

**SECURE TEXT TRANSFER VIA BLUETOOTH USING HYBRID
ENCRYPTION**

FAKHRUL HAKIMI B SAIDI

CA09095

FACULTY OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING

UNIVERSITI MALAYSIA PAHANG

UNIVERSITY MALAYSIA PAHANG
CENTER FOR GRADUATE STUDIES

We certify that the thesis entitled Secure Text Transfer Via Bluetooth Using Hybrid Encryption is written by Fakhrul Hakimi B Saidi. We have examined the final copy of this thesis and in our opinion; it is fully adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science(Computer System and Networking). We here with recommend that it be accepted in fullfillment of the requirements for the degree of Bachelor of Computer Science(Computer System and Networking).

Name of External Examiner:

Signature:

Institution:

Name of Internal Examiner:

Signature:

Institution:

**SECURE TEXT TRANSFER VIA BLUETOOTH USING HYBRID
ENCRYPTION**

FAKHRUL HAKIMI B SAIDI

**A thesis submitted in fulfilment of the requirements
for the award of the degree of
Bachelor of Computer Science(Computer System and Networking)**

Faculty of Computer Science & Software Engineering

UNIVERSITY MALAYSIA PAHANG

JUNE 2012

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Computer Science(Computer System and Networking).

SIGNATURE

NAME OF SUPERVISOR:

POSITION:

DATE:

SIGNATURE

NAME OF CO-SUPERVISOR:

POSITION:

DATE:

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledge. The thesis has not been accepted for any degree and is not concurrently submitted for award of other degree.

SIGNATURE

NAME OF SUPERVISOR:

POSITION:

DATE:

ACKNOWLEDGEMENT

Assalamualaikum. Firstly, thank you Allah for His blessings through the accomplishment of the Secure Text Transfer Via Bluetooth Using Hybrid Encryption and my thesis. I am very honored and grateful to En. Syahrizal Azmir B. Md. Sharif for being my supervisor. His advises and comments have been a great contribution for the achievement of my thesis.

I would also like thank my parents Mr. Saidi and Mrs. Sauziah for their love, morale and financial support and motivation. Not forgetting to all my friends for their time guiding and teaching me in order to finish the project.

I would like to extend my gratitude to my classmates who have been kind in sharing knowledge and time to help me with my project. I really appreciate it.

Thank you.

ABSTRACT

Secure Text Transfer via Bluetooth Using Hybrid Encryption is a system to secure the text before it transfer via Bluetooth. This system helps the user to secure their text using hybrid encryption. Hybrid encryption will make the text become more secure because it uses the combination of two encryption algorithm. This system content 2 layer of encryption and decryption. Besides that, this system also ensures only the true receiver wills receiver the text. During Bluetooth connection, the user must change their key passkey.

ABSTRAK

Keselamatan Penghantaran Perkataan Melalui Bluetooth Menggunakan Gabungan Penyulitan ialah sistem untuk memberi keselamatan kepada perkataan sebelum menghantar melalui Bluetooth. Sistem ini menolong pengguna untuk memberi keselamatan kepada perkataan menggunakan gabungan penyulitan. Gabungan penyulitan akan membuat perkataan akan menjadi lebih selamat kerana ia menggunakan gabungan dua penyulitan. Sistem ini mempunyai 2 lapis penyulitan dan penyahsulitan. Disamping itu, sistem ini juga memastikan hanya penerima sebenar akan menerima perkataan daripada penghantar. Semasa gabungan Bluetooth, pengguna mesti menukar kunci penghantaran.

TABLE OF CONTENT

CHAPTER	TITLE	PAGE
	ACKNOWLEDGEMENT	vi
	ABSTRACT	vii
	TABLE OF CONTENTS	ix-xi
	LIST OF FIGURES	xii-xiii
	LIST OF TABLE	xiii
	LIST OF APPENDIX	xiv
1	INTRODUCTION	1
	1.1 Introduction	1
	1.2 Problem Statement	2
	1.3 Objective	3
	1.4 Scope	3
	1.5 Thesis Organization	3
2	LITERATURE REVIEW	5
	2.1 Introduction	5
	2.2 The Concept of the Project	6
	2.2.1 The Concept of Security	6
	2.2.2 The Concept of File Transfer	8
	2.2.3 The Concept of Bluetooth Technology	9
	2.3 Basic Bluetooth Security	10
	2.3.1 Authentication	10
	2.3.2 Confidentiality	12
	2.3.3 Authorization	12
	2.4 Techniques	12
	2.4.1 Hybrid Encryption	14
	2.4.2 Type Of Algorithm	14
	2.4.3 Programming Languages	22

2.4.4	Type Of Application	25
2.5	Bluetooth Security Risk	27
2.6	Comparison Between Existing Application	29
3	METHODOLOGY	29
3.1	Software Development Life Cycle	31
3.1.1	Waterfall Model	32
3.1.1.1	Analysis And Definition	33
3.1.1.2	System And Software Design	34
3.1.1.2.1	Interface Design	34
3.1.1.2.2	Flowchart of The System	36
3.1.1.2.3	Use Case Diagram	38
3.1.1.2.4	Context Diagram	39
3.1.1.2.5	Level 0 Diagram	40
3.1.1.3	Implementation	41
3.1.1.4	System Testing	42
3.1.1.5	Operations and Maintenance	43
3.2	System Requirement	43
3.2.1	Software Requirement	44
3.2.2	Hardware Requirement	44
4	SYSTEM DEVELOPMENT AND TESTING	45
4.1	Connect Bluetooth Device	45
4.2	System Development	46
5	RESULTS AND DISCUSSION	58
5.1	Results	58
5.2	Discussion	59
5.2.1	Strength	59
5.2.2	Weakness	60

5.3	System Enhancement	60
6	CONCLUSION	62
	REFERENCES	63
	APPENDICES	65

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.0	File Transfer	9
2.1	Symbol Of Bluetooth	9
2.2	Bluetooth Security	10
2.3	Authentication Process	11
2.4	Blowfish Algorithm	15
2.5	Twofish	16
2.6	Basic Structure of AES Algorithm	18
2.7	Small Example Of Splay	21
3.1	Example of SDLC Waterfall	33
3.2	The Flow of project	34
3.3	Logical Interface for Login The System	35
3.4	Logical Interface at Sender sides	35
3.5	Logical Interface at Receiver sides	36
3.6	Flowchart of the system	37
3.7	Use Case Diagram for the system	38
3.8	Context Diagram of the system	39
3.9	Level 0 Diagram	40
3.10	Blowfish Algorithm	41
3.11	Twofish Algorithm	42
4.1	Select Device	45
4.2	Set key passkey	46
4.3	Enter pairing code	46
4.4	Success Interfaces	47
4.5	Login Interface	48

FIGURE NO.	TITLE	PAGE
4.6	Login Interface with message box	48
4.7	Register interface	49
4.8	Register interface with message box success	50
4.9	Register interface with message box username and password	50
4.10	Login interface with username and password	51
4.11	Encrypt & Decrypt interface with message box port can't empty	52
4.12	Encrypt & Decrypt interface with message box port close	53
4.13	Insert text to encrypt	53
4.14	Encrypt text	54

LIST OF TABLE

TABLE NO.	TITLE	PAGE
1	Module security level specification file transfer	7
2	Symmetric versus Asymmetric	13
3	Comparison between algorithm	21
4	Comparison between existing system	29
5	Comparison between existing application and Secure text Transfer via Bluetooth sing Hybrid Encryption	30
6	Software requirement	43
7	Hardware Requirement	43

LIST OF APPENDIXES

APPENDIX	TITLE	PAGE
1	Gantt Chart	64
2	User Manual	65

BORANG PENGESAHAN STATUS TESIS

JUDUL: SECURE TEXT TRANSFER VIA BLUETOOTH USING HYBRID ENCRYPTION

SESI PENGAJIAN: _____

Saya: FAKHRUL HAKIMI B SAIDI

(HURUF BESAR)

mengaku membenarkan tesis (Projek Sarjana Muda/Sarjana/Doktor Falsafah)* ini disimpan di Perpustakaan Universiti Malaysia Pahang dengan syarat-syarat kegunaan seperti berikut:

1. Tesis adalah hakmilik Universiti Malaysia Pahang
2. Perpustakaan Universiti Malaysia Pahang dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (4)

SULIT

(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

TERHAD

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

Disahkan oleh

(TANDATANGAN PENULIS)

(TANDATANGAN PENYELIA)

Alamat Tetap:
Lot 359, Kg Ana, Jal Besar,
16210 Tumpat,
Kelantan

Nama penyelia:
En. Syahrizal Azmir Bin Md. Sharif

Tarikh: _____

Tarikh: _____

- CATATAN: * Potong yang tidak berkenaan.
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh tesis ini perlu dikelaskan sebagai SULIT atau TERHAD.
*** Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan, atau disertasi bagi pengajian secara

CHAPTER 1

INTRODUCTION

1.1 Introduction

Bluetooth technology is a transmission specification for digital data exchange between 2 or more devices over short range that uses radio waves for communication. Wireless signals of Bluetooth usually cover up to 10 meters and it can communicate at less than 1 Mbps. These technologies were use in large company such as Sony Ericsson, Nokia, Motorola, and IBM. There are a few version of Bluetooth such as Bluetooth version 1.2, Bluetooth version 2.0 and Bluetooth version 3.0. Bluetooth version 3.0 is the best technology compare to the other version because it can transfer the data in high speed rate.

The file can transfer using Bluetooth technology is include documents, image and voice over the devices like PDAs, phones and laptop. Even though Bluetooth is slower in transferring file compared to the other wireless technology but with this technology, it will decrease the uses of wire and cable to transfer the file of data. Many people from a different background like lecture, doctor, teachers and other professional use Bluetooth technology to transfer the file of data.

The malicious hacker using Bluetooth connections to steal the phone book, photo and calendar information or it allow the hacker to make the phone call or send an SMS

using one's mobile. The billing records would certainly point directly to the owner of the phone and real sender of the SMS. The security for the file transfer using Bluetooth technology is not so efficient so that the file and the personal information have been taken by the intruders. As a customer of Bluetooth technology, it is important for the customer to secure the file when using Bluetooth technology as a medium to transfer the file from one device to the other device. Secure the file when its transfer is important to avoid the file hacked from a bad person. The hackers can break in, stealing, disrupting, sabotage, modify and it will make the user of Bluetooth technology a problem when it happens. Unfortunately, some user only knows how to transfer but don't know how to secure it when it transfer. So, this project is carried out to produce an application to Secure Text Transfer via Bluetooth Using Hybrid Encryption.

Hybrid Encryption is a method of encryption that combines two or more encryption schemes and include a combination of symmetric and asymmetric encryption to take the advantages of the strengths of each of the encryption. The two type of encryption schemes use in this project is encryption algorithm and description algorithm. Encryption algorithm is the algorithm to translate of data into a secret code and this is the efficient way to achieve data security. Decryption is the process of decoding data that has been encrypted into a secret format.

1.2 Problem Statement

One of the problem encountered leading to this project is because the text from the user may be stealing or modify by the hackers for a some reason. So people who send sensitive information over a wireless connection need to take precautions to make sure the text are safe. The text will hack by the hackers if no security were uses. The default Bluetooth system is not enough for preventing the intruder. It means the text security must be enhance to make the text transferring using Bluetooth will be more secure and power than before.

1.3 Objectives

The objectives of the project are:

- i. To ensure the true receivers only receive the text and access it.
- ii. To increase the security of the text.
- iii. To develop 2 layer of encryption and decryption.

1.4 Scopes

The scopes of the project are:

- i. Using non-video and non-audio in file transferring.
- ii. Using text only.
- iii. Using Hybrid Encryption to make text transferring more secure.
- iv. Using Bluetooth technology.

1.5 Thesis organization

This thesis consists of six chapters. First is chapter 1. It consist the whole idea of the project that will be develop and it also include the objective of the project, problem statement and the scopes of work.

In Chapter 2, it will explain about literature review of the project. The literature review will be discussed about the algorithm and current technologies that will use during the project.

Chapter 3 will be discussing the approach, method or technology that will use in the project. Besides that, designing and implementation of the project also will be including in Chapter 3. The information that will including in thesis are introduction on how the project has been conduct, project methodology, methodology selection justification, and software and hardware necessity.

Chapter 4 will explain about the designed of the project development and all the process that was involved in development of the project. Besides that, in this chapter also contain the explanation about the method involve in the development and how it develop.

Chapter 5 is contain the result and data analysis that have been acquired and it also included result analysis, project limitation, suggestion and project enhancement.

Chapter 6 will be discuss about conclusion of the development project and summarizing about it.

CHAPTER 2

LITERATURE REVIEW

This chapter discusses about the literature review of Secure Text Transfer via Bluetooth Using Hybrid Encryption. There are several main sections in this chapter. The first main section in this literature review is introduction. Then, the next main section is describes about the concept of this project. After that, the basic of Bluetooth security will be discussed in this main section. Next, there are two main sections will be discussed that is techniques and Bluetooth security risk. The last main section discussed in this project is the existing security and vulnerabilities in Bluetooth.

2.1 Introduction

The information about this literature review gets from journal, web page, article and source relevant to this project. The aim for literature review is to get a clearer information and perceptive in developing Secure Text Transfer via Bluetooth Using Hybrid Encryption. So, this chapter will explain on all information needed for this project. The firstly section in this literature review will descript the concept for this project. The main concepts of this security are Secure Text Transfer via Bluetooth Using

Hybrid Encryption. This section includes the definition of security, file transfer, and Bluetooth technology.

Besides that, in this chapter also will be described about the basic Bluetooth security, techniques, Bluetooth security risk, and the existing security and vulnerabilities in Bluetooth. The technique section explains the technique will use in this project, the type of algorithm and the type of programming languages. In Bluetooth security risk section explains the type of security risk in Bluetooth. This section explains detail about it. The last sections discuss the existing security and vulnerabilities in Bluetooth. This section shows the Bluetooth version and its vulnerabilities.

2.2 The Concept of the Project

There are several concepts that are needed to give clearly defined about this project. The first concept is security. The next concept is file transfer and the last concept is Bluetooth technology.

2.2.1 The Concept of Security

According to the web pages, security is the degree of protection against danger, damage, loss, and crime. Security is important things for everyone whether student, lecturer or professional person. For company, the security is very important to secure the important things. The Institute for Security and Open Methodologies (ISECOM) defines that the security as a form of protection where a separation is created between the assets and the threat. This includes but is not limited to the elimination of either the asset or the threat. Security was defined as a national study in a United Nations study (1986), so any countries can develop and progress safely.

Security can be compared related to the concepts of safety, continuity, and reliability. The difference between security and reliability is that security must take into account the actions of people attempting to cause destruction.

Table 1 - Module Security Level Specification File Transfer

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Security Requirements Section	Level
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Safety is freedom from any danger or from liability to any danger or harm, and safeness. The quality of making safe or secure, or of giving confidence, justifying trust, insuring against harm or loss. In simple word, the word reliable to mean that something is dependable and that it will give the same outcome every time. The reliability is the ability of an apparatus, machine, or system to consistently perform its intended or required function or mission, on demand and without degradation or failure.

In Bluetooth security procedures, it includes of authorization, authentication and optional encryption. Authentication is proving the identity of a computer or computer user, or in Bluetooth case, proving the identity of one piconet member to another. Authorization is the process of denying access to a network resource. Encryption is the translation of data into secret code that can't be read by unauthorized person. It is used between Bluetooth devices so that eavesdroppers cannot read its contents.

2.2.2 The Concept of File Transfer

File transfer is the movement of one or more file from one location to another location.. An electronic stored file can be moved by physically moving the electronic storage medium, such as a computer diskette, hard disk, or compact disk from one place to another place or by sending the files over a telecommunications medium like Bluetooth, wireless or infrared. On the Internet, the File Transfer Protocol (FTP) is use as a common way to transfer a single file or a relatively small number of files from one computer to another.

File Transfer Protocol (FTP) is a standard network protocol are used to transfer files from one location to another location over a TCP based network, such as the Internet. File Transfer Protocol is built on a client server architecture and utilizes separate control and data connections between the client and server. FTP users may authenticate themselves using a clear text sign in protocol but can connect anonymously if the server is configured to allow it.



Figure 2.0: File Transfer

2.2.3 The Concept of Bluetooth Technology

The name of Bluetooth is taken from the 10th century Danish King Harald Blatand Harold Bluetooth in English. During the formative stage of the trade association a code name was needed to name the effort. King Blatand was instrumental in uniting warring factions in parts of what is now Norway, Sweden, and Denmark. The Bluetooth technology is designed to allow communication between different devices like computer - mobile phone and computer - camera[10].



Figure 2.1: Symbol Of Bluetooth

Bluetooth wireless technology is the most widely supported, versatile and it is the secure wireless standard on the market today. Bluetooth works in the open 2.4 GHz ISM band and now found in any products such as input devices, printers, medical devices,

VoIP phones, white boards and surveillance cameras [10]. 20 years ago, the only way to connect computer together for sharing information and resources is through cables from one computer to other computer. This can be not only cumbersome to set up, but it can get messy real quick. Bluetooth provide a solution to this problem by providing a cable free environment. The cost to transfer a file also become less [3].

Bluetooth can form ad hoc networks of several devices, called piconets. When the first Bluetooth connect, master that initiates the connection and the others are slaves devices. One connection can have maximum seven actives devices and one slaves devices. All communication within a piconetneeds goes through thepiconet master. When two or more piconets together, they will become scatternet. It can be used to eliminate Bluetooth range restrictions [10].

2.3 Basic Bluetooth Security



Figure 2.2: Bluetooth Security

In Bluetooth standard, there are 3 basic security services:

2.3.1 Authentication

Authentication is verify the identity of communicating devices like Bluetooth and the user of authentication is not provided natively by Bluetooth Karen [13].

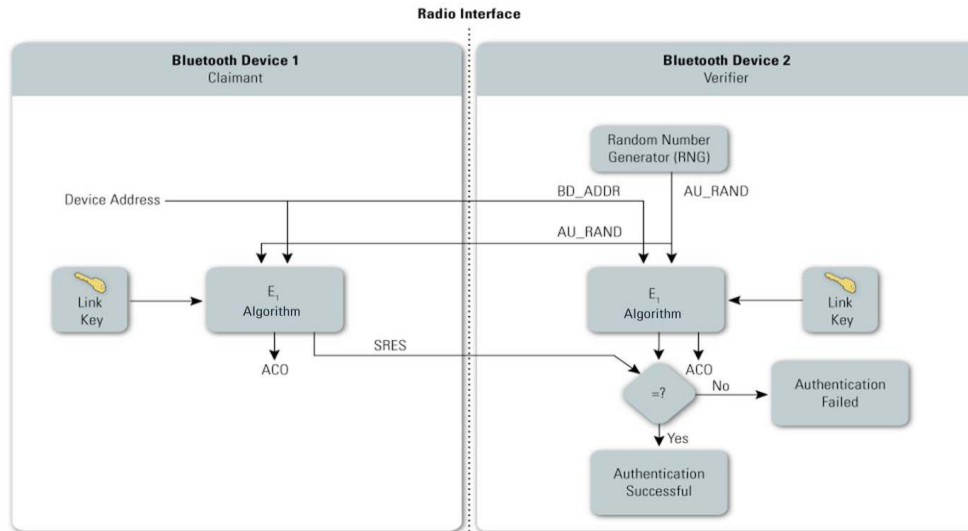


Figure 2.3: Authentication Process

The steps in the authentication process are as follows:

- **Step 1.** The verifier transmits a 128 bit random challenge (AU_RAND) to the claimant.
- **Step 2.** The claimant uses the E_1 algorithm to compute an authentication response using his unique 48 bit Bluetooth device address (BD_ADDR), the link key, and AU_RAND as inputs. The verifier performs the same computation. Only the 32 most significant bits of the E_1 output are used for authentication purposes. The remaining 96 bits of the 128 bit output are known as the Authenticated Ciphering Offset (ACO) value, which will be used later to create the Bluetooth encryption key.
- **Step 3.** The claimant returns the most significant 32 bits of the E_1 output as the computed response, SRES, to the verifier.
- **Step 4.** The verifier compares the SRES from the claimant with the value that it computed.
- **Step 5.** If the two 32 bit values are equal, the authentication is considered successful. If the two 32 bit values are not equal, the authentication has failed.

2.3.2 Confidentiality

Confidentiality is preventing information access by unauthorized user caused of eavesdropping by ensure that only authorized devices can access and view the data [13]. Bluetooth technology has three Encryption Modes, but only two of them actually provide confidentiality. The modes are as follows:

- **Encryption Mode 1**-No encryption is performed on any traffic.
- **Encryption Mode 2**-Individually addressed traffic is encrypted using encryption keys based on individual link keys, broadcast traffic is not encrypted
- **Encryption Mode 3**-All traffic is encrypted using an encryption key based on the master link key.

2.3.3 Authorization

The last basic security service is authorization. Authorization is allowing the control of resources by ensuring that device is authorized to use services before the it transfer a file[13].

2.4 Techniques

The concept of securing messages through cryptography has a long history. Julius Caesar was created one of the earliest cryptographic systems to send military messages to his generals [11]. The cryptography is the art of protecting information by changing it into an unreadable text, called cipher text. Only the person who has a secret key can decrypt the message into readable text. Encrypted messages can be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

Cryptography is used to protect e-mail messages, credit card information, corporate data and other things. Encryption systems used what is known as symmetric cryptography. Symmetric cryptography uses the same key to encryption and decryption the text. Using symmetric cryptography, it is safe to send encrypted messages without any

fear of interruption by unauthorized user. A major advance in cryptography occurred with the invention of public-key cryptography. The primary feature of public-key cryptography is that it removes the need to use the same key for encryption and decryption. With public-key cryptography, keys come in pairs of matched “public” and “private” keys. The public portion of the key pair can be distributed in a public manner without compromising the private portion, which must be kept secret by its owner.

Table 2 : Symmetric versus Asymmetric

Characteristic	Symmetric	Asymmetric
Key used for encryption / decryption	Same key is used	One key used for encryption and another different key is used for decryption
Speed of encryption / decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size	More than original clear text size
Key agreement / exchange	A big problem	No problem at all
Number of keys required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue	Same as the number of participants, so scales up quite well.

2.4.1 Hybrid Encryption

In this project use the hybrid encryption method. Hybrid encryption is a method of encryption that combines two or more encryption schemes and include a combination of symmetric and asymmetric encryption to take the advantages of the strengths of each of the encryption. Encryption algorithm is the algorithm to translate of data into a secret code that can't read by unauthorized user and this is the efficient way to achieve data security. Decryption is the process of decoding data that has been encrypted into a format that can be read [2].

An encryption system in which the sender and receiver shared a onekey that will used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keys a public key to encrypt messages and a private key to decrypt the message. Symmetric key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric key cryptography is sometimes called secret key cryptography. The most popular symmetric key system is the Data Encryption Standard (DES) [2].

2.4.2 Type Of Algorithm

- Blowfish

Blowfish is a symmetric block cipher that can be used for encryption and secure the data. The blowfish keys 32 bits to 448 bits and that make it ideal for securing data. Blowfish was designed in year 1993 by Bruce Schneider as a fast, free alternative to existing encryption algorithm. Blowfish is unpatented and the license is free for all users. The example Blowfish algorithm is a Feistel Network, iterating a simple encryption 16 times.

The block size of Blowfish algorithm is 64 bits and key can be any length up to 448 bits [12]. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of text is very efficient on large

microprocessors. It is suitable for application where the key does not change often, like a communication link or an automatic file encryptor. It is significantly faster than most encryption algorithm when implemented on 32-bit microprocessor with large data caches.

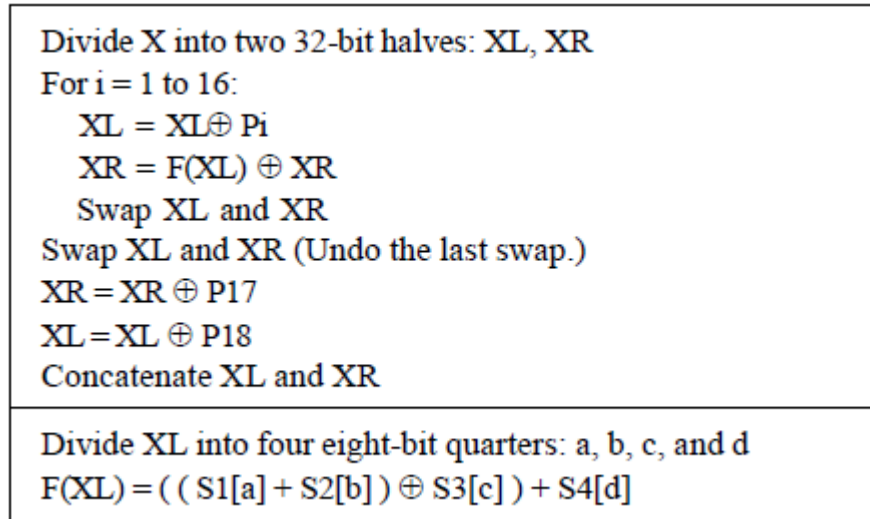


Figure 2.4: Blowfish algorithm [12].

- Twofish

From Wikipedia, Twofish is a symmetric key block cipher. It has a block size of 128 bits and key sizes up to 256 bits. Twofish was designed by Bruce Schneider, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson, the "extended Twofish team" who met to perform further cryptanalysis of Twofish and other AES contest entrants included Stefan Lucks, Tadayoshi Kohno, and Mike Stay.

Twofish is related to the earlier block cipher that is Blowfish algorithm. Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes). Twofish borrows some features from other designs. For the example are the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers. Twofish algorithm also uses the same Feistel structure as DES.

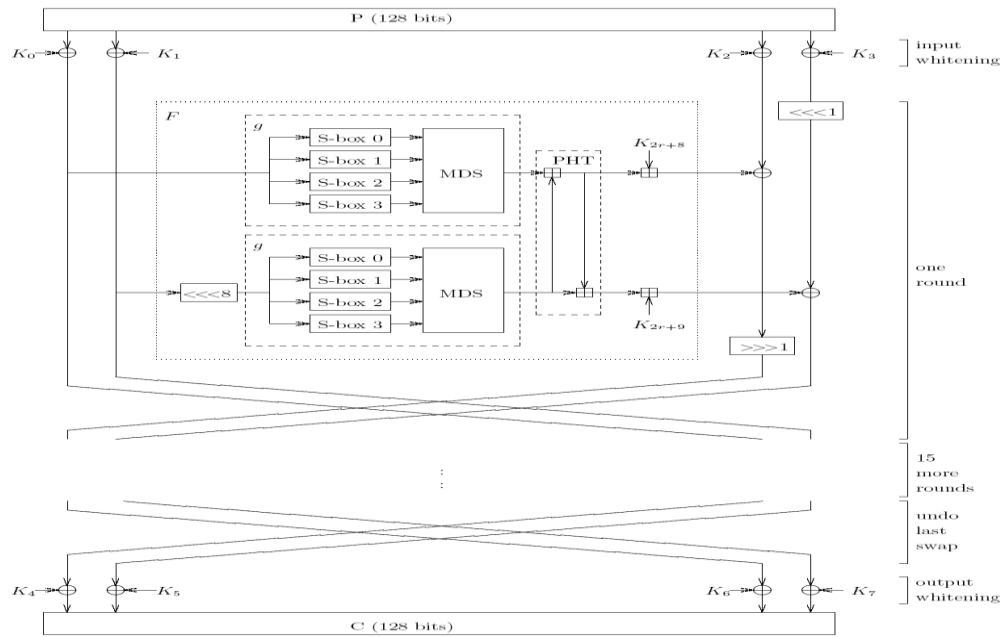


Figure 1: Twofish

Figure 2.5: Twofish

- Cast

Cast is encryption algorithm similar to earlier algorithm that is blowfish. It is designed by Stafford Taveres and Carlisle Adams, and name "CAST" represents the first letters of their names. CAST algorithm is gaining more and more popularity from other encryption algorithm. The cast encryption algorithm belongs to a class of private key block ciphers are composed of substitution boxes (S-boxes) with fewer input bits than output bits [9]. It has 2 type of cast algorithm that is Cast-128 and Cast-256. Cast 128 is licence free algorithm and it available for everyone. CAST-128 is a 12 or 16 round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits (but only in 8-bit increments) [15]. The full 16 rounds are used when the key size is longer than 80 bits. Components include large 8×32 -bit S-boxes based on bent functions, key-dependent rotations, modular addition and subtraction, and XOR operations.

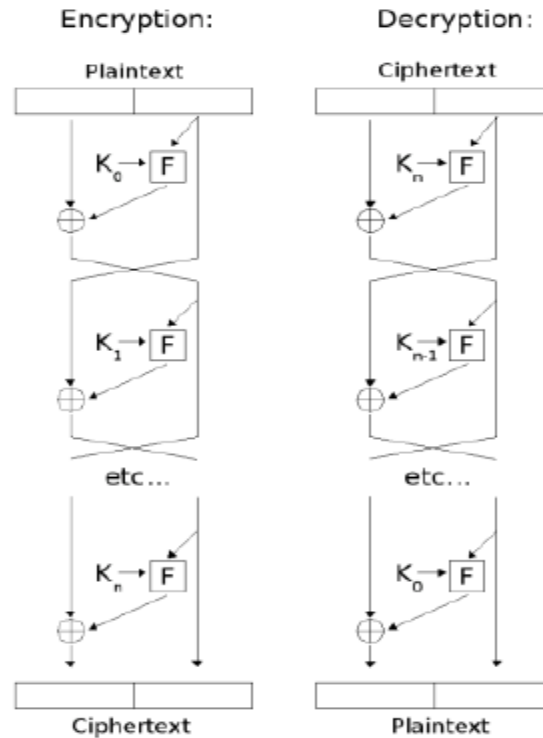


Fig. 1 CAST-128 Encryption and Decryption

There are three alternating types of round function, but they are similar in structure and difference only in the choice of the exact operation (addition, subtraction or XOR) at various points. The second cast algorithm is Cast-256. CAST-256 is a symmetric cipher designed in accordance with the CAST design procedure. It is an extension from CAST-128 cipher and has been submitted as a candidate for NIST's Advanced Encryption Standard (AES) effort. CAST-256 is a block cipher published in June 1998 [8].

However, it was not among the five AES finalists. It is an extension of an earlier cipher, CAST-128. Both were designed according to the "CAST" design methodology invented by Carlisle Adams and Stafford Tavares. Howard Heys and Michael Wiener also contributed to the design. CAST-256 uses the same elements as CAST-128, including S-boxes, but is adapted for a block size of 128 bits. Acceptable key sizes are 128, 160, 192, 224 or 256 bits. CAST-256 also composed of 48 rounds, sometimes described as 12 "quad-rounds", arranged in a generalised Feistel network. Similarly to the Data Encryption Standard (DES) and other proposed of block cipher, the Cast algorithm

consists of series of round of substitutions in order to achieve the “confusion” and “diffusion” principal [11].

- AES

The AES algorithm will be at least as strong as Triple DES and it is much faster Triple DES. Many security systems will always use both Triple DES and AES for at least next five years. After that, AES may supplant Triple DES as the default algorithm on most systems if it lives up to its expectations. But Triple DES will be kept around for compatibility reasons for many years after that. So the useful lifetime of Triple DES is far from over, even with the AES near completion. For the foreseeable future Triple DES is an excellent and reliable choice for the security needs of highly sensitive information.

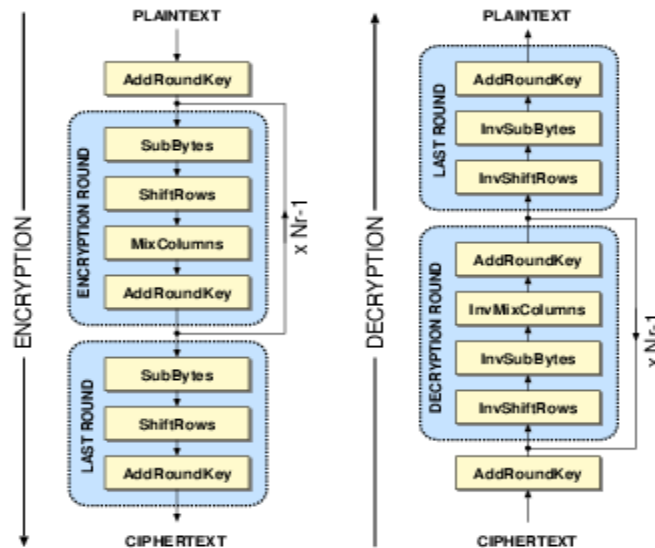


Figure 2.6: Basic Structure of AES Algorithm

- Substitution Cipher

Substitution cipher is a method of encryption by which units of plaintext are replaced with cipher text. The receiver decipheres the text by performing an inverse substitution to get the plain text.

There are a few types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher. Then if a cipher that operates on larger

groups of letters is termed polygraphic cipher. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the cipher text.

- Data Encryption Standard (DES)

The Data Encryption Standard (DES) was developed by an IBM team around 1974 and adopted as a national standard in 1977. Triple DES is a minor variation of this standard. Triple DES runs three times slower than standard DES, but is much more secure than DES if used properly. The procedure for decrypting text is the same as the procedure for encryption text, just a reverse process. Like DES, data is encrypted and decrypted in 64-bit chunks. There are some weak keys that someone should be aware of if all three keys, the first and second keys, or the second and third keys are the same, then the encryption procedure is the same as standard DES.

This situation must be avoided because it is the same as using a really slow version of regular DES. Triple DES widely use than DES because DES is so easy to break with today's rapidly advancing technology.

- MD5

Nowadays, the MD5 Algorithm is a widely used and it produces a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been use in a wide variety of security applications and is also commonly used to check data integrity. MD5 was design by Ron Rivest in 1991 to replace MD4.

However, it has since been shown that MD5 is not collision resistant. MD5 is not suitable for applications like SSLcertificates or digital signatures. In 1996, a flaw was found with the design of MD5and while it was not a clearly fatal weakness, cryptographers began recommending the use of other algorithms, such as SHA-1.

- RSA

The RSA algorithm is named after Ron Rivest, Adi Shamir and Len Adleman, who developed it in 1977. The basic technique was discovered in 1973 by Clifford Cocks of CESG (part of the British GCHQ) but this was a secret until 1997. The patent taken out by RSA Labs has expired. The RSA cryptosystem is the most widely-used public key cryptography algorithm in the world. It can be used to encrypt a text without exchanging a secret key separately.

The RSA algorithm can be used for public key encryption and digital signatures. Its security is based on the difficulty of factoring large integers. Party A can send an encrypted message to party B without any prior exchange of secret keys. A just uses B's public key to encrypt the message and B decrypts it using his private key, which only he knows. RSA can also be used to sign a message. A can sign a message using their private key and B can verify it using A's public key [16].

- KIST

The next algorithm is Kist. This algorithm uses an asynchronous key sequence and a splay tree. It is very efficient in the usage of both space and time. Some elements for security have been tested and it is done. Kist are composed of key insertion and splay tree encryption. Splay trees were first described in 1983 by Sleator and Tarjan and the details were presented in 1985 [7].

Splay trees were originally intended as self-balancing binary search trees with the property that recently accessed nodes are quick to access again. The difference between a compression splay tree and a search splay tree is that the compression tree does not require a lexicographic ordering of the nodes that simplifies the algorithm [7]. Kist algorithms have some characteristic and advantages, that is:

- i. Asynchronous key sequences were used.
- ii. A splay tree is used so that the substitution is dynamic.
- iii. The splay encryption is fast and it uses small spaces.
- iv. Cipher texts are composed in most cases

- v. The block size of the plain text and keys size are flexible.
- vi. It is good for message integrity [7].

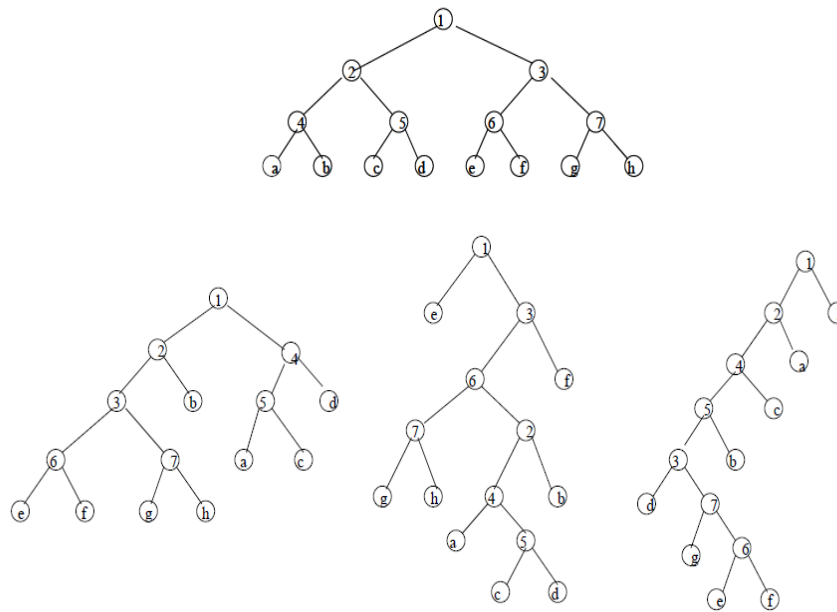


FIGURE 2.7: SMALL EXAMPLE OF SPLAY [7].

Table 3 : COMPARISON BETWEEN ALGORITHM [1].

Characteristic	BLOWFISH	TWOFISH	DES	MD5	AES
The block size	64 bits to 448 bits	128 bits	64 bits	128 bits	128 bits
Algorithm Structure	Feistel Network	Feistel Network	Feistel Network	Feistel Network	Substitution-Permutation Network
The key size	32 bits to 448 bits	18,192,256 bits	56 bits	128 bits	128,192,256 bits
Rounds	16	16	16	4	10,12 or 14

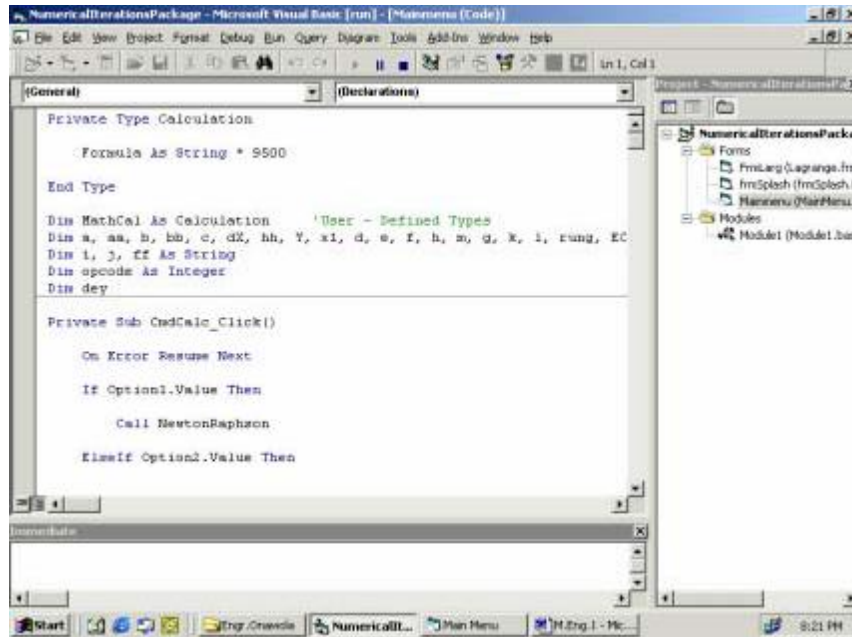
2.4.3 Programming Languages

- Visual basic

Visual basic is the basic programming languages and it also known as vb. It is a Microsoft Window programming language, visual basic program are created in an Integrated Development Environment (IDE), which allows the programmer to create run and design Visual basic programs easily. It's also allowing a programmer to create a programs in a fraction of time that normally takes to code programs without using IDEs. The wide spread use of BASIC Language with various types of computer led to many enhancement to the languages with the development of Microsoft Windows Graphical User Interface (GUI) in the late 1980's and the early 1990's

Visual basic is the most widely uses RAD language. Rapid Application Development (RAD) is the process of rapidly creating an application. Visual Basic provides a useful feature such as Graphical User Interface(GUI), events handling access to Win 32 API, Object-oriented features, error handling, structured programming and much more. Before Visual Basic appeared, developing Microsoft windows based application very difficult and cumbersome process. Visual basic greatly simplifies window application development. A few programming languages are text based and text based languages which do not allow user to work directly with GUI but visual basic is a graphical based language which allows user to work directly with GUI. Graphical based language can be used to develop windows program quickly.

Visual Basic have a disciplined to writing programs that are clearer than unstructured programs, easy to test, debug and can be easily modify. It allows for the creation of powerful and professional looking application with less time and coding. It allows for strong typing that has wide variety of input data types and support Rapid Application Development (RAD). It has a complete editing and debugging facilities and has the ability to generate a Dynamic Link Libraries (DLL'S), it allows for easier management of document and it is easy to learn [6].



Example of code and design in visual basic

- Fortran

FORTRAN (Fortran Translator) was developed by IBM Corporation between 1954 and 1957. It used for scientific and engineering application that requires complex mathematical computation but it is a text base programming language [6].

- C-programming Languages

C- programming language was developed by Dennis Richie in 1972 at Bell laboratories. C language is a very popular language among the computer user, it was first used to develop the UNIX Operating system. C++ is an extension of C, developed by Bjarne Stroustrup in the early 1980's also at Bell laboratories. C++ provides a number of features that "spruce up" the C language has the capabilities for doing so called Object Oriented Programming (OOP). Many people believe that (OOP) can greatly improve the software development process C++ has become the dominant system implementation language [6].

```
int main()
int crypt;
int x,y;
int key;
char input;
{
printf("Do you want your characters encrypted [1] or decrypted [2]? \n");
scanf("%d", crypt);
printf("Enter a key");
scanf("%d", key);

while((x=getchar())!=EOF && crypt=1)
{
printf("Enter data to encrypt.\n");
fflush(stdin);
gets(input);
if(x >='A' && x <='Z')
{
if((y = x + key) <= 'Z')
putchar(y);
else
{
y = x - key;
putchar(y);
}
}
else if(x >='a' && x <='z')
{
if((y= x + key) <= 'z')
putchar(y);
else
```

```
{  
y = x - key;  
putchar(y);  
}  
}  
else  
putchar(x);  
}  
return 0;  
}
```

Example of code in c programming

- Java

Java was developed by SUN Micro system and it was released in 1995. Java is based on C and C++ and has a few features with C and C++. Java includes extensive libraries for doing multimedia, networking, multi reading graphics data base access and much more. Microsoft version of Java is called visual J++ many people believe that Java and visual J++ will be the most significant long-term competitor to Visual Basic [6].

2.4.4 Type of Application

- Standalone Application

A standalone or thick client refers to an application running on a desktop environment such as windows or Mac platforms. When the Graphical User Interface (GUI) was developed by Apple in the 1980s, it made it possible to do in an easier way on a desktop computer. The users could perform of the work without having to remember the commands. The thick client architecture, where the code runs on the client as well as the processing of data. With the spreading from internet the thin client model became more popular. The thin client also became popular because the standalone applications more complex and depended on third party controls.

One of the top arguments against thick clients is when it comes to deployment. Imagine if thousands of clients that must be updated. This is not an easy task and it takes a lot of time to update all clients. In the future this argument will no longer be used because Microsoft has come up with something called ClickOnce deployment. ClickOnce is a part of the .Net 2.0 Framework and will be further enhanced in the next version of Windows, code-named "Longhorn".

Another problem with a standalone application is the platform dependency. A thick client requires a local runtime environment. For example a Windows Form application will only run on a windows platform with the .Net framework installed.

These drawbacks are compensated with the ability to work offline. It is possible for the application to run offline but it can only work with local data due to the non existing internet connection. Because all computation is done on the computer that the application is running on, the amount of data transmitted over the internet is reduced. The client retrieves data from a data source, makes some computation on it and then sends it back to the server. In the case of web based application the data is passed back and forth between the client and the server each time a new calculation is to be done. If many clients are connected to the server at the same time this leads to allot of processing on the server and the power of the clients is not used [14].

- Web based application

The World Wide Web came to life in the early 1990s when CERN laboratory in Switzerland needed to distribute documents and graphics via the Internet. To run resources in the form of executable programs the CGI (Common Gateway Interface) was invented. The CGI allowed a web browser to execute resources on a web server. This took web sites to another level, what we could call web applications and made it possible to use far more logic than HTML could accomplish. The developers were able to accomplish standard data processing functionality such as database access and they could distribute it across the world.

As the World Wide Web grew users became more comfortable with using various applications on the web. The users did not have to run different programs for each function that they wanted to perform.

Before the web became dynamic the only thing that could be requested from a web server was static pages. Every line of the HTML page was written by the designer before it was placed on the web server. When a client requests a static page the server reads the request and finds the right page. The server then sends the requested page back to the client.

The development of building dynamic web pages led to a software program called application server. When the web server receives a request for a dynamic page, it passes this page to the application server. The application server reads the code on the page and finishes the page according to the instructions in the code. The page that is returned from the application server to the web server is static. The web server then sends this page back to the requesting browser.

An application server lets work with resources on the server, such as databases. It does not communicate directly with the database. It uses a database driver that acts as an interpreter to receive data from the database. The main advantage of a web based solution is that it is centralized. This has its advantages in easy update and deployment. The only requirements on the clients are that a web browser is installed and that the clients have an internet connection. The hardware on the server is often more powerful than the average client. Another advantage is that a web application is platform independent. The same software can be accessed through a web browser regardless of the client's operative system [14].

2.5 Bluetooth Security Risk

Bluetooth technology and associated devices are susceptible to general wireless networking threats such as denial of service attacks, eavesdropping, man-in-the middle, message modification and resource misappropriation. They are also threatened by more specific Bluetooth related attacks that target known vulnerabilities in Bluetooth implementation can provide attackers with unauthorized access to sensitive information and unauthorized usages of Bluetooth devices and other system or networks to which the devices are connected [15].

In Bluetooth technology also have several Bluetooth security risks.

- The first risk is Bluejacking. Bluejacking is the process of sending unsolicited messages or business cards to Bluetooth-enabled devices. This does not involve altering any data from the devices but nonetheless. Devices that are set in non-discoverable mode are not susceptible to Bluejacking. In order for Bluejacking to work, the sending and receiving devices must be within 10 meters of one another. While Bluejacking is usually not done with malicious intent, repetitive bogus messages can be annoying to the user and in some cases can render the product inoperable.
- Bluesnarfing is a method of hacking into a Bluetooth-enabled mobile phone and copying its entire contact book, calendar or anything else stored in the phone's memory. By setting the devices in non-discoverable it becomes significantly more difficult to find and attack the devices. However, the software tools required to steal information from Bluetooth-enabled mobile phones are widely available on the web and knowledge of how to use them is growing.
- The next level of sophistication in Bluetooth hacking is Bluebugging where the victim device is controlled by the attacker who sends commands to perform actions as if having physical access to the devices. This is a functionally analogous to Trojans. The tools for Bluebugging include ones that run off the PCs, which means laptops with high range Bluetooth connectivity, which makes things even worse.
- Lastly is Bluetooth phishing which typically means social networking in short range and possibility of harassment from the security point of view. Then there are programs for Bluetooth PIN code cracking as well.

2.6 Comparison Between Existing Applications

Table 4 : COMPARISON BETWEEN EXISTING SYSTEM

	VB Triple-DES File Encryption Utility using the TDEScipher 32-bit DLL	File Encryption and Encrypted text embedding in an image
The number of key bits used	56, 112 or 168 bits	40-128 bits
Type of algorithm	DES and Triple DES	RC4
The languages	Visual Basic	Visual C++
Type of Application	Standalone	Standalone

Table 5 : COMPARISON BETWEEN EXISTING APPLICATIONS AND SECURE TEXT TRANSFER VIA BLUETOOTH USING HYBRID ENCRYPTION

	VB Triple-DES File Encryption Utility using the TDEScipher 32-bit DLL	File Encryption and Encrypted text embedding in an image	Secure Text Transfer via Bluetooth Using Hybrid Encryption
The number of key bits used	56, 112 or 168 bits	40-128 bits	128 bits
Type of algorithm	DES and Triple DES	RC4	MD5, Substitution Cipher
The languages	Visual Basic	Visual C++	Visual Basic
Type of Application	Standalone	Standalone	Standalone

CHAPTER 3

METHODOLOGY

In this chapter will discuss about the methodology that will be using in the development of Secure Text Transfer via Bluetooth Using Hybrid Encryption. It also will briefly describe about the strategy and the techniques applied during carrying out the research.

3.1 System Development Life Cycle (SDLC)

The software development life cycle (SDLC) is the process of creating or altering software systems, and the models and methodologies that people use to develop these systems [1].

Every project must have the SDLC (Software Development Lifecycle). Choosing the right SDLC methodology for the project is as important to the success of the project as the implementation of any project management best practices. Choose the wrong software methodology will add time to the development cycle. Adding extra time to the development cycle will increase the project's budget and very likely prevent from delivering the project on time.

Choosing the wrong methodology can also hamper the effective management of the project and may also interfere with the delivery of some of the project's goals and objectives. Software development methodologies are another tool in the development shop's tool inventory; much like the project management best practices are tools in the project manager's tool kit.

3.1.1 Waterfall Model

Many System Development Life Cycle (SDLC) models have been created over the years, but the two most commonly in use these days. They are Waterfall Method and Agile Method [2]. For this project will use Waterfall Method as a guide to develop this project.

The waterfall model is sequential software development process, is which the process is flowing downwards like the waterfall. That the reason why it call as a waterfall design. The phases in the design are through the analysis, design, implementation, testing and maintenance. All this phase is relay on each other and the flow is like waterfall from the top to the bottom.

The advantages of waterfall design are the stages development cycle enforces discipline. Which every phase has a defined start and end point. Other than that, the progress can conclusively identified which tough the use of milestones by both vendor and client. The other advantages on waterfall design are the developing of the system of software will be more sequential because it will need to be done by phase. Waterfall designs also improve quality. This means by the phase that been design in the waterfall.

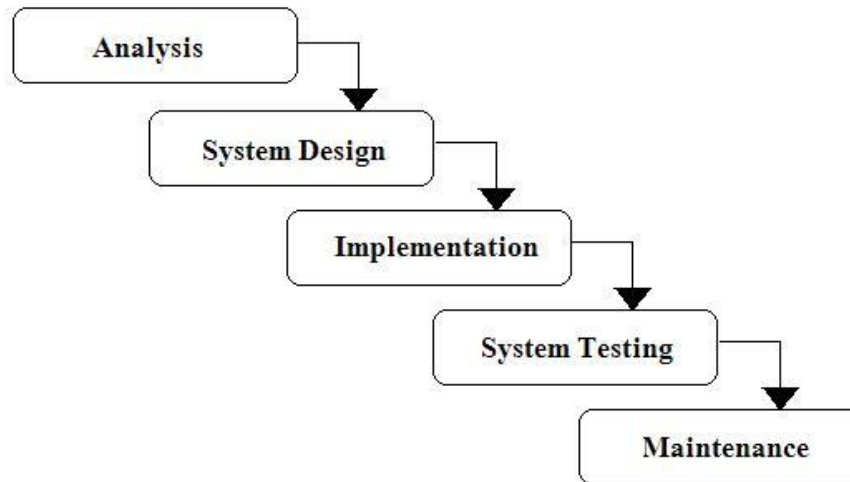


Figure 3.1 Example of SDLC Waterfall

3.1.1.1 Analysis And Definition

In this phase, the scope and the objective of the project is defined. The project which is Secure Text Transfer via Bluetooth Using Hybrid Encryption, main objective is to avoid the hackers from hack or interrupt the text and increase the security when using Bluetooth technology. Hybrid encryption method will avoid the text that transfer through Bluetooth easy hack by hackers.

This phase start defining the scope of this project which using non-video and non audio are in text transferring, using Hybrid encryption to make the text more secure and using Bluetooth technology.

The purpose of this project is to use Hybrid Encryption for encrypt the text before transfer via Bluetooth technology. Besides that, through this phase user will find that by using Hybrid encryption in secure text will make file more secure. The comparison of algorithm have discuss in Literature Review.

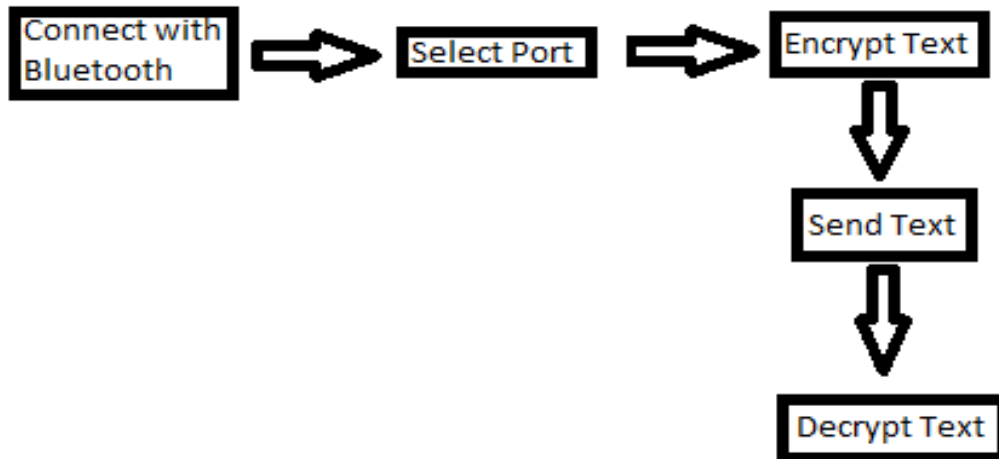


Figure 3.2: The Flow of project

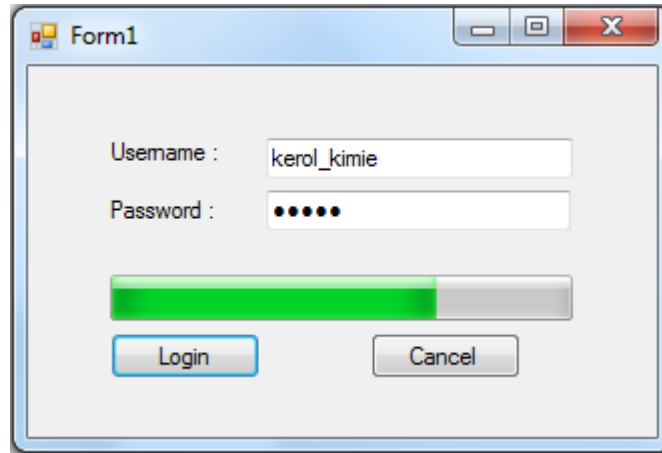
For this project, first the user must connect two laptops with the Bluetooth connection. Then, at the sender side the sender must select the port and at the receiver side also must do the same things. After that, the sender must encrypt the text and send it to receiver. The receiver will receive the text and decrypt the text.

3.1.1.2 System And Software Design

Design is the second phase in SDLC method whereby the features and the interface of the project system is created and design. System design helps in specifying hardware and system requirement and also helps in defining the overall system architecture. In designing the system, it is important making the flow chart to show the flow of the system.

3.1.1.2.1 Interface Design

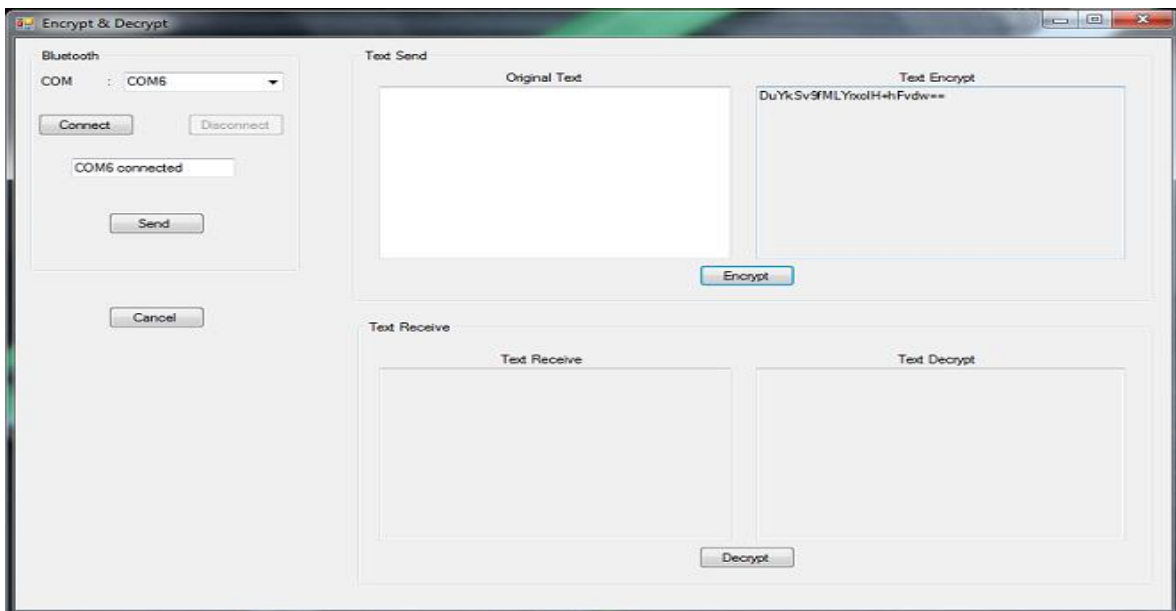
For this project, the interfaces created using Visual Basic. This interface starts with the description of the features and the operations of the system in details including the process diagram, workflow of system and screen shots of the interface. The logical designs for all interfaces of the project are illustrated in Figure 3.4 – Figure 3.5.



The screenshot shows a standard Windows-style window titled "Form1". It contains a login form with the following elements:

- A "Username" label followed by a text input field containing the text "kerol_kimie".
- A "Password" label followed by a password input field with six black dots.
- A green progress bar below the password field, approximately 60% full.
- Two buttons at the bottom: "Login" and "Cancel".

Figure 3.3: Logical Interface for Login the system



The screenshot shows a complex application window titled "Encrypt & Decrypt". It is divided into several sections:

- Bluetooth Section:** Located on the left, it includes a "COM" dropdown menu set to "COM6", "Connect" and "Disconnect" buttons, a status indicator "COM6 connected", and a "Send" button.
- Text Send Section:** Located in the top right, it contains two text areas: "Original Text" (empty) and "Text Encrypt" (containing the string "DuYkSv9FMLYxolH+hFvdw=="). Below these is an "Encrypt" button.
- Text Receive Section:** Located in the bottom right, it contains two text areas: "Text Receive" (empty) and "Text Decrypt" (empty). Below these is a "Decrypt" button.
- Control Section:** A "Cancel" button is located at the bottom left of the main interface area.

Figure 3.4: Logical Interface at Sender sides

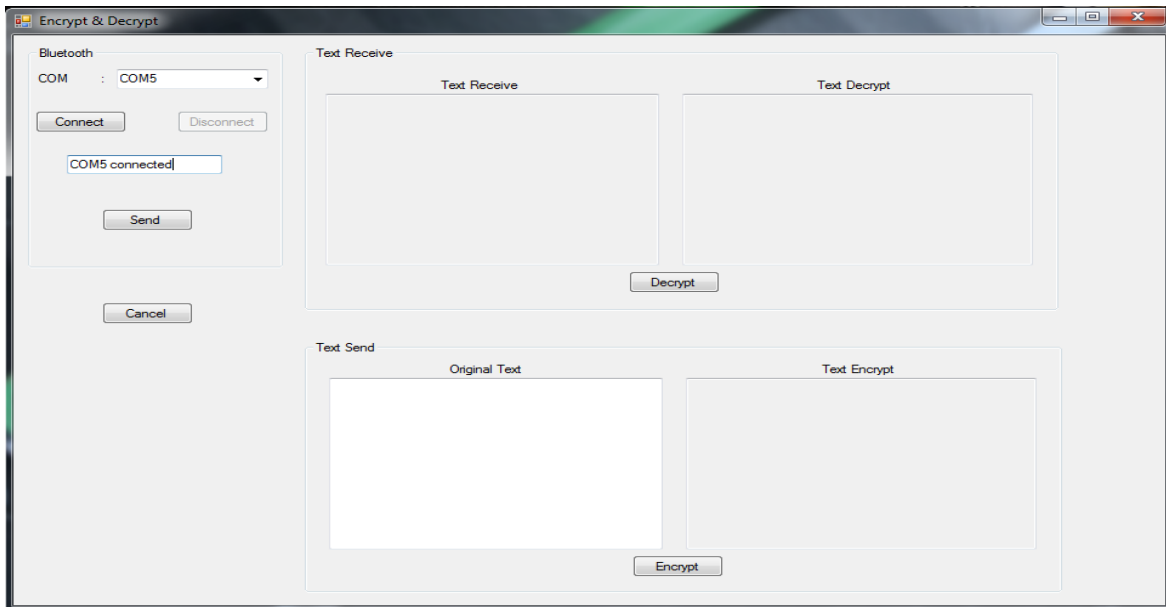


Figure 3.5: Logical Interface at Receiver sides

3.1.1.2.2 Flowchart of The System

For designing the system, it is important for making the flow chart of the system. The figures below are the flow chart of this Secure Text Transfer via Bluetooth Using Hybrid Encryption.

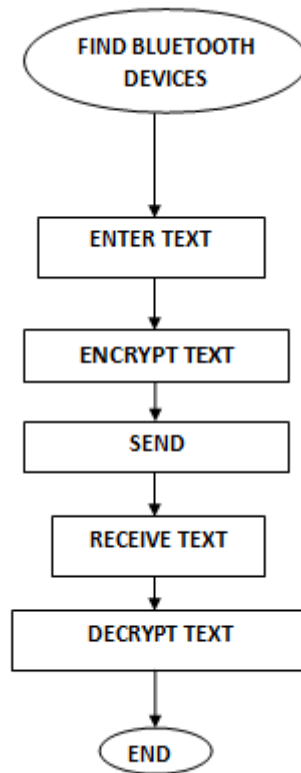


Figure 3.6: Flowchart of the System

First of all, the sender must find Bluetooth devices to send the text to receiver. The texts that will transfer using Bluetooth are write in the text box. The text transfers are non-video and non-audio. The sender must encrypt the text and send the text to receiver via Bluetooth. The receiver will receive the text and the receiver must decrypt the text to get the plain text. Besides that, the receiver also can send the encrypt text to sender and the sender also can decrypt the text. They are use the same process.

3.1.1.2.3 Use Case Diagram

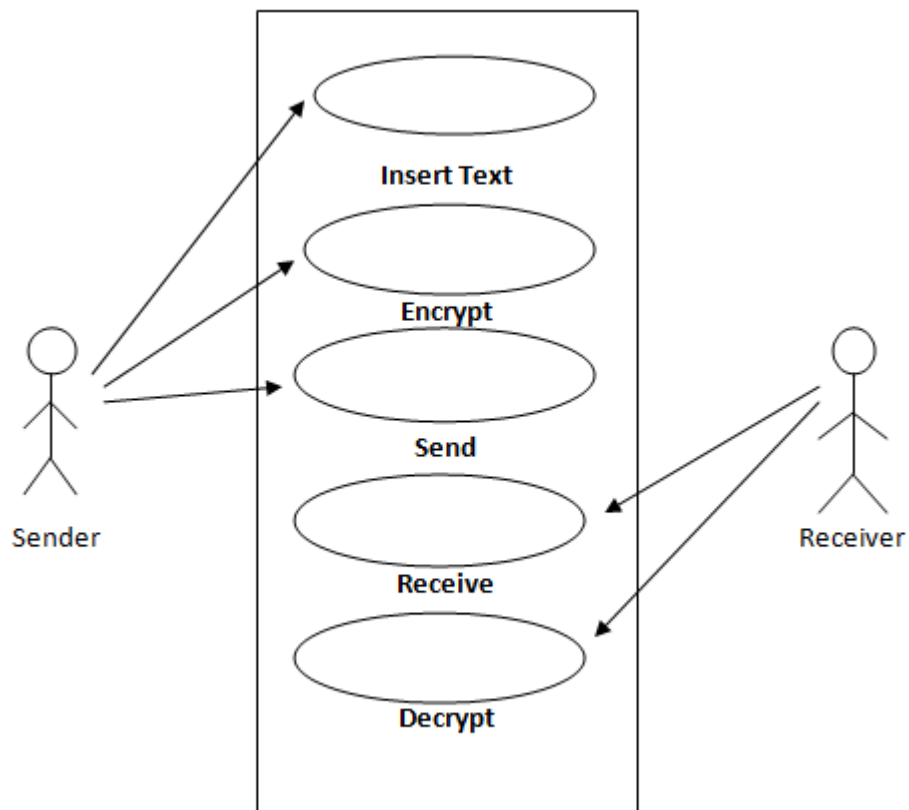


Figure 3.7: Use Case Diagram for the system

Figure 3.7 shows the use case diagram for the system. Based on the diagram, it shows that two people involve in the system. The users are sender. The sender needs to select the text. After that, the sender needs to encrypt the text and send to receiver. After the sender sends the text, the receiver receives the text. After that, the receiver needs to decrypt the file that was encrypt.

3.1.1.2.4 Context Diagram

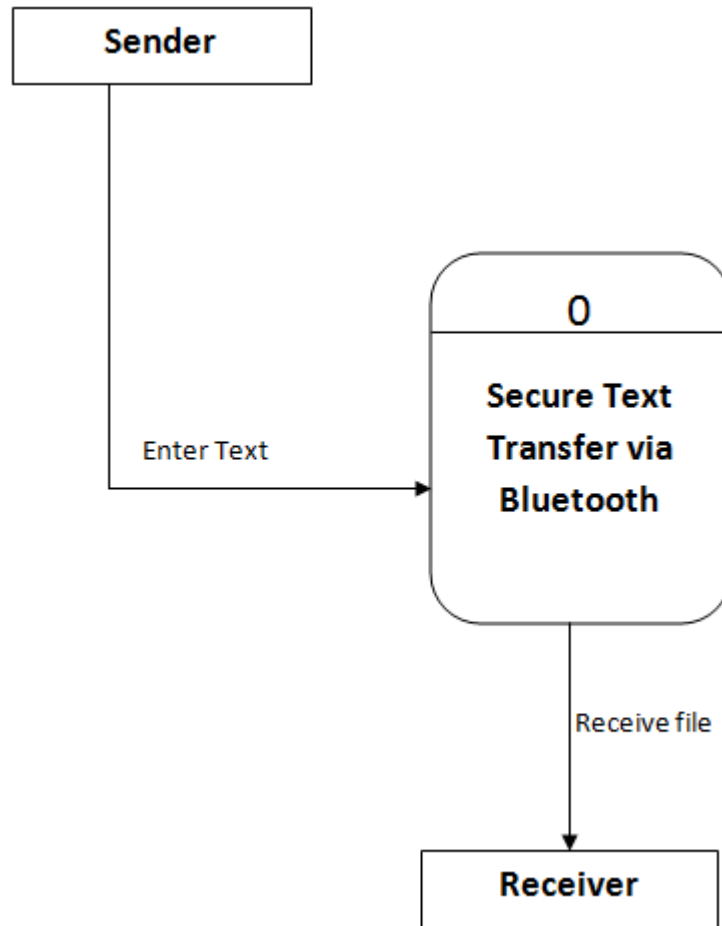


Figure 3.8: Context Diagram of the system

Figure 3.8 above shows the context diagram for the system. It is the overview of the system. Based on the figure 3.8, have two people that interact with the system. The first person is the sender which is the important person. The sender selects the text and encrypts the text. After that the sender will send the text to receiver. The receiver will receive the text and have to decrypt the text.

3.1.1.2.5 Level 0 Diagram

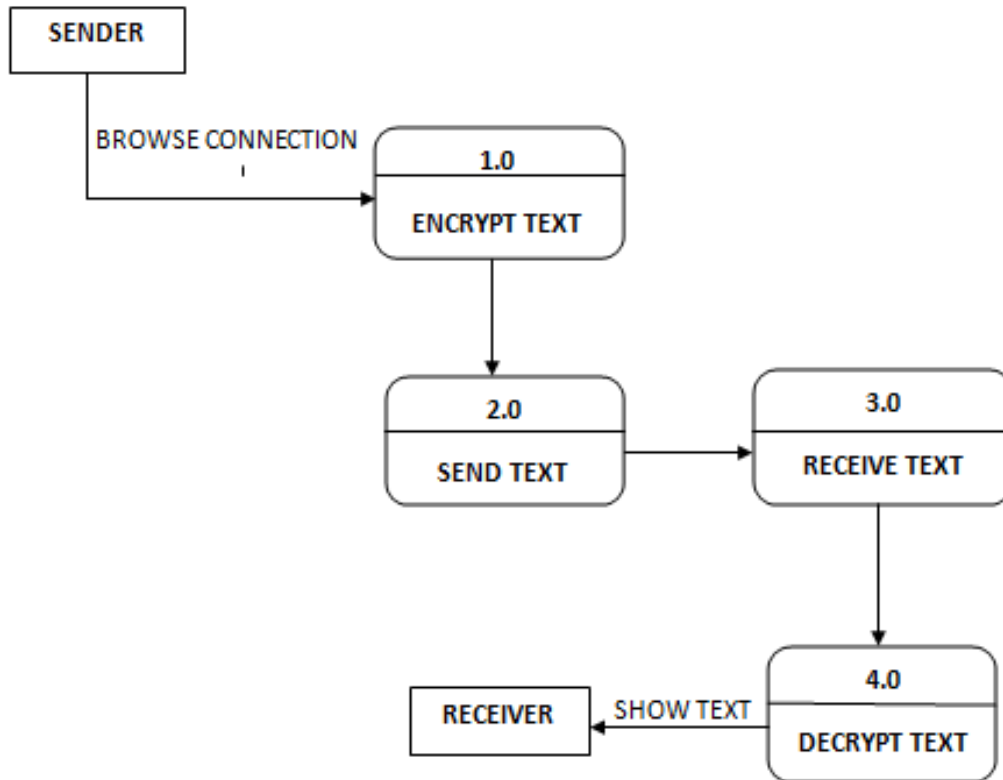


Figure 3.9: Level-0 Diagram

Based on level-0 diagram show above, the first entity is sender. At process 1.0, the sender needs to encrypt the text that will send to receiver. At 2.0 process, the sender will send the text to receiver. The process 3.0 starts with the receiver receive the text from sender. At 4.0 process, the receiver need to decrypt the text to get the plain text form sender. Then, the text that was decrypt show to the receiver.

3.1.1.3 Implementation

During this phase, the system of Secure Text Transfer via Bluetooth Using Hybrid Encryption is develop using Visual Basic Languages. The reason for using this kind of languages is because is easier than other languages and it easy to design the interfaces.

At this phase, the algorithms that will use are selected and build on Microsoft Visual 2008. The system will be develop based on encryption of file using hybrid encryption and transfer the file using Bluetooth.

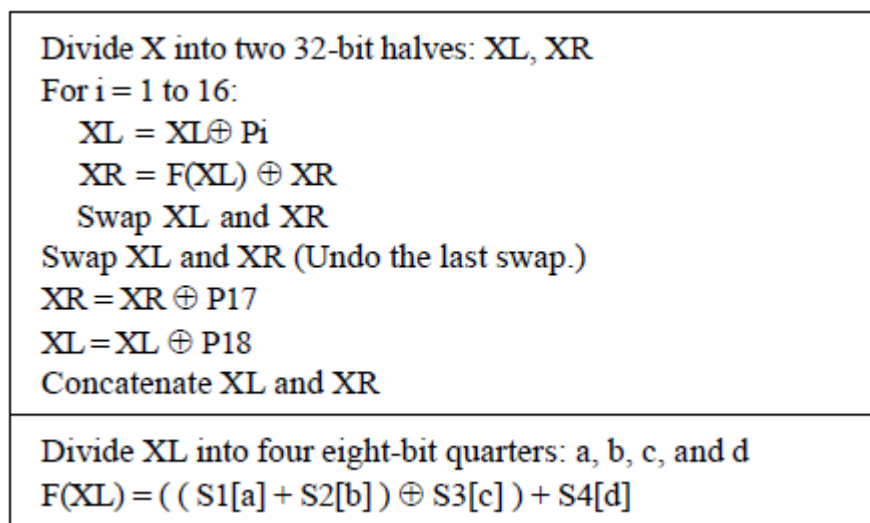


Figure 3.10: Blowfish algorithm

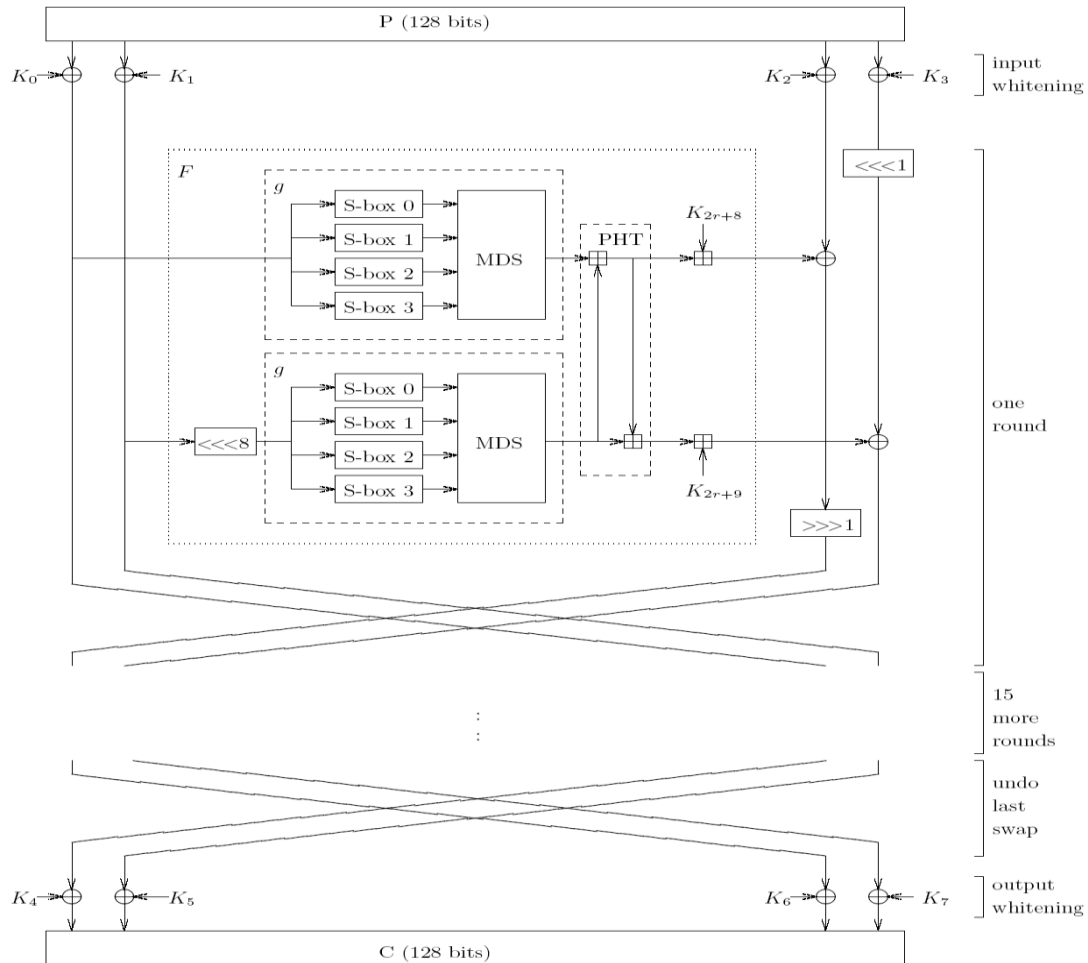


Figure 1: Twofish

Figure 3.11: Twofish

3.1.1.4 System Testing

After implementation phase, the testing phase is used to make sure the project created will work well in different environments. Testing is made to know the actual result and the expected result. The traditional way of testing usually needs testers so that the program will be exploited in different manners.

For this project, the testing section will be implemented after the system was developed. Testing the system will know if the system has the same problem or not. Besides that, with these activities, it will also know if the objective of the project is achieved or not. Testing will be executed by a programmer using Visual Basic. The programmer will try to run the project, if the project

execute well, the programmer can send the file using Bluetooth. If the projects have a problem, the programmer will develop or repair it again.

3.1.1.5 Operation and Maintenance

The final phase of this method is maintenance which is an information system is systematically repaired and improved. The organization should continuously monitor performance of the system to ensure that it is consistent with pre-established user and security requirement and that needed system modification are incorporated. Any changes from user or customer will be modified by programmers to reflect changing business conditions.

A programmer will make sure adjustment or changing reflect to the user enquiry. It will changes due to user request to make further improvement and if error was occur, the system must build again. The activities involved are transform request into changes, designing changes and implementation changes. The objective of this phase is to maximize return on the IT investment. A well design system will be reliable, maintainable and scalable.

3.2 System Requirements

This secure text transfer via Bluetooth is build at computer and this system needs some software and hardware. There are hardware and software that area already been determined in order to build this project.

3.2.1 Software Requirement

For developing the system, there have some software requirement:

Table 6 : Software Requirement

ITEM	DESCRIPTION
Microsoft Office Word 2007	Application to documents the paper work.
Microsoft Visual Studio 2008	Software to create the interfaces and develop the application.

3.2.2 Hardware Requirement

For developing the system, there have some hardware requirement:

Table 7 : Hardware Requirement

ITEM	DESCRIPTION
Laptop	Microsoft 7 Ultimate Intel Core2 Solo Processor RAM, 1.4GHZ 70 free hard disk space
USB Bluetooth Adapter	This Bluetooth adapter use for the laptop doesn't have Bluetooth application.

CHAPTER 4

SYSTEM DEVELOPMENT AND TESTING

4.1 Connect Bluetooth Device

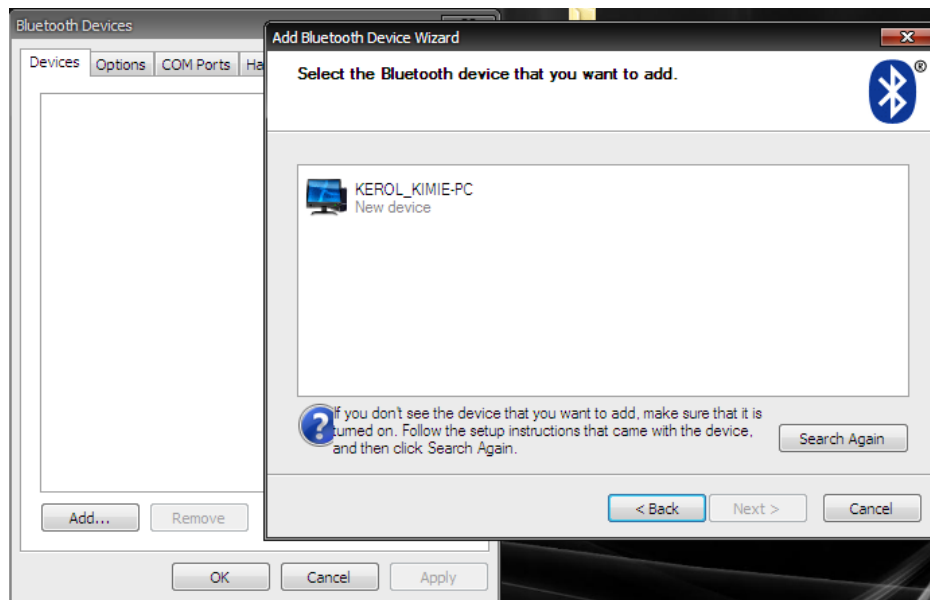


Figure 4.1 : Select Device

- Click button Add

- Click the devices name and click next
- If devices not appear, search it again by click button Search Again

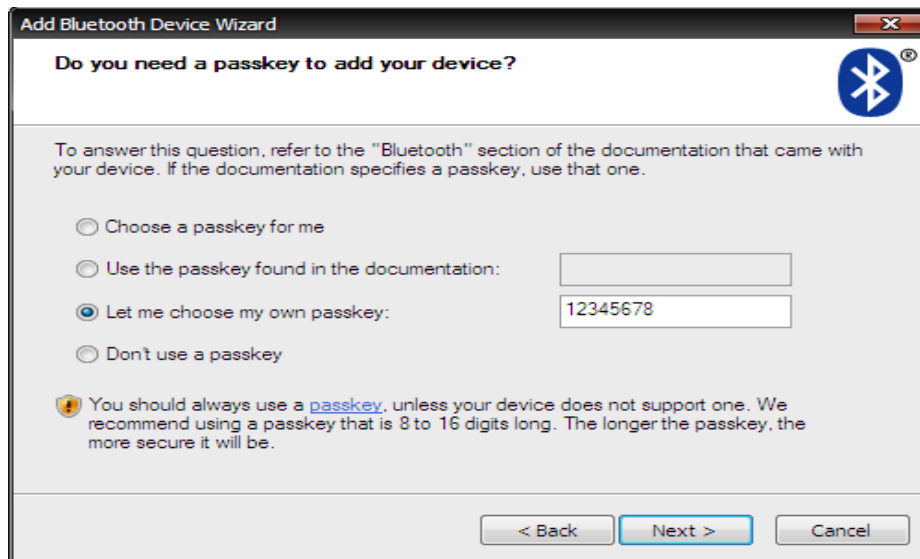


Figure 4.2 : Set key passkey

- To make only authorized user access the connection, choose 'Let me choose my own passkey'.
- Insert the key
- Click button Next

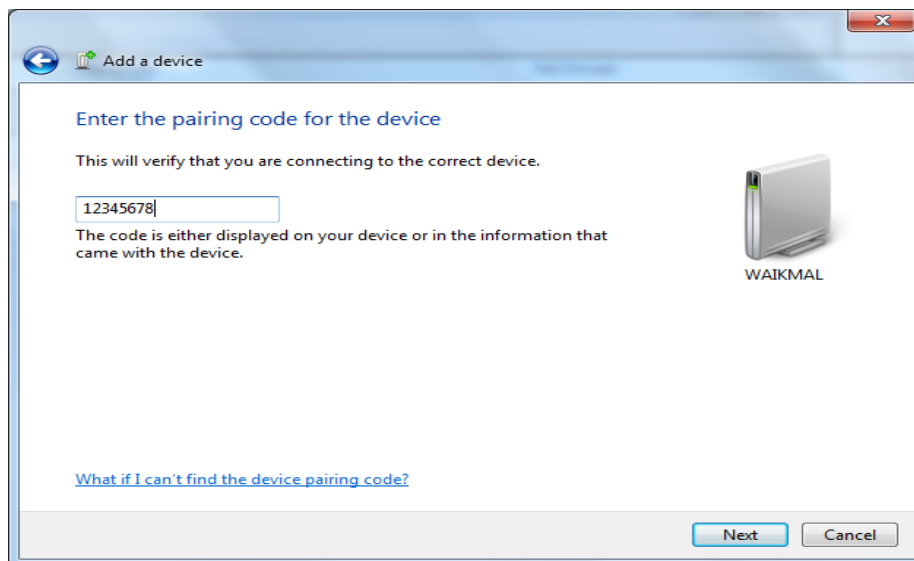


Figure 4.3: Enter pairing code

- The other sides must insert the key same with their partner to access the connection.
- Click button Next

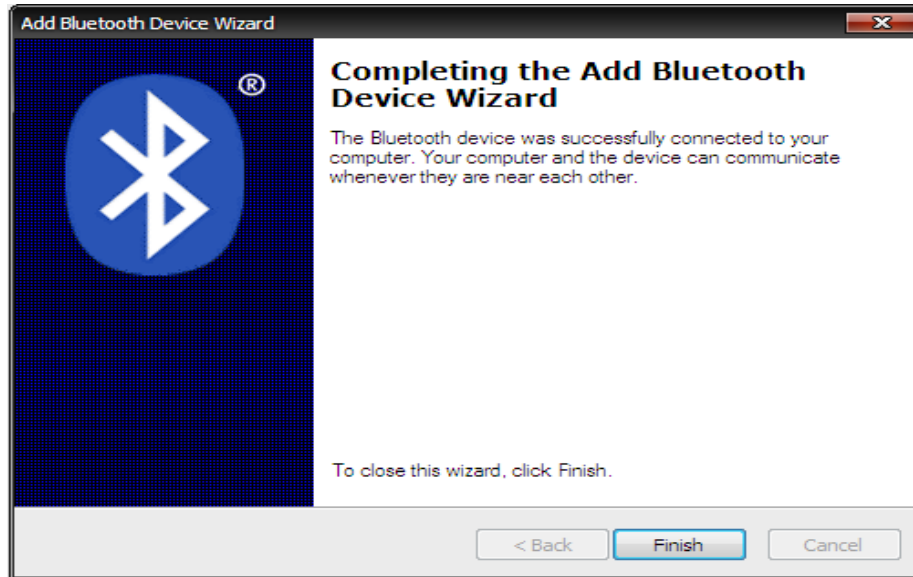


Figure 4.4 : Success interface

- Click button Finish
- The Bluetooth have been connected.

4.2 System Development

The figure 4.6 shows the login form. The user at sender sides and receiver sides need to register their username and password for the first use. They must click button first login form to enter their username and password. If they just click button login without insert username and password that was register, message box will appear to show the message they must enter username and password (Figure 4.7). Cancel button are use to stop the system.

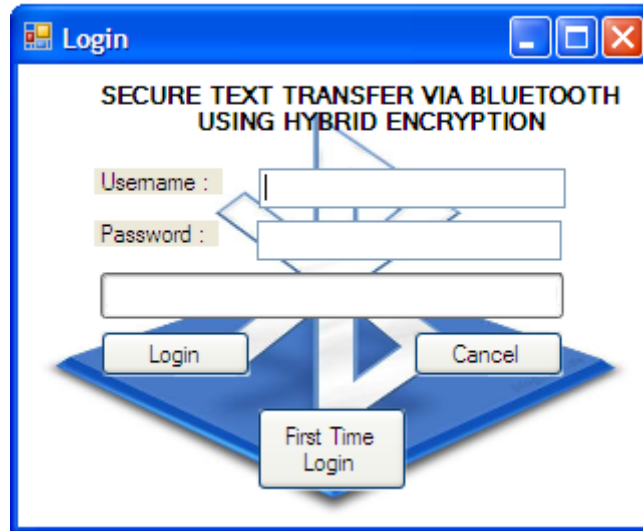


Figure 4.5 : Login Interface

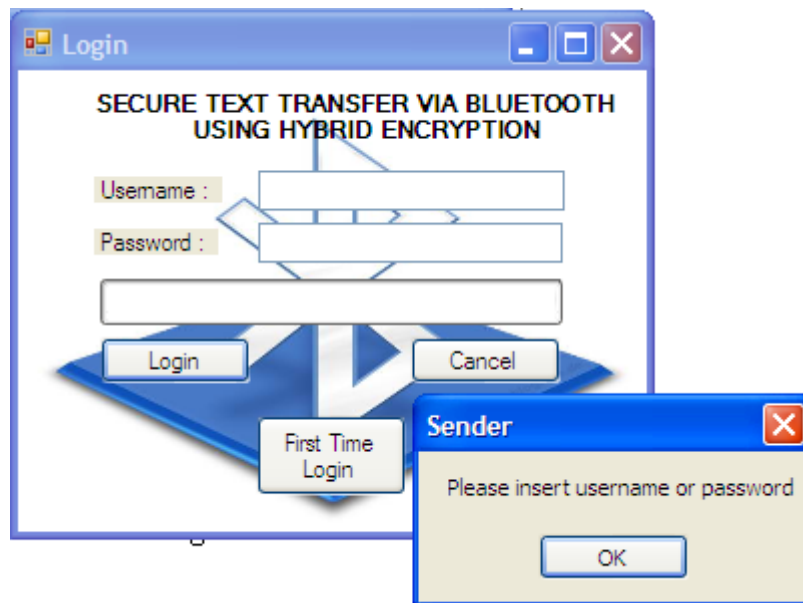


Figure 4.6 : Login Interface with message box

```

Public Class Form1
    Private Sub btnlogin_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnlogin.Click
        Try
            Dim login =
Me.UsernamePasswordTableAdapter1.UsernamePasswordString(txtusername.Text,
txtpassword.Text)
            If login Is Nothing Then
                MsgBox("Username or Password is not valid")
                txtpassword.Text = ""
                txtusername.Text = ""
            Else
                Timer1.Start()
            End If
        Catch ex As Exception
            MsgBox("Please insert username or password")
        End Try
    End Sub

```

For the first use, they must click first time login button at login form. After that, register form will appear (Figure 4.8). They must insert username and password in text box at register form. After they insert username and password, they must click register button and the message box will appear (Figure 4.9). If just click the button register without insert the username and password, message box will appear to tell them compulsory to insert username and password (Figure 4.10).



Figure 4.7: Register interface

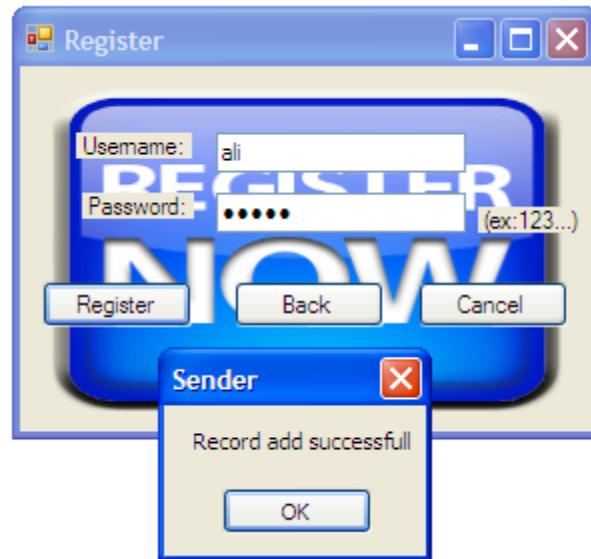


Figure 4.8: Register interface with message box success

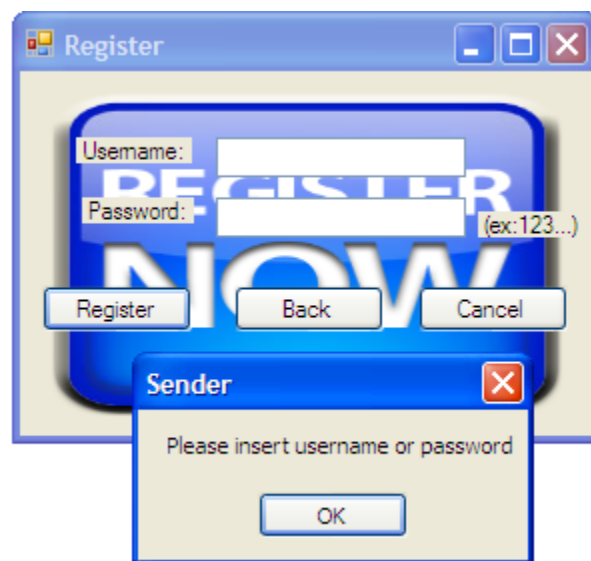


Figure 4.9: Register interface with message box username and password

```

Public Class Form4
    Private Sub btncancel_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btncancel.Click
        Me.Close()
    End Sub

    Private Sub btnregister_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnregister.Click
        Try
            Form1.UsernamePasswordTableAdapter1.Insert(0,
Me.txtusername.Text, Me.txtpassword.Text)
            MsgBox("Record add successfull")
            txtpassword.Text = ""
            txtusername.Text = ""
        Catch ex As Exception
            MsgBox("Please insert username or password")
        End Try
    End Sub

    Private Sub btnback_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnback.Click
        Form1.Show()
        Me.Hide()
    End Sub
End Class

```

After they have register for the first time, they can use their username and password and insert into username and password text box at login form. They must click button login to login into system.

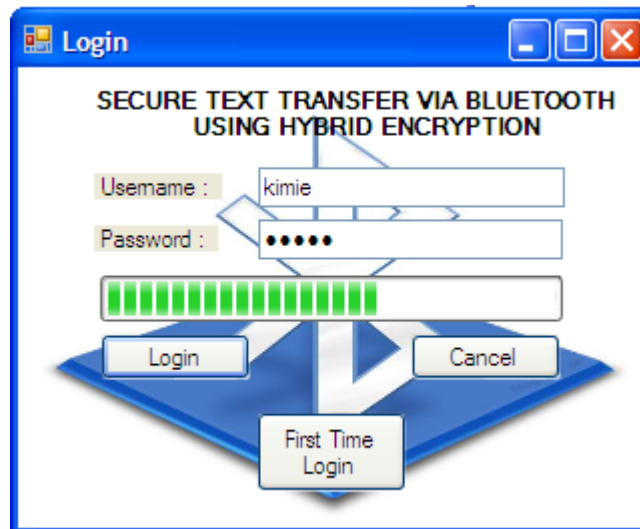


Figure 4.10: Login interface with username and password

At encrypt and decrypt form, they must select the com port at combo box. If they just click the button connect without insert the com port, the message box will appear (Figure 4.12). Message box also will appear if they just click button send without connect the com port first (Figure 4.13). The text will encrypt must write in original text at both sides (Figure 4.14). Then, they must click button encrypt to encrypt the text. The encrypt

text will appear at text encrypt in group box text send (Figure 4.15). To send the text, they must click button send. The receiver will receive the text send by sender at text receive in text Receive group box. Text receive can't read, so they must decrypt the text by click button decrypt. Decrypt text will appear at text decrypt text box.

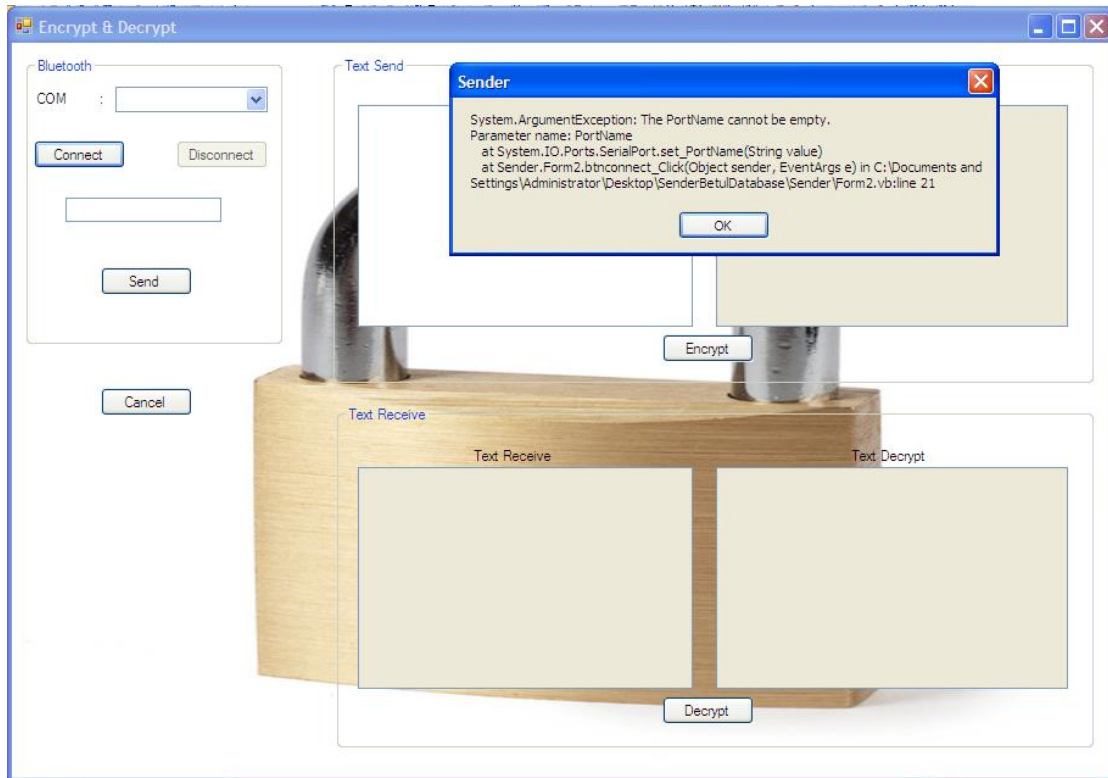


Figure 4.11: Encrypt & Decrypt interface with message box port can't empty

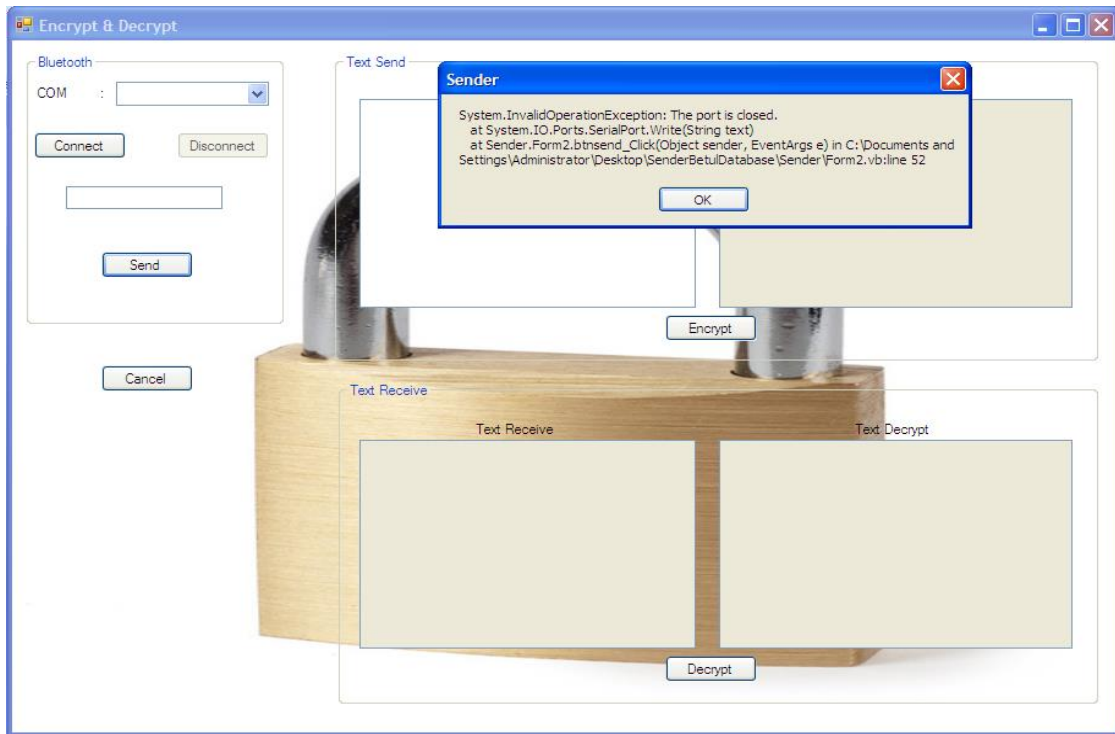


Figure 4.12 : Encrypt & Decrypt interface with message box port close

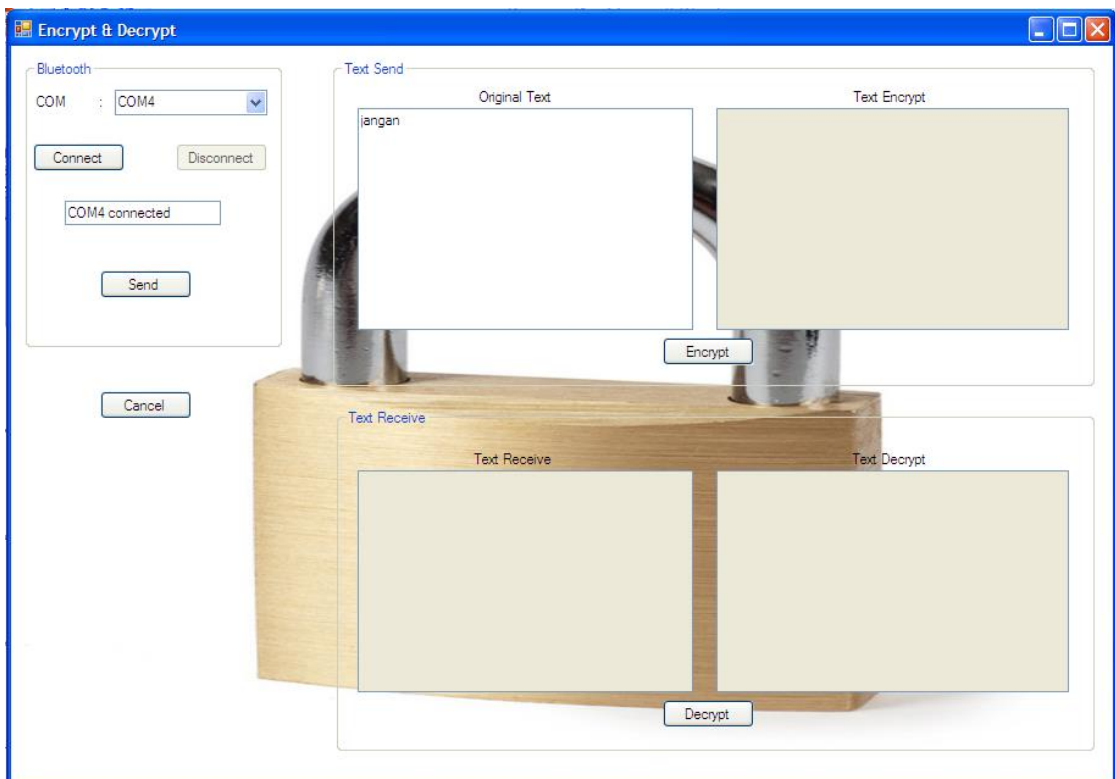


Figure 4.13 : Insert text to encrypt

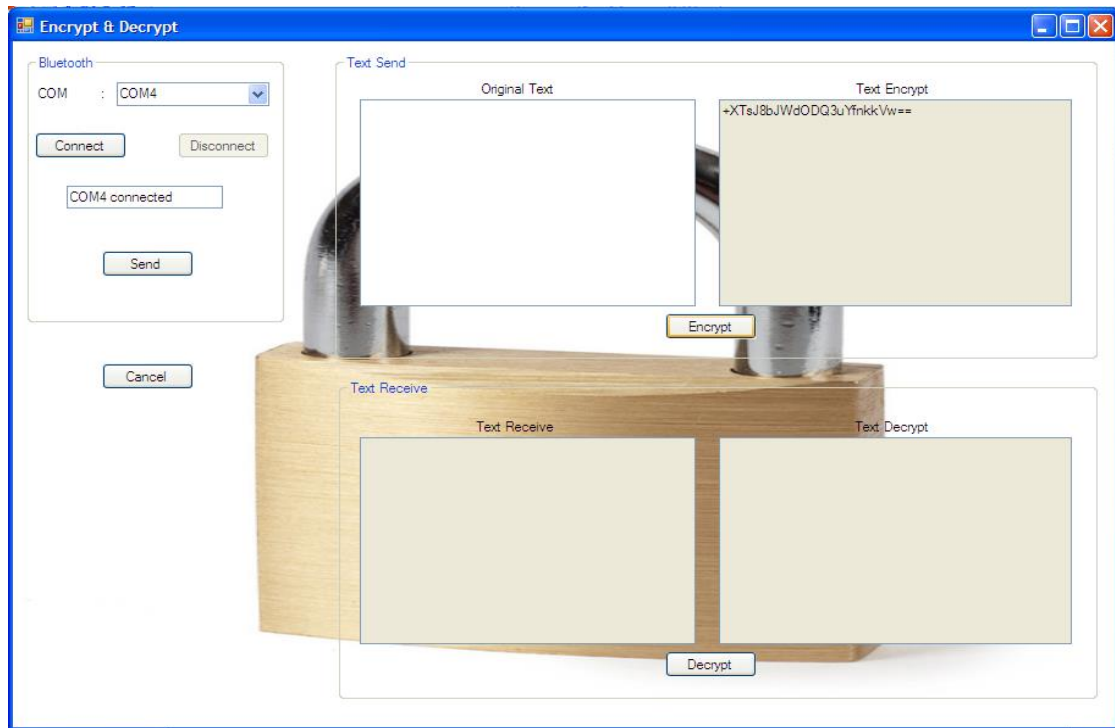


Figure 4.14 : Encrypt text

```
Imports System.Security.Cryptography
Public Class Form2
    'Object Creation
    Dim FuncCls As New CommonFunctionsCls ()
    Dim WithEvents serialPort As New IO.Ports.SerialPort
    Private Sub Form2_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load
        For i As Integer = 0 To
            My.Computer.Ports.SerialPortNames.Count - 1
                cmbcom.Items.Add(
                    My.Computer.Ports.SerialPortNames(i))
            Next
        btndisconnect.Enabled = False
    End Sub
    Public Delegate Sub myDelegate()
    Private Sub btnconnect_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnconnect.Click
        If serialPort.IsOpen Then
            serialPort.Close()
        End If
        Try
            With serialPort
                .PortName = cmbcom.Text
                .BaudRate = 96000
                .Parity = IO.Ports.Parity.None
                .DataBits = 8
                .StopBits = IO.Ports.StopBits.One
                '.Encoding = System.Text.Encoding.Unicode
            End With
            serialPort.Open()
            lblstatus.Text = cmbcom.Text & " connected."
            btnconnect.Enabled = False
            btndisconnect.Enabled = True
        Catch ex As Exception
            MsgBox(ex.ToString)
        End Try
    End Sub
End Class
```

```

Private Sub btndisconnect_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btndisconnect.Click
    Try
        serialPort.Close()
        lblstatus.Text = serialPort.PortName & " disconnected."
        btnconnect.Enabled = True
        btndisconnect.Enabled = False
    Catch ex As Exception
        MsgBox(ex.ToString)
    End Try
End Sub
Private Sub btncancel_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btncancel.Click
    Me.Close()
End Sub

Private Sub btnsend_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnsend.Click
    Try
        serialPort.Write(encrypttxt.Text & vbCrLf)
    Catch ex As Exception
        MsgBox(ex.ToString)
    End Try
    encrypttxt.Text = ""
End Sub

```

```

Private Sub btnencrypt_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btnencrypt.Click
    Dim a, b, c, d, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w,
x, y, z As String
    a = "a"
    b = "b"
    c = "c"
    d = "d"
    f = "f"
    g = "g"
    h = "h"
    i = "i"
    j = "j"
    k = "k"
    l = "l"
    m = "m"
    n = "n"
    o = "o"
    p = "p"
    q = "q"
    r = "r"
    s = "s"
    t = "t"
    u = "u"
    v = "v"
    w = "w"
    x = "x"
    y = "y"
    z = "z"
    encrypttxt.Text = inputtxt.Text
    encrypttxt.Text = Replace(encrypttxt.Text, a, "*")
    encrypttxt.Text = Replace(encrypttxt.Text, b, "!")
    encrypttxt.Text = Replace(encrypttxt.Text, c, "#")
    encrypttxt.Text = Replace(encrypttxt.Text, d, "$")
    encrypttxt.Text = Replace(encrypttxt.Text, f, "&")
    encrypttxt.Text = Replace(encrypttxt.Text, g, "^")
    encrypttxt.Text = Replace(encrypttxt.Text, h, "<")
    encrypttxt.Text = Replace(encrypttxt.Text, i, "(")
    encrypttxt.Text = Replace(encrypttxt.Text, j, ")")

```

```

encrypttxt.Text = Replace(encrypttxt.Text, k, "-")
encrypttxt.Text = Replace(encrypttxt.Text, l, "+")
encrypttxt.Text = Replace(encrypttxt.Text, m, "_")
encrypttxt.Text = Replace(encrypttxt.Text, n, "?")
encrypttxt.Text = Replace(encrypttxt.Text, o, "|")
encrypttxt.Text = Replace(encrypttxt.Text, p, "\")
encrypttxt.Text = Replace(encrypttxt.Text, q, "}")
encrypttxt.Text = Replace(encrypttxt.Text, r, "]")
encrypttxt.Text = Replace(encrypttxt.Text, s, "{")
encrypttxt.Text = Replace(encrypttxt.Text, t, "[")
encrypttxt.Text = Replace(encrypttxt.Text, u, ":")
encrypttxt.Text = Replace(encrypttxt.Text, v, ";")
encrypttxt.Text = Replace(encrypttxt.Text, w, "/")
encrypttxt.Text = Replace(encrypttxt.Text, x, "`")
encrypttxt.Text = Replace(encrypttxt.Text, y, "~")
encrypttxt.Text = Replace(encrypttxt.Text, z, ">")
encrypttxt.Text = FuncCls.EncryptPassword(encrypttxt.Text.Trim)
inputtxt.Text = ""
decrypttxt.Text = ""
End Sub

```

```

Private Sub btndecrypt_Click(ByVal sender As System.Object, ByVal e
As System.EventArgs) Handles btndecrypt.Click
    decrypttxt.Text = FuncCls.DecryptPassword(receivetxt.Text)
    Dim a, b, c, d, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w,
x, y, z As String
    a = "*"
    b = "!"
    c = "#"
    d = "$"
    f = "%"
    g = "^"
    h = "<"
    i = "("
    j = ")"
    k = " "
    l = "+"
    m = "-"
    n = "?"
    o = "|"
    p = "\"
    q = "}"
    r = "]"
    s = "{"
    t = "["
    u = ":"
    v = ";"
    w = "/"
    x = "`"
    y = "~"
    z = ">"
    decrypttxt.Text = decrypttxt.Text
    decrypttxt.Text = Replace(decrypttxt.Text, a, "a")
    decrypttxt.Text = Replace(decrypttxt.Text, b, "b")
    decrypttxt.Text = Replace(decrypttxt.Text, c, "c")
    decrypttxt.Text = Replace(decrypttxt.Text, d, "d")
    decrypttxt.Text = Replace(decrypttxt.Text, f, "f")
    decrypttxt.Text = Replace(decrypttxt.Text, g, "g")
    decrypttxt.Text = Replace(decrypttxt.Text, h, "h")
    decrypttxt.Text = Replace(decrypttxt.Text, i, "i")

```

```

decrypttxt.Text = Replace(decrypttxt.Text, j, "j")
decrypttxt.Text = Replace(decrypttxt.Text, k, "k")
decrypttxt.Text = Replace(decrypttxt.Text, l, "l")
decrypttxt.Text = Replace(decrypttxt.Text, m, "m")
decrypttxt.Text = Replace(decrypttxt.Text, n, "n")
decrypttxt.Text = Replace(decrypttxt.Text, o, "o")
decrypttxt.Text = Replace(decrypttxt.Text, p, "p")
decrypttxt.Text = Replace(decrypttxt.Text, q, "q")
decrypttxt.Text = Replace(decrypttxt.Text, r, "r")
decrypttxt.Text = Replace(decrypttxt.Text, s, "s")
decrypttxt.Text = Replace(decrypttxt.Text, t, "t")
decrypttxt.Text = Replace(decrypttxt.Text, u, "u")
decrypttxt.Text = Replace(decrypttxt.Text, v, "v")
decrypttxt.Text = Replace(decrypttxt.Text, w, "w")
decrypttxt.Text = Replace(decrypttxt.Text, x, "x")
decrypttxt.Text = Replace(decrypttxt.Text, y, "y")
decrypttxt.Text = Replace(decrypttxt.Text, z, "z")
receivetxt.Text = ""
End Sub

```

```

Private Sub DataReceived( _
ByVal sender As Object, _
ByVal e As System.IO.Ports.SerialDataReceivedEventArgs) _
Handles serialPort.DataReceived

    receivetxt.Invoke(New _
        myDelegate(AddressOf updateTextBox), _
        New Object() {})
End Sub
Public Sub updateTextBox()
    With receivetxt
        .Font = New Font("Garamond", 12.0!, FontStyle.Bold)
        .AppendText(serialPort.ReadExisting)
        .ScrollToCaret()
    End With
End Sub
End Class

```


CHAPTER 5

RESULT AND DISCUSSION

In this chapter, the output that the system produced will be discussed. The details about the outcome, assumption and the further for this system will also be discussed in this chapter. The discussion hopefully can give ideas and more benefits to the future developer in order to upgrade and enhance the performance and functionality of the system in future.

5.1 Results

The output of the Secure Text Transfer via Bluetooth using Hybrid Encryption will satisfy the following objectives:

- i. To ensure the true receivers only receive the text and access it.
 - To ensure the true receiver only receive the text, the sender need to insert the key in connection of Bluetooth. At the receiver site, the receiver need to insert the key same with sender.

- ii. To increase the security of the text.
 - Using Hybrid Encryption method to encrypt the text, this procedure will avoid the hackers from hack the text. This method will make file become more secure.
- iii. To develop 2 layer of encryption and decryption.
 - Two layers of encryption and decryption will make text become more secure. For the first layer, the text will encrypt with the first algorithm, then the text will encrypt again using the second algorithm.

This system will help the entire person who wants to send their text through Bluetooth using hybrid Encryption. This method will make the text become more secure to avoid from unauthorized user from hack the text

5.2 Discussion

5.2.1 Strength

- i. The text that was encrypt using Hybrid encryption will be more secure.
 - The technique use to encrypt the text is Hybrid Encryption. This technique will give more security to the text. The text that will encrypt will use two different type of encryption.
- ii. Only the true receivers can access the text.
 - During transfer the text via Bluetooth technology, the sender needs insert the key to send a text to ensure the right receiver receive the text. At the receiver site, the receiver needs to enter the same keys with sender to receive the text.
- iii. The receiver also can send the text to sender.
 - At receiver sides also have a button to send the text. Before the receivers send the text, receiver must encrypt the text first. At sender sides also have a button to decrypt the text send by receiver.

5.2.2 Weakness

- i. Can't encrypt and send audio and video.
 - This system can't encrypt and send audio and video because the capacity to send audio and video are large. So, the large amount of capacity send through Bluetooth will make the sending are slow or fail.
- ii. Use already Bluetooth device in Laptop
 - The connection between two laptop using Bluetooth device in laptop. This system only has a button to connect with Bluetooth and send the text via Bluetooth.
- iii. Need to install at sender devices and receivers devices.
 - This system need to install at sender device and receiver devices because encryption and decryption need to use the same algorithm.
- iv. Use a simple algorithm
 - In this system, the algorithm use is MD5 and substitution cipher. The combination between this two algorithm make the text become more secure but for substitution cipher it is old.

5.3 System Enhancement

Suggestion that would really make Secure Text Transfer via Bluetooth using Hybrid Encryption a better system are:

- i. Use a complex encryption algorithm and the algorithm new for the user.
- ii. The system can encrypt and decrypt audio and send via Bluetooth.
- iii. This system can connect the Bluetooth connection and change key passkey using visual basic.

CHAPTER 6

CONCLUSION

Secure Text Transfer via Bluetooth using Hybrid Encryption is a new way to secure the text that send via Bluetooth. This system will increase the security of text transfer to avoid text transfer hack by unauthorized user. By using Hybrid Encryption, user will encrypt their text using combination of two algorithms. Using this method will secure text before transfer it through a Bluetooth device.

Some research has been done to make the analysis in order to develop this system. The researches are based on journal, web, and article and also from some book. From this resource, the information about developing the system was collected.

For methodology of this project, the waterfall model form the System Development Life Cycle was chosen. The waterfall model has five phases. Each phase in the model have their own roles for this project so that the project can be developed easily and run smoothly. The system needs the sender to connect the Bluetooth with receiver.

They must change the key passkey and the key passkey must same. After connect, the sender must encrypt the text before transfer the text. After the receiver receives the text, the receiver must decrypt the text.

As the conclusion, the Hybrid Encryption will make the text transfer via Bluetooth more secure.

References

- [1] <http://www.kellermansoftware.com/t-ArticleStrongestAlgo.aspx>
- [2] http://www.webopedia.com/TERM/H/hybrid_encryption.html
- [3] www.bluetooth.com
- [4] http://bokler.com/source_code/tdesutil_vb.html
- [5] http://www.codeproject.com/KB/security/image_embedding1.aspx
- [6] Abdulkadir Baba Hassan, Onawola Hassan and Matthew Sunday Abolarin(2006)-
The Application of Visual Basic Computer Programming Languages to
Simulate Numerical Iteration-University of Technology Minna.
- [7] R. Wei and Z.Zeng-KIST:A new encryption algorithm based on splay-Lakehead
University Thunder Bay.
- [8] Carlisle Adams(2000)-The CAST-256 Encryption Algorithm.
- [9] H.M Heys and S.E Tavares-On the Security of the Cast Encryption Algorithm-
Queen's University Kingston.
- [10] Colleen Rhodes(2007)-Bluetooth Security-East Carolina University.
- [11] Ian Curry(2001)-An Introduction to Cryptography and Digital Signatures.
- [12] Michael C.J Lin and Youn-Long Lin- A VLSI Implementation of the Blowfish
Encryption/Decryption Algorithm-National TsingHua University.
- [13] Karen Scarfone and John Padgette(2008)-Guide to Bluetooth Security-National
Institute of Standard and Technology.
- [14] MatrinLofberg and PatrikMolin(2005)-Web vs Standalone Application-School of
Engineering Blekinge Institute of Technology.

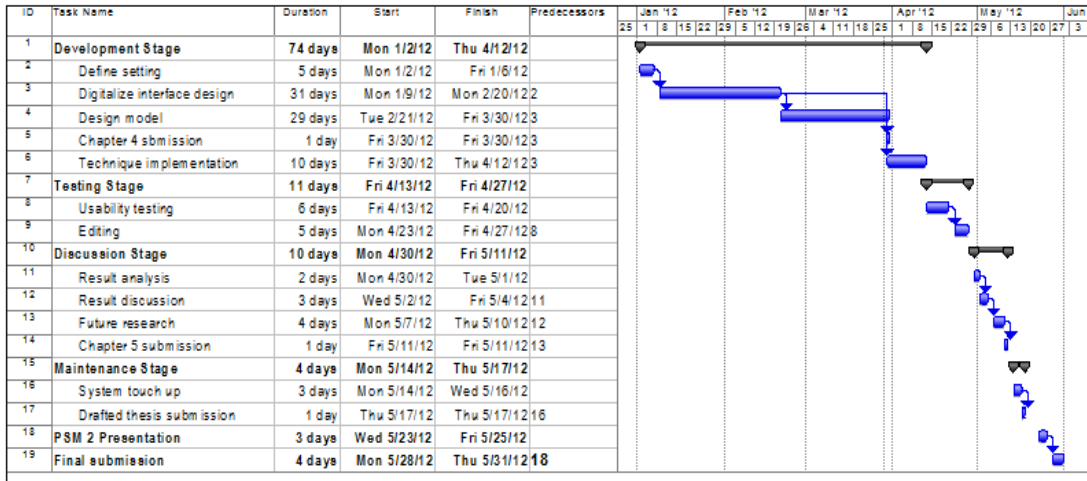
Referrences

- [15] Krishmurthy GN, Dr. V Ramaswamy- Encryption Quality Analysis and Security Evaluation of Cast-128 Algorithm and its Modified Version using Digital Images.
- [16] http://www.di-mgt.com.au/rsa_alg.html.

Appendix 1

Gant Chart

PSM 2



Appendix 2

USER MANUAL

SECURE TEXT TRANSFER VIA BLUETOOTH USING HYBRID ENCRYPTION

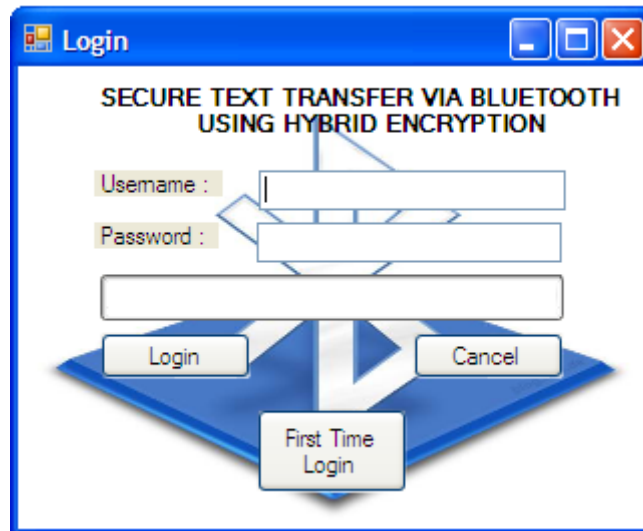
SECURE TEXT TRANSFER VIA BLUETOOTH USING HYBRID ENCRYPTION

SENDER

Before run the system, connect the Bluetooth devices to the laptop.

Connect the Bluetooth (have shown in Chapter 4).

Run the system.



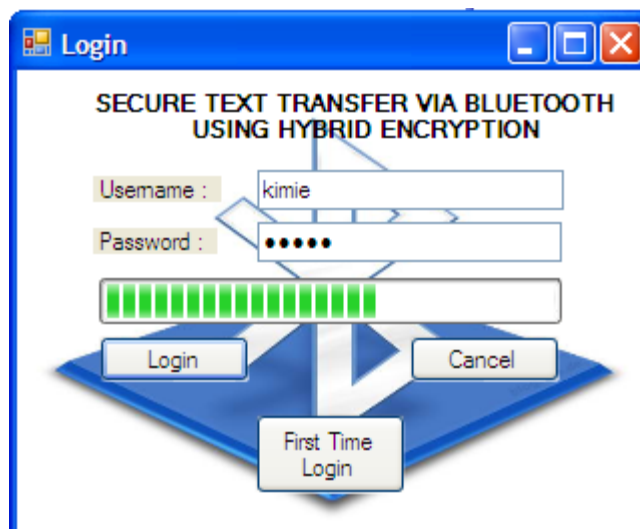
1. Click the first time login for the first time use.



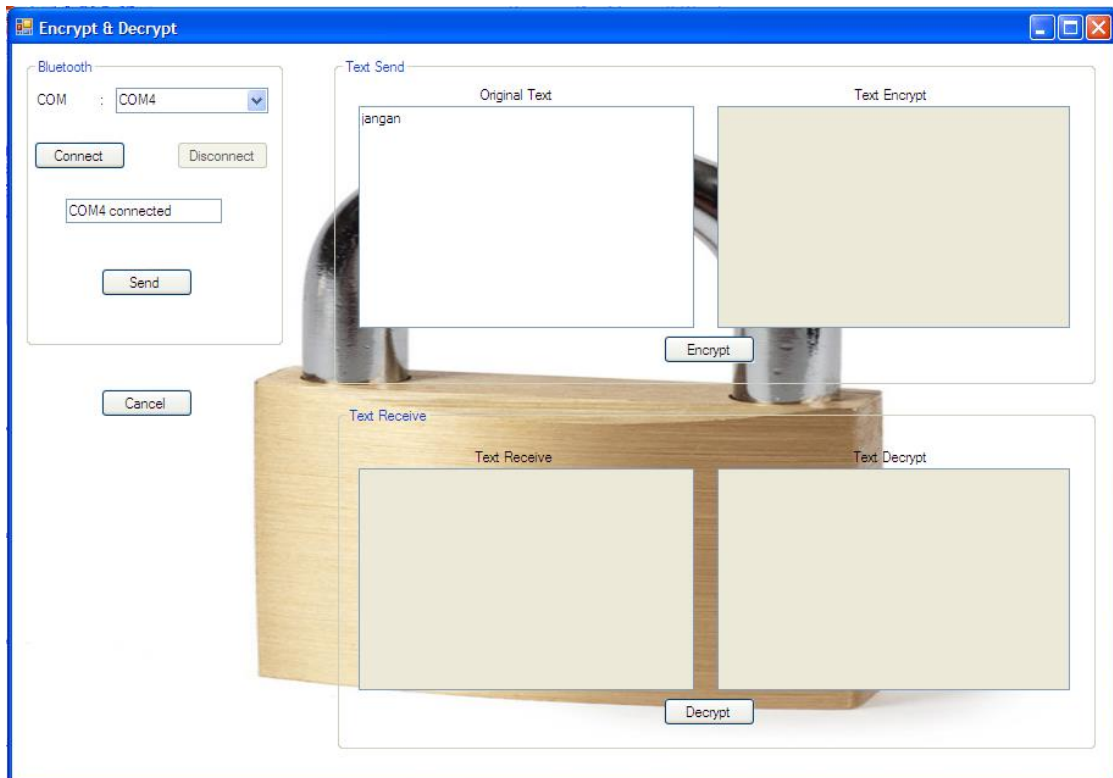
2. Insert the username and password.
3. Click button register.



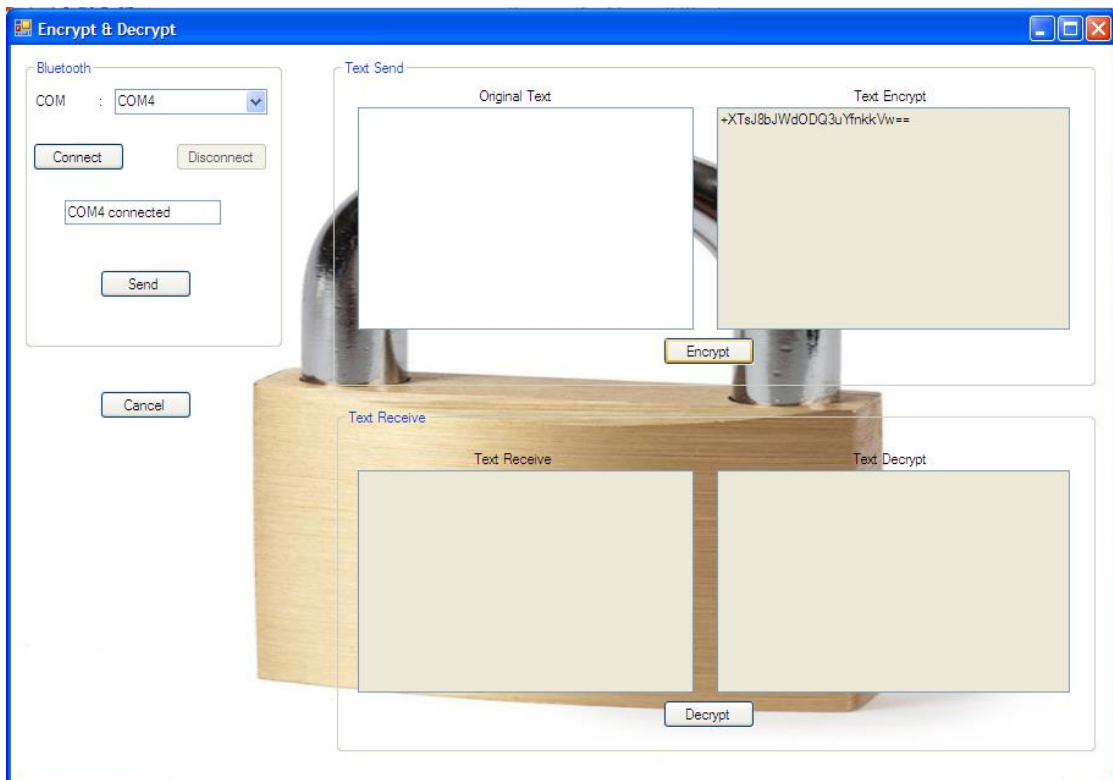
4. Click button back.
5. Insert the username and password that have been register. Click button login



6. Select the com port. Click button connect.
7. Write the text to encrypt. Click button encrypt.



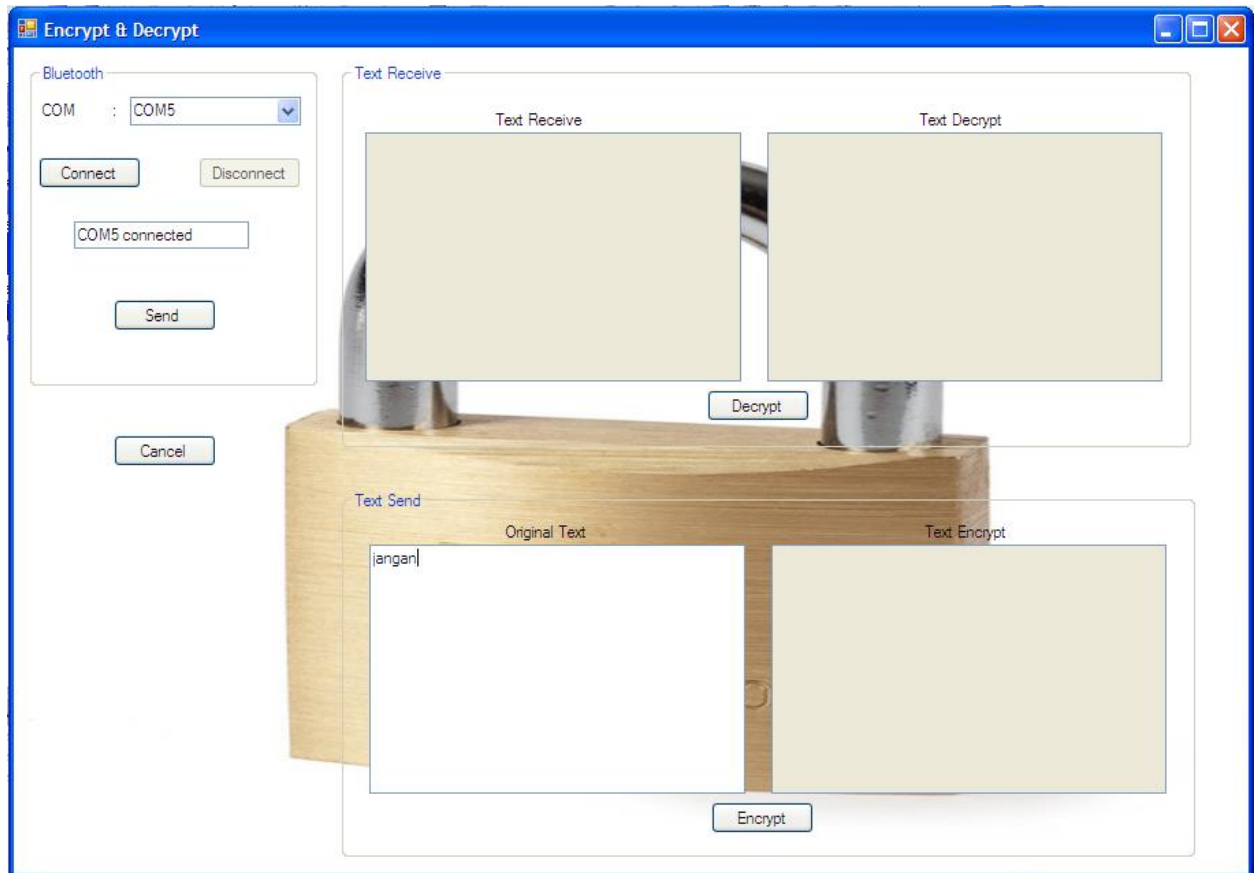
8. Click button send.



Sender also can receive the text

RECEIVER

9. Same step with sender from step 3 – 9.
10. Receive the text at text receive.



11. Click button decrypt. Plain text will show at text Decrypt.

****Receiver also can send the encrypt text****

