly we use private key algorithm and if we want to send messages secretly we use public key algorithm.

Public-key cryptography has evolved from early models such as Küchlin's to more sophisticated systems that have provided the privacy and data security that we need in the modern world. Secret-key cryptography lags behind asymmetric cryptography. Combinations of the two can be implemented for improved security but secret-key cryptography by itself proves insecure against man in the middle attacks. Asymmetric cryptography has been the foundation for secure data exchange over networks and while it still has its shortcomings, new ideas still come forth as the field continues to evolve.

REFERENCES

[1] Kishnamurthy G. N, Dr.V.Ramaswamy and Mrs.Leela.G.H ,―Performance Enhancement of Blowfish algorithm by modifying its function‖ Proceedings of International Conference on Computers, Information, System Sciences and Engineering 2006, University of Bridgeport, Bridgeport, CT, USA. pp. 240-244.

[2] Knudsen L., "Block Ciphers: A Survey", State of the Art in Applied Cryptography: Course on Computer Security and Industrial Cryptography (Lecture Notes in Computer Science no. 1528), Springer-Verlag, pp. 18-48, 1998.

[3] Manikandan G., Krishnan. G, ―A Novel Approach to the Performance and Security Enhancement Using Blowfish Algorithm‖, International journal of Advanced Research in Computer Science, 2011.

[4] Ramaswamy V., Kishnamurthy G. N., Leela G. H., Ashalatha M. E., ―Performance enhancement of CAST –128 Algorithm by modifying its function‖ Proceedings of International Conference on Computers, Information, System Sciences and Engineering 2007, University of Bridgeport, Bridgeport, CT, USA.

[5] Schneier B., (1995). Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons.

[6] Schneier B., ―Description of a New Variable-Length Key, 64- Bit Block Cipher (Blowfish)‖, Fast Software Encryption, Cambridge Security Workshop proceedings (December 1993), Springer-Verlag, 1994, pp. 191-204.

[7] William Stallings, Cryptography and Network Security, 3rd Ed, Wiley, 1995.