ENHANCING ARDUINO BASED SECURE KEYBOARD USING RSA ALGORITHM

NORDALILAH BINTI IDRIS

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS*

JUDUL : ENHANCING ARDUINO BASED SECURE KEYBOARD USING RSA ALGORITHM

SESI PENGAJIAN: 2016/2017

Saya NORDALILAH BINTI IDRIS .
(HURUF BESAR)

mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. ** Sila tandakan (/)

_____	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	

(TANDATANGAN PENULIS)

Alamat Tetap: NO 1,JALAN NAFIRI
11/5C, 40000 SHAH ALAM, SELANGOR

Tarikh : 23.5.2017

(TANDATANGAN PENYELIA)

MOHD ZAKI BIN MAS'UD
(Nama Penyelia)

Tarikh : 23.5.2017

CATATAN: * Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM)
** Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

ENHANCING ARDUINO BASED SECURE KEYBOARD USING RSA ALGORITHM

NORDALILAH BINTI IDRIS

This report is submitted in partial fulfillment of the requirements for the Bachelor of Computer Science (Computer Security)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2017

DECLARATION

I hereby declare that this project report entitled

ENHANCING ARDUINO BASED SECURE KEYBOARD USING RSA ALGORITHM

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : _____ Date : 23.5.2017
NORDALILAH BINTI IDRIS

SUPERVISOR : _____ Date : 23.5.2017
MOHD ZAKI BIN MAS'UD

DEDICATION

This thesis is dedicated to my parents, who taught me that the best kind of knowledge to have is that which is learned for its own sake. Their sacrifice had inspired me from the day I learned how to read and write until what I have become now.

I would also like to express a very special thanks to my husband for his love and patience. I am really thankful for his patience and understanding that were inevitable to make this work possible. I cannot find the appropriate words that could properly describe my appreciation for their devotion, support and faith in my ability to achieve my dream.

Many thanks go to friends for their excellent co-operation, inspirations and supports during this study. This experience with all you guys will be remembered as important memory for me.

Thank you.

ACKNOWLEDGEMENT

First of all, I am grateful to The Almighty God, Allah for giving me the opportunity, the passion and the strength to complete this project.

Mr Mohd Zaki bin Mas'ud has been the ideal thesis supervisor. I am grateful and would like to express my sincere gratitude to my supervisor for his invaluable guidance, continuous encouragement and constant support. I really appreciate his guidance from the initial to the final level. Without his advice and assistance it would be a lot tougher to complete this project. I also sincerely thanks and deeply appreciated for the time spent proofreading and correcting my mistakes. I am very grateful to have Mr Mohd Zaki as my thesis supervisor .

My sincere thanks also to all the lecturers and members of the Faculty of Information Communication and Technology who helped me in many ways and made my education journey at UTeM pleasant and unforgettable.

Lastly I would like to thanked everyone involved who helped contributes to my final year project directly or indirectly. I would like to acknowledge their comments and suggestions, which was crucial for the successful completion of this study.

ABSTRACTS

The title for the final year project is enhancing Arduino based secure keyboard using RSA algorithm. RSA algorithm by Ron Rivest, Adi Shamir and Leonard Adleman also known as asymmetric cryptography. Asymmetric cryptography have two different keys to accomplish a secure communication between two parties where one of them called encryption key and made public while the other called decryption key and made private. In this system the keyboard received the plain text input from the user. Then, the data input transmitted into the Arduino Leonardo for the encryption process. The key was generated by using RSA algorithms. Any encryption will be done in the Arduino Leonardo and transfer to personal computer (PC). Programming language C will be used to write encryption code in Arduino Leonardo . After that, the encryption process is done by using the public key. The cipher text will be transmitted to the computer for displayed . For decryption process, user can decrypt the cipher text by using sender private key. Visual Basic will be used to write decryption code in personal computer (PC). After decryption is done, all the encrypted and decrypted data save in text file. The development of this project is using an additional hardware which is Arduino Leonardo and the keyboard for user input. The main devices in this project are keyboard, Arduino Leonardo and personal computer (PC) . This system will enhancing Arduino based secure keyboard using RSA algorithm thus it secure the content of the information from unauthorized user .

ABSTRAK

Tajuk projek sarjana muda ini ialah untuk meningkatkan keselamatan papan kekunci dengan Arduino menggunakan algoritma RSA oleh Ron Rivest, Adi Shamir dan Leonard Adleman juga dikenali sebagai kriptografi asimetri. Kriptografi asimetri mempunyai dua kunci yang berbeza untuk mencapai komunikasi yang selamat antara dua pihak iaitu salah seorang daripada mereka dipanggil kunci penyulitan dan diumumkan, manakala yang lagi satu kekunci dipanggil penyahsulitan dan dijadikan peribadi. Di dalam sistem ini, papan kekunci menerima input teks biasa daripada pengguna. Kemudian, input data dihantar ke dalam Arduino Leonardo untuk proses penyulitan. Kunci telah dijana dengan menggunakan algoritma RSA. Segala penyulitan akan dilakukan di Arduino Leonardo dan selepas itu dihantar ke komputer peribadi (PC). Bahasa pengaturcaraan C akan digunakan untuk menulis kod penyulitan dalam Arduino Leonardo. Selepas itu, proses penyulitan dilakukan dengan menggunakan kunci awam. Teks cipher akan menghantar kepada komputer untuk paparan data. Untuk proses penyahsulitan, pengguna boleh menyahsulitkan teks cipher dengan menggunakan penghantar kunci persendirian. Visual Basic akan digunakan untuk menulis kod penyahsulitan dalam komputer peribadi (PC). Selepas penyahsulitan dilakukan, semua data disulitkan dan dibuka akan disimpan dalam bentuk fail text. Pembangunan projek ini menggunakan perkakasan tambahan iaitu Arduino Leonardo dan papan kekunci untuk input pengguna. Peranti utama dalam projek ini adalah papan kekunci, Arduino Leonardo dan komputer peribadi (PC). Sistem ini akan meningkatkan keselamatan papan kekunci dengan Arduino Leonardo menggunakan algoritma RSA oleh itu ia menjamin kandungan maklumat daripada pengguna yang tidak dibenarkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION	MEANING
PS	Problem Statement
PQ	Project Question
PO	Project Objective
PC	Project Contribution
RSA	Rivest, Shamir and Adleman
AES	Advanced Encryption Standard
DES	Data Encryption Standard
IDE	Integrated Drive Electronic

CHAPTER I

INTRODUCTION

1.1. Introduction

The purpose of this final year project is to use Rivest-Shamir-Adelman (RSA) algorithm for protecting the data input communications between a human interface device and a computer application from keylogger. Project objective is to enhance Arduino based secure keyboard. Arduino based secure keyboard is an add on module to secure the keyboard from keylogger. Developed by a previous final year project it used a symmetric cryptography to encrypt and decrypt the data. Even though it is secured, it still inherited the drawback of a symmetric cryptography algorithm which are using the similar pair key to encrypt and decrypt. Based on this reason this project will enhanced the secure keyboard module by introducing RSA algorithm that will encrypt the plain text data using the public key and decrypt cipher text using the private and public key.

Encryption module on the keyboard include an encryption key that is used for encrypt plain text data before the data is passed through Arduino Leonardo to computer. A secure data entry in a computer system featuring an encryption technique integrated within the device itself so that each transmission of data from the peripheral device is encrypted, giving it a high level of security with its initial transmission.

Encryption on Arduino Leonardo single chip microprocessor is secure because encryption are on the same chip by storing encryption keys and secure data in EEPROM memory . There is no opportunity for external interference, which could compromise the integrity of the data enabling maintenance of a high security level. The device can be applied to a keyboard used as data entry devices. Since each device utilizes a microcontroller in its standard configuration, the encryption technique of the present invention can be applied efficiently.

A secure keyboard can protect the data input communications between a human interface device and a computer application. This protection is even available when the computer is being exploited by a keylogger. The keylogger intercepts every human interface device input and keeps track of it. The attacker can often discover valuable information from the user. Hence, by providing a secure keyboard that incorporated an encryption module, the data keyed into the computer can be secured. The highest levels of security are available when an advanced cryptographic standard, RSA algorithm used to encrypt and decrypt data input. It is an asymmetric cryptographic algorithm that have two different keys.

RSA is one of the first practical public key cryptosystem algorithm. It is normally used for secure data communication. The private key must be kept secret however the public key can be shared with everyone. This is one reason why RSA has come to be the most commonly used asymmetric algorithm because it offers a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic transmission and data storage.

1.2 Problem Statement

There are some problem statement had been identified on the previous developed. The Problem Statement (PS) is shown as below in Table 1.1:

Table 1.1: Summary of Problem Statement

PS	Problem Statement
PS1	Keylogger is always the target and the main threat to keyboard since it capture keystrokes from keyboard .
PS2	Data is delivered through a non-secured transmission channel due to the same key used for both encrypting and decrypting .

1.3 Project Question

The Project Question (PQ) are discussed from the Problem Statement (PS) in Table 1.2. The Table 1.2 below shown the Summary of Project Question (PO).

Table 1.2: Summary of Project Question

PS	PQ	Project Question
PS1	PQ1	How to achieve the high level security requirement in cryptography ?
PS2	PQ2	How can Arduino Leonardo will help to encrypt and decrypt the data from keylogger ?

1.4 Project Objective

The Project Objective (PO) are developed based on Problem Statement and Project Question. The Table 1.3 below shown the Summary of Project Objective.

Table 1.3: Summary of Project Objective

PS	PQ	PO	Project Objective
PS1	PQ1	PO1	To enhance of a secure keyboard.
		PO2	To design secure algorithm that can be used to protect information during the transmission.
		PO3	To develop encryption and decryption model of secure keyboard using asymmetric key for secure data transmission.

1.5. Project Scope

1. The developer who develop a secure keyboard encryption and decryption.
2. The users who input data through keyboard communication will be encrypted and decrypted.
3. The Arduino Leonardo device that used to encrypt the data input from user using the public key to the computer will be decrypt the encrypted data using the private key.

1.6 Project Contribution

Table 1.4 show the project contribution. Project contribution is to show how this product can contribute back to organizations and individuals.

Table 1.4: Summary of Project Contribution

PS	PQ	PO	PC	Project Contribution
PS1	PQ1	PO1	PC1	Proposed enhancement module for the previous secure keyboard project.
		PO2	PC2	Applied RSA algorithm in encrypting and decrypting on a secure keyboard.
		PO3	PC3	Development of a secure keyboard data input and output in keyboard communication will be encrypted and decrypted.

1.7 Thesis Organization

Chapter 1: Introduction

This chapter discusses problem statement about this project, project objective to achieve when doing this project, project question, scope, project contribution, thesis organization, and conclusion.

Chapter 2: Literature Review

This chapter review 20 articles that related to the research done on this project. This chapter discuss issues that related to project and compare all the articles that have been read and find any similarities with the project that will be develop.

Chapter 3: Methodology

This chapter discusses project methodology and how it would be carried out. The project milestones of this project also will be discuss in this chapter. A milestone is about step what to do to keep track with the project and explain in details every stage on the milestone.

Chapter 4: Analysis and Design

This chapter discusses problem analysis, requirements analysis, high-level design and detailed design of this project. The results about the analysis of the preliminary design and the result of the detailed design is define here. The detailed about design and system architecture also included in this chapter.

Chapter 5: Implementation

This chapter discusses software development environment setup, software configuration management and implementation status. The activity involved in the implementation phase and the expected output was state here.

Chapter 6: Testing

Chapter 6 is about testing. All the results of the testing need to be record even though it fails and need to justify. After explain the test design and plan, the project need to discuss more about test results and analysis in this chapter.

Chapter 7: Project Conclusion

This chapter discusses project summarization, project contribution, project limitation and future work. This chapter will describe about how the objective has been achieved by integrating the information from the implementation and testing phase in the previous chapter. The significant result in this project will be conclude and the weaknesses and strength of your project is also being discusses.

1.8. Conclusion

In conclusion, this chapter to explain the background for this project and to state the problem for this development until it is complete. The objective need to achieve and the project must follow the objectives of the systems and solve the problem statements that occur. Next activities need to be developed for next chapter is literature review about others article that related to our project. The next chapter is chapter II which is literature review, find related articles with the project and study the articles.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

A computer is a device characterized by a processor, memory, and input/output (I/O) devices. A user can interact with a computer using a human interface device (HID) such as a keyboard .The computer can present information to the user using a display device. Like any other keyboard, the secure keyboard communicates with a computer via a communications port. The HID inputs are encrypted before being passed to the computer and thence the application. Therefore, a secure link exists from the HID to the application. Choosing strong encryption and unique encryption and decryption keys allows applications to be keyed to a specific secure keyboard (Eduardo S. Pinheiro 2010).

Secure communication between a keyboard and a component, such as a piece of software running on a computer. A keyboard communicates user entered data to an electronic device, such as a computer. When a user presses a key on the keyboard, the keyboard generates data representative of the particular key that was pressed example the ASCII code for the letter “e”, and this data is received by a component in the computer, such as a device driver.

The device driver then presents the data to whatever program running on the computer is currently receiving input example by placing the data into the input buffer for whichever application program is active (Peinado & Benaloh 2007).

Systems and methods of managing keystroke data in embedded keyboard environments may involve transferring a mode request from a management controller to an embedded controller of a keyboard via a dedicated communication channel. Keystroke activity can be detected at the keyboard, and keystroke data may be transferred from the embedded controller to the management controller via the dedicated communication channel in response to the keystroke activity and the mode request. In addition, the management controller may be used to encrypt the keystroke data, wherein the encrypted keystroke data can be transmitted from the management controller to an off-platform service via a network controller (Nitin V Sarangdhar 2015).

The method may include initiating a secure data input mode at a user input device coupled with a computing system and the user input device is a peripheral input device for receiving input into the computing system. Inputted data from the user input device to the computing system, wherein the user inputted peripheral device data is encrypted with an encryption key that is based on the user identification data, the encryption key tying the encrypted user inputted peripheral device data to the user input device and a specific user .Transmit the encrypted user inputted peripheral device data to the computing system, the encrypted user inputted peripheral device data to remain hidden from the operating system of the computing system.

Decrypt the encrypted data within the physical bounds of the data transducer, and generate a data output, from the decrypted encrypted data, for presentation to the user with the data transducer, wherein the received encrypted data to remain hidden from the operating system of the computing system(Lee et al. 2014) .

Decryption apparatus includes an input memory which is coupled to receive encrypted data, and an output transducer for presenting decrypted data to a user. A decryption processor is coupled to read and decrypt the encrypted data from the input memory but is incapable of writing to the input memory, and is coupled to convey the decrypted data to the output transducer for presentation to the user(Lior Frenkel 2010).

An asymmetric crypto-key is a key used to transform messages, such as to encrypt a message, decrypt a message or form a digital signature on a message. An asymmetric crypto-key has a public portion and at least one private portion. The public portion is widely known or available. If an asymmetric crypto-key has only one private portion, that private portion is known only to the user with whom the asymmetric crypto-key is associated. If it has multiple private portions, at least one of these portions is known to the user with whom the key is associated, and the other portion or portions is/are known to at least one other entity. For single private portion asymmetric crypto-keys, a message encrypted with the public portion can be decrypted with the private portion, and vice-versa. A message signed with the private portion can be authenticated with the public portion. When an asymmetric crypto-key has more than one private portion, each private portion is used to transform a message (Examiner-alan & Richardson 1998).

To protect transmitted data from eavesdropping by someone other than the desired receiver, we need to disguise the message before sending it into a non-secure communication channel. This is achieved by a cryptosystem. In 1978, Rivest, Shamir, and Adleman invented a method to implement the public-key cryptosystem, which is known as the RSA cryptosystem since it provides high security and is easy to implement, so it quickly became the most widely used public-key cryptosystem.

However, developing an inexpensive hardware device for real-time RSA encryption and decryption is still a challenge. Finding an efficient hardware implementation for

RSA is one of the important tasks that remain to be done in cryptography(Wu et al. 2001).

A processor generates an asymmetric crypto-key, such as an RSA (Rivest, Shamir and Adleman) crypto-key, which is associated with the user and includes a private key and a public key. It computes a first key portion based on a stored random number generation function, Which has one or more constants such as a salt and/or iteration count, and a first value of a constant, and a second key portion based on the computed first key portion and one of the private key and the public key. It additionally computes another first key portion based on the stored random number generation function and a second value of that constant, and another second key portion based on the computed other first key portion and the one key. The computed first and second key portions and the computed other first and second key portion form first and second splits of the one key of the asymmetric crypto-key (Ravinderpal Singh Sandhu, Oak Hill Va , Desa 2010).

Both public and private sectors have become increasingly dependent on electronic data processing. This digital data are going through an insecure channel from one place to another and anyone can easily get those important data without the concerns of the sender. So, protecting these important data is crucial task in data communication and Public Key Cryptography is one of the best ways to protect digital data from the unauthorized access. RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures.

The RSA is the most popular public key cryptographic algorithm that is used to help ensure data communication security .It is simply based on two main cryptographic processes. First, using a public key it converts an input data called the plaintext into an unrecognizable encrypted output called cipher text (encryption process), such that it is

impossible to recover the original plaintext without the encryption password in a reasonable amount of time. Second, using a private key, the RSA then converts the unrecognizable data back to its original form (decryption process) (Rahman et al. 2012).

To provide information security, numerous cryptographic algorithms were proposed by various researchers, out of which RSA algorithm is one the most popular algorithm. RSA algorithm uses linear congruence method which restricted the operation to specific class of values. RSA algorithm needs exponential time for decryption of message. By extending the RSA algorithm using congruence class and selecting the key in random, the security of algorithm can be increased. Higher the congruence class index, higher will be its level of security. For each of the congruence class element, complexity of algorithm will be same but there will be increase in the level of security. The basic idea behind this implementation is that by converting the given linear congruence into congruence class and solving them algebraically, actual information can be produced (Yongo E., Manyala J.O., K. Kito., Y. Matsushita., Outa N.O. 2016).

Arduino microcontroller boards as an inexpensive and flexible alternative. These boards connect to standard experimental software using a USB connection and a virtual serial port, or by emulating a keyboard. Arduino is the name of a family of microcontroller boards. The boards are a combination of an ATMEL microprocessor including RAM, flash memory, and input/output channels. Thus, these boards have the same general structure as common personal computers, but their performance is of course only a fraction of those. Part of the Arduino package is a programming environment, where code is written in a simplified C-like language, and transferred to the Arduino using a USB cable. After programming, an Arduino can work while being connected to a PC or operate standalone. Several features make the Arduino family an interesting tool as a measurement platform. First of all, it connects easily by USB to a Windows PC, and can transmit data using a virtual serial port to these operating systems.

Second, it is open source hardware, which means that everybody can access, modify, and use the board design(Schubert et al. 2013).

2.2 Related Work/Previous Work

According to Bernd Grossmann (2010) , the keyboard has data entry modules for entering data, and a keyboard control device comprising a receiving device to receive the entered data and an encryption device to encrypt the received data via encryption algorithm, where the encryption algorithm is a program code. A transmission connection transmits the encrypted data to an external example electronic cash register, connected to the keyboard control device, where the encryption algorithm is selected by a user from multiple predefined encryption algorithms and is associated with the modules. An independent claim is also included for a method for secure transmission of data from a keyboard to an external device.

Besides that, an article (Christopher Reon Gentle 2001) show a method and keyboard for protecting data generated by the keyboard by reading data from a keypad of the keyboard, encrypting the read data, and transmitting the encrypted data from the keyboard to a computer. A method for protecting by the computer data generated by a keyboard where the keyboard is connected to the computer by receiving encrypted data from the keyboard by the computer, and decrypting the encrypted data. A method for protecting by a server the data generated by a keyboard where the keyboard is connected to the server via a network and a computer by receiving encrypted data from the keyboard by the server, and decrypting the encrypted data.

Furthermore, in this article by Lior Frenkel (2016) ,data encryption is widely used in preventing unauthorized access to data. Various methods of data encryption are known in the art. In general, these methods use a key to convert data to a form that is unintelligible to a reader (human or machine), and require an appropriate key in order to decrypt the data. Symmetric encryption methods use the same key for both encryption and decryption. Such symmetric methods include the well-known DES (Data Encryption Standard) and AES (Advanced Encryption Standard) algorithms.

Then, an article Martin et al. (2002) said that in symmetric key crypto there is only one key. It is used for both encryption and decryption. A key refers to any code that yields plain text when applied to cipher text. This key is shared by both sender and receiver. If the key is disclosed the secrecy of the information is compromised. The key is known to both the sender and the receiver, hence does not protect the sender from the receiver forging a message & claiming is sent by sender. Lengthy keys are used to increase the security and to decrease the chances of identifying the key through brute force. It is relatively fast as it uses the same key for encryption and decryption .However, more damage if can occur if the key is compromised. When someone gets their hands on a symmetric key, they can decrypt everything that was encrypted with that key. Since symmetric encryption is used for two-way communication, both sender and receiver end data gets compromised.

In addition Deshpande et al. (2009) said that , Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS), is an approved cryptographic algorithm that can be used to protect electronic data. The AES can be programmed in software or built with pure hardware. In cryptography, the AES, also known as Rijndael, is a block cipher adopted as an encryption standard by the US government, which specifies an encryption algorithm capable of protecting sensitive information. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher)

information. Encryption converts data to an unintelligible form called cipher-text. Decryption of the cipher-text converts the data back into its original form, which is called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Besides that, an article from Cheung (2004) ,in some conventional encryption applications, it is necessary to send data to a hard disk to be encrypted and retrieve data from the hard disk for decryption. One such application is personal video recording (PVR). In such systems, the encryption/decryption functions are implemented by separate devices between the ATA host adapter and the ATA bus connector.

ATA stands for AT Attachment, a standardized interface used by storage devices such as hard disk drives, CD drives and DVD drives. ATA compatible drives may also be referred to as integrated drive electronics (IDE) drives. One drawback with conventional separate device implementations is that unencrypted or "clear" data is available at the interface between the ATA host adapter and the external encryption/decryption chip, and can be intercepted and stored in unencrypted form. Additionally, the encryption used in conventional systems is not particularly "strong" and could be broken relatively easily.

Furthermore, in this article by (Al-Haija et al. 2014) , Arduino is an open source microcontroller board which can be programmed using free development software. The Arduino uses a simplified version of C/C++ programming language. With Arduino board, we can write a program to control physical systems by read and write analog/digital signal. Therefore, some analog sensors are needed to be connected to the Arduino to read analog signals, and the ADC (Analog to Digital Converter) is the responsible to convert these signals to digital signals. To program and configure the Arduino, we have used the Integrated Development Environment (IDE) software.

Arduino is one of the most popular microcontrollers. It can be used in applications to provide many security features.

Then, an article Higinio Rubio,Enrique Soriano (2015) show the development of a platform based on Android in order to monitor a mechatronics system based on an Arduino microcontroller. Nowadays, Arduino is an open microcontroller system which makes easy the monitoring and control systems. The system allows the on-line data monitoring and data recovery, in a remote way, using Android devices. Referring to Arduino, it is an open hardware platform, based on a microcontroller board and a development environment designed to facilitate the use of electronics in multidisciplinary projects. This makes it a widely known and used platform. Arduino can be used to develop stand-alone interactive objects or can be connected to computer software.

2.3 Critical Review of Current Problem and Justification

In symmetric encryption there is only one key. It is used for both encryption and decryption. A key refers to any code that yields plain text when applied to cipher text. This key is shared by both sender and receiver. If the key is disclosed the secrecy of the information is compromised. The key is known to both the sender and the receiver, hence does not protect the sender from the receiver forging a message and claiming is sent by sender. Lengthy keys are used to increase the security and to decrease the chances of identifying the key through brute force. It is relatively fast as it uses the same key for encryption and decryption. However, more damage if can occur if the key is compromised. When someone gets their hands on a symmetric key, they can decrypt everything that was encrypted with that key. Since symmetric encryption is used for

two- way communication, both sender and receiver end data gets compromised(Meenakshi Shankar 2001).

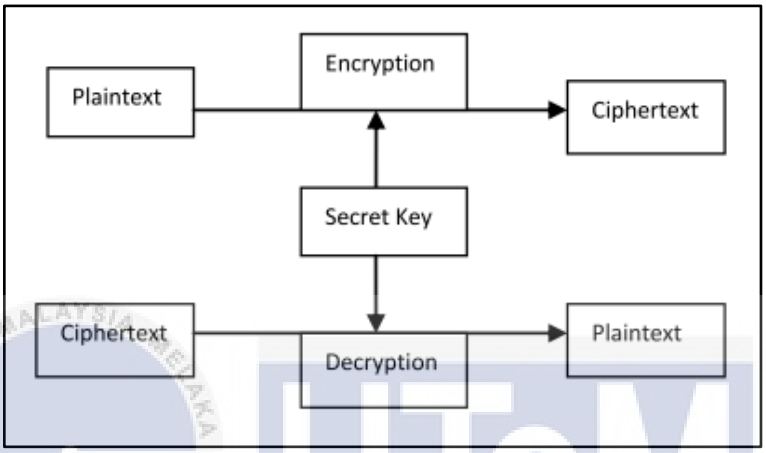


Figure 2.1: Symmetric Key Cryptography Process

In this encryption process the receiver and the sender has to agree upon a single secret (shared) key. Given a message (called plaintext) and the key, encryption produces unintelligible data, which is about the same length as the plaintext was. Decryption is the reverse of encryption, and uses the same key as encryption. Popular symmetric key algorithms including DES, AES (Rijindael), Blowfish, were implemented, and their performance was compared by encrypting input files of varying contents and sizes(Thakur & Kumar 2011).

The Table 2.1 shows comparison between three most common symmetric key cryptography algorithms DES, AES, and Blowfish

Table 2.1: Comparison between three most common symmetric key

Data Encryption Standard(DES)	Advanced Encryption Standard(AES)	Blowfish
DES was the first encryption standard to be published by NIST (National Institute of Standards and Technology). DES uses a 56 bit key and the key actually looks like a 64 bit quantity, but one bit of each 8 octets is used for odd parity on each octet. There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher	AES also known as the Rijndael (pronounced as Rain Doll) algorithm, is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES was introduced to replace the DES. Brute force attack is the only effective attack known against this algorithm.	Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Weak keys problem, no attack is known to be successful against it.

Encryption plays an essential role in protecting the privacy of electronic information against threats from a variety of potential attackers. In so doing, modern cryptograph employs a combination of conventional or symmetric cryptographic systems for encrypting data and public key. Assessing the strength required of the symmetric cryptographic systems is therefore an essential step in employing cryptography for computer and communication security. Technology readily available today, makes brute force attacks against cryptographic systems considered adequate for the past several years both fast and cheap. General purpose computers can be used but a much more efficient approach is to employ commercially available Field Programmable Gate Array (FPGA) technology. For attackers prepared to make a higher initial investment custom made, special purpose chips make such calculations much faster and significantly lower the amortized cost per solution. As a result cryptosystems with 40-bit keys offer virtually no protection at this point against brute force attacks. As cryptosystems often succumb to smarter attacks than brute force key search, it is also important to remember that the key lengths discussed are the minimum needed for security against the computational threats considered.

Fortunately the cost of very strong encryption is not significantly greater than that of weak encryption. Therefore to provide adequate protection against the most serious threats well-funded commercial enterprises or government intelligence agencies, keys used to protect data today should be at least 75 - bits long. To protect information adequately for the next 20 years in the face of expected advances in computing power ,keys in newly deployed systems should be at least 90 bits long(Schneier 1996). The Table 2.2 shows the critical review of current problem and justification in different method, advantages and disadvantages.

Table 2.2: Critical Review of Current Problem and Justification

Method	Description	Advantages	Disadvantages
Comprising encryption and decryption module	Obtain input from the keyboard, encrypting the input and comprises an encryption key. Passing to the computer and decrypting the encrypted input utilizing the transferred decoding module wherein an application confirmation module, utilizes a relating application module signature.	The data information is secured from threat	Sharing the key
Secure communication with a keyboard.	The device driver is currently receiving input by placing the data into the input buffer for whichever application program is active). One problem in using a keyboard to receive data is when the data is sensitive or then needs to be kept secret.	Data transfer are encrypted	Using secret key
Rolling key function	A method involving storing a current copy of the key. The key is concurrently updated at each secure module using a respective clock. It also comprising encrypting data according to 3DES.	Have automatic updated encryption key	Not easily to decrypted by unauthorized person

The encryption key stored by the programmable human input device	The encryption key stored by the programmable human input device is associated with the accessed service. It stored encryption keys includes a public encryption key portion of a public/private encryption key pair.	Have both public/private key of programmer	Attacker can know the both of key easily
Measure response latencies by using Arduino microcontroller boards	Using Arduino boards as an inexpensive and flexible alternative. These boards connect to software using a USB connection and a virtual serial port or by emulating a keyboard. In our solution, an Arduino measures response latencies after being signaled the start of a trial and communicates. It will response back to the PC over a USB connection	The delay can be solved by using Arduino.	Response boxes can be fashioned out of cheap equipment. Parallel ports are disappearing fast from modern computers, and are not available on modern laptops.

2.4 Proposed Solution

After comparing all the journal/article that related, the improvement that will be implement in this project is to enhancing Arduino using RSA algorithm, the system that will be develop is more secure and easy to understand. Firstly, to keep the data secure, the data should be encrypted with RSA algorithms after public and private key was generated. The review on the previous research has given requirement to enhancing Arduino based secure keyboard using RSA algorithm and the process development of secured keyboard is involved a keyboard, Arduino Leonardo and computer.

Firstly, to keep the data secure, the data should be encrypted with RSA algorithms after public and private key was generated. The public key is used to encrypt the data while the private key is used to decrypt the data. RSA algorithm is used to secure and to encrypt and decrypt the information purpose. RSA algorithms was choose in this project because the process to produce the private key from the public key and modulus is difficult. Thus, it is highly secure. Computing the reverse of e is very difficult for the attackers. The downsides of this algorithms is it was complex to generate the key. The process of the factorization method and factorizing a large number is very difficult. Then, the process also quite slow. The Table 2.3 shows comparison between AES and RSA

Table 2.3: Comparison between AES and RSA

Algorithm	AES	RSA
Advantage	Symmetric algorithms, provide integrity and confidentiality, high speed	Asymmetric algorithm, provide data security and data integrity, high performance in term of security.
Disadvantage	Less security and efficiency	Consume maximum time

Arduino is the name of a group of microcontroller boards. The boards are a combination of an ATMEL microprocessor including RAM, flash memory, and input/output channels. In this manner, these boards have the same general structure as personal computers. Most Arduino boards are equipped with extra chips that change over the serial communication from the microprocessor into USB that connects then to a computer. The USB cable connects Arduino and computer, and gives a serial association. On the computers side, driver software makes a virtual serial (COM) port. This serial port can be gotten to with any software that can communication with a serial port.

Part of the Arduino package is a programming domain, where code is composed in language like C-language or java language and exchanged to the Arduino using a USB cable. Ensuing to programming, an Arduino can work while being connected with a computer or work standalone. A few components make the Arduino fascinating tool as a measurement platform. As a matter of first significance, the interfaces connected successfully by USB to a Windows PC, Mac, or Linux machine, and can transmit data using a virtual serial port to these working structures. Besides that, it is open source hardware, which means that everybody can access, modify, and use the board design. Refer to Figure 2.2.

Figure 2.2: Arduino Leonardo microcontroller boards

In conclusion, the proposed solution for data security and integrity issue is that this project want to provide two ways of securities that is RSA algorithm for data security and data integrity. The review on the previous research have been read and complement the objective of the developing system. Thus, the system have been improve and solve the problem statement of the development from the article/journal.

The objective of the development system is:-

i. To explore the enhancement of a secure keyboard,
ii. To design secure algorithm that can be used to protect information during the transmission
iii. To develop encryption and decryption model of secure keyboard using asymmetric key for secure data transmission.

The problem statement stated which are:-

i. Data is delivered through a non- secured transmission channel due to the same key used for both encrypting and decrypting
ii. Keylogger is always the target and the main threat to keyboard since it capture keystrokes from keyboard.

2.5 Conclusion

In conclusion, from this chapter, minimum 20 related article/journal about the enhancing Arduino based secure keyboard using RSA algorithm have been review. Data security and integrity in the computer is very important to us to make sure the data that we keep in the computer is secure and does not altered by unauthorized user. As the problem of data leakage has become more seriously incident happened, we need the algorithm to prevent this problem arise again in the next time. So, this project have come up with an algorithm to secure the data and the integrity of the data itself using RSA algorithm. Chapter 3 which is methodology discuss what method used to develop the project. It determined what approaches needed to use to complete the project within the time. Milestones about projects need to be prepared in this chapter.

CHAPTER III

METHODOLOGY

3.1 Introduction

This chapter explained in details about the method use for the development of the project. The project flow described based on activity for every stage. The project tools for enhancing Arduino based secure keyboard using RSA algorithm explained the process on how to test the simulation and to implement encryption in Arduino and decryption to decrypt the encryption input that have been transfer from Arduino to computer. The project flow is described based on activity for every stage. This chapter explained in detail about the method of this project.

3.2 Methodology

Methodology describes the methods and principles that are used for this project . In this case, this chapter will explain the step that will be used during the accomplishment of this project. The methodology used in this project is based on Waterfall model .

Waterfall model was chosen because this model is simple and also very easy use and understand. Each level has a review process and specific deliverables, so it is easy to manage due to the rigidity of the model. Waterfall model works well as this project is a small project. The phase does not overlap because each phases must be processed and completed one at a time. There are five stages in this model that is requirement and analysis, system design, implementation, verification and maintenance. Each stages have different activities and it will be explain below. Figure 3.1 shows the waterfall model.

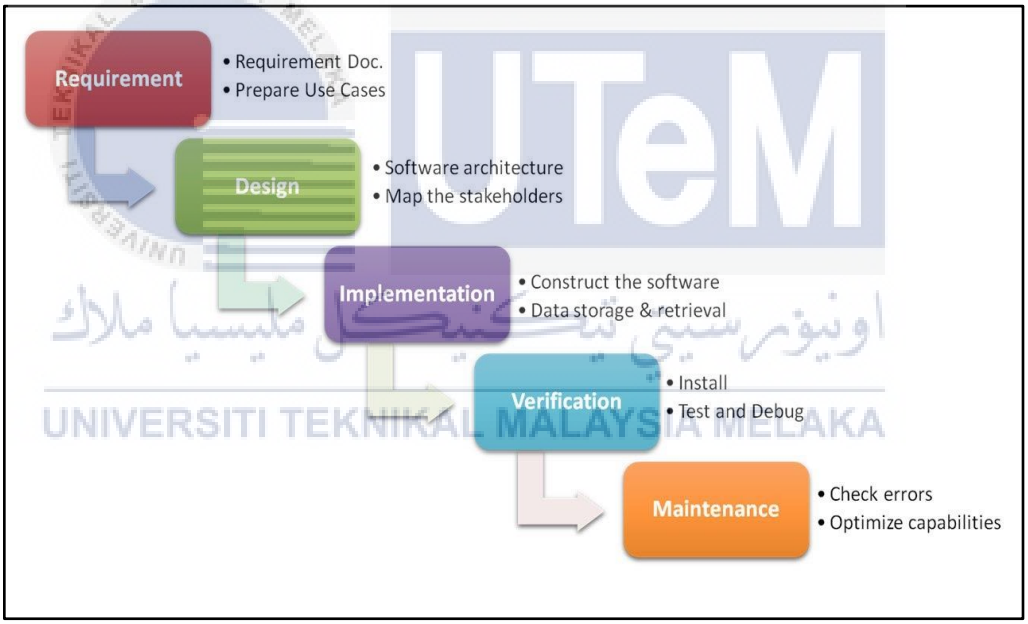


Figure 3.1: Waterfall Model

3.2.1. Phase 1: Requirement and Analysis

This is the first phase, the problem about data security and data integrity was identified. Proposal was created during this phase. After the proposal was approved by the committee, this project can be proceed with Chapter 1. In Chapter 1 , the problem statement, scope, and project objectives are defined . In analysis phase, the study about the structure of the system is being discussed in Chapter 2. The algorithms that need to be use in this project is being finalized. The chosen algorithms to complete the project is RSA algorithm

3.2.2. Phase 2: System Design

The design of an interface for this project is used to make the user use this system more easily and understandable. This step will start to design the tools to enhancing Arduino based secure keyboard by using RSA algorithm in encryption and decryption module. The keyboard are connected to the Arduino Leonardo which implement the RSA algorithm and display the cipher text on the computer screen.

3.2.3. Phase 3: Implement

The most critical phase in this project is implementation phase. In this phase, the coding was develop and the code need to be tested. The algorithms that has been choose for this project is RSA algorithms. The code is being tested to prevent the bugs and error from occur during the final presentation later. Implementation will be done after the tools is working without any problems. Implementation will review the design after done and always be design with the end user mind.

3.2.4. Phase 4: Verification

This phase test the tools whether it working finely or not and to make sure to achieve the objective of the project.

3.2.5. Phase 5: Maintenance

This phase test maintenance need to be done to repair and improve the system. This phase will fixed the error on the system until the system running smoothly.

3.3 Project Milestones

Project milestone it shows the timeframe and activities done to complete the task for the project. The timeline of this project is shown in the Gantt chart. The duration of the Gantt charts consists of 15 weeks to complete the project. Gantt chart is used to make sure that the project complete based on the duration explained. Based on the Gantt chart, the longest duration is the design and implementation phase. The design and implementation phase are the most important phase to make sure the requirement of the project is functional. The milestones explain about the flow of the project within the duration to complete the project. Table 3.1 shows the milestone of the project.

Table 3.1: Milestones

Activity	Responsibility	Date Start	Date End
Submission proposal	AJK	Week 1	Week 1
Prepare chapter 1 and chapter 2	Student and Supervisor	Week 1	Week 2
Submission of Chapter 1 and Chapter 2 and discussion	Student and Supervisor	Week 2	Week 3
Prepare the analysis chapter 3 and project progress	Student and Supervisor	Week 3	Week 3
Submission of chapter 3 and discussion	Student and Supervisor	Week 4	Week 4
Design and Implementation of the project	Student	Week 5	Week 10
Prepare chapter 4 and discussion	Student and Supervisor	Week 8	Week8
Progress evaluation	Student and Supervisor	Week 10	Week 10
Improvement of chapter 4 and prepare for PSM 1 presentation	Student	Week 11	Week 11
Presentation PSM 1	Student ,Supervisor and Evaluator	Week 12/13	Week 12/13
Continue PSM 2	Student and Supervisor	Week 14	Week 14

The Table 3.2 below shows the Gantt chart of this project.

Table 3. 2: Gantt chart

Duration (week) / Task name	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
CHAPTER 1 : INTRODUCTION															
CHAPTER 2 : LITERATURE REVIEW & METHODOLOGY															
CHAPTER 3: ANALYSIS															
CHAPTER 4: DESIGN & IMPLEMENTATION															
DEMO 1 : PRODUCT															
DEMO 2: REPORT															
CHAPTER 5 : TESTING & ANALYSIS															
CONCLUSION															
DEMO FINAL (PRODUCT&REPORT)															

3.4 Conclusion

In conclusion, I have choose Waterfall model for project methodology. This project planning involved five stages which is requirement analysis phase, design phase, implementation phase, verification phase and maintenance phase. The milestones was created to make sure this project can be done in a given time.

The milestone and Gantt chart shows the activities and date or week for the project to develop within the duration. This phase is important to make sure the project is success. The next chapter is analysis and design that describe the analysis of the preliminary design and the detailed design of the project.

CHAPTER IV

ANALYSIS AND DESIGN

4.1 Introduction

In this chapter, the discussion briefly explained about the analysis and design for enhancing Arduino based secure keyboard using RSA algorithm. The design and analysis are important in developing the software. The analysis will make sure that the new design follow the objectives of the project. The hardware and software required in this project are explained in this chapter. This chapter proposes efficient hardware design and an architecture of RSA algorithm using Arduino Leonardo. The design for this system is the user input the data through the keyboard and encrypt by the Arduino Leonardo . Encrypted data is passed on to the computer. Computer is used to decrypt the cipher text into plain text and save it in text file. RSA algorithm secure communication by using the encryption key that was made as a public while the other one called decryption key is made for private usage.

4.2 Problem Analysis

From the analysis of this project, there are several problems that have been known from the existing secure keyboard by symmetric algorithm. From the problem explained, this project will enhancing Arduino based secure keyboard using RSA algorithm thus it secure the content of the information from unauthorized user. The analysis is about the problem faced by the system and to improve the functionality and quality of the system in order to make the system become better.

Symmetric key cryptography is well recognized in modern cryptography. Those issue regards to symmetric key cryptography is that we need one particular key to encrypt a plain text and the same key can be used to decrypt the cipher text. The main problem of symmetric key cryptography is that the same key is used for encryption and decryption process. The data transmission needs of security and so that the secure transmission is on demands. The process of designing systems that are concerned with the study of transmission data over non-secure channels is called cryptography.

The other problem is a non-protective data that can be trace by other people which they can use to steal the important information of the user and exposed the user to the threat especially keylogger. Keylogger attack capture each data input and monitor all the activities of the victims without their knowledge. The attacker steals the credential information from the user input for data misuse. The data lost will make the users loss their money, dignity, credibility and crucial information. To overcome that vulnerabilities, this project will provide the data security and data integrity through encryption and decryption method together with hash algorithms. The purpose of this project is to enhance the security and also proposed a solution to overcome this problem.

4.3 Requirement analysis

The analysis and design before enhancing Arduino based secure keyboard has been discussed which this project is will follow the design to develop a successful secure keyboard using RSA asymmetric encryption and decryption algorithm.

4.3.1 Data Requirement

The Figure 4.1 shows the flow chart diagram for the system. The keyboard receive the plain text input from the user. Then, the data input transmitted into the Arduino Leonardo for the encryption process. The key was generated by using RSA algorithms. In this phase, the public key and private key is calculated. After that, the encryption process is done by using the public key. The data input after process encryption called cipher text that will transmit to the computer for display the encrypted data.

Next, for decryption process user decrypt the cipher text by using sender private key. The hash value of the encrypted data is also being calculated at the same time and compare it with the hash value of the sender. If the hash value of the receiver same with the hash value of the sender, then the data was safe and have not modified by other user. After decryption is done using RSA algorithm, the plain text shown in Windows Forms, Visual Basic . Computer is used to decrypt the cipher text and save it in text file.

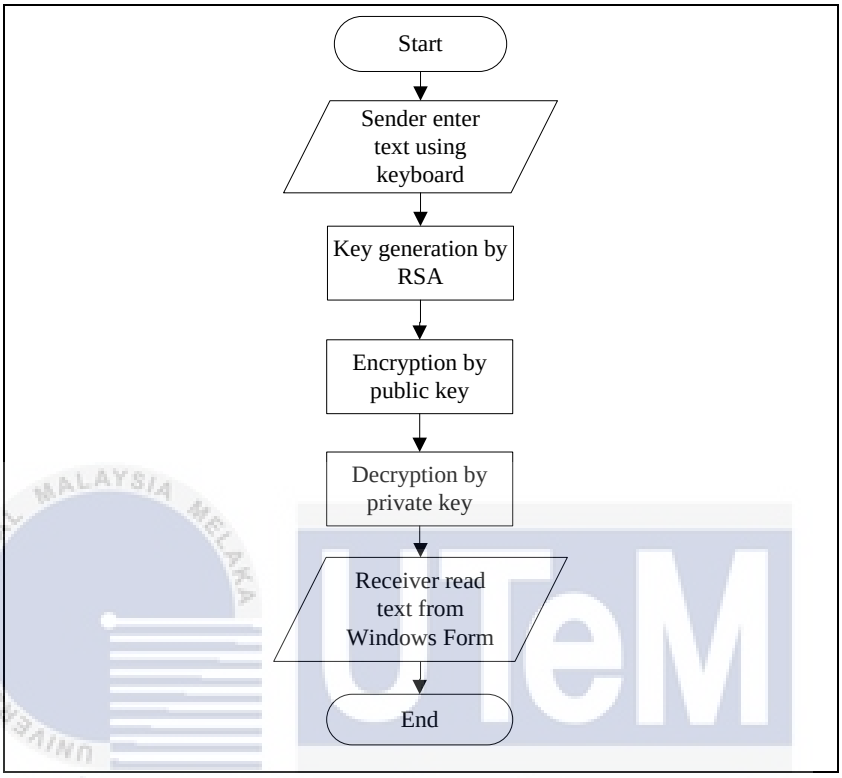


Figure 4.1: Flow Chart Diagram

4.3.2. Functional Requirement

Functional requirement described an interaction between the system and its environment. It described how the system should operate and what the user can expect and benefit from the system. The design of the modules and function must follow this requirement. The purpose of encryption and decryption using RSA algorithm is to secure the communication of the information. RSA algorithms was chosen in this project because the process to produce the private key from the public key is difficult. Thus, it is highly secured and difficult for the attackers to sabotaged.

The secured keyboard implement the data input from the keyboard to be encrypted through the Arduino Leonardo and sent to the computer for decryption. After the key was generated, the data will be encrypt by using the public key. Next, the decryption is to decrypt the cipher text using private key. In the interface, there is a button that called decrypt button. The decrypt button is to decrypt the encrypted data. This button will decrypt the cipher text using private key.

The Figure 4.2 below shows the data flow diagram. This system encrypt the data that user have entered by using the keyboard. When the data is entered, the data will be encrypted using the RSA algorithm by using the public key to encrypt the program. The encrypted will be transmitted to the computer for display. The decryption process will use a different key which is a private key to convert cipher text into plain text. After the decryption is done, the plain text will be shown in Windows Forms Application, Visual Basic and it is save in text file.

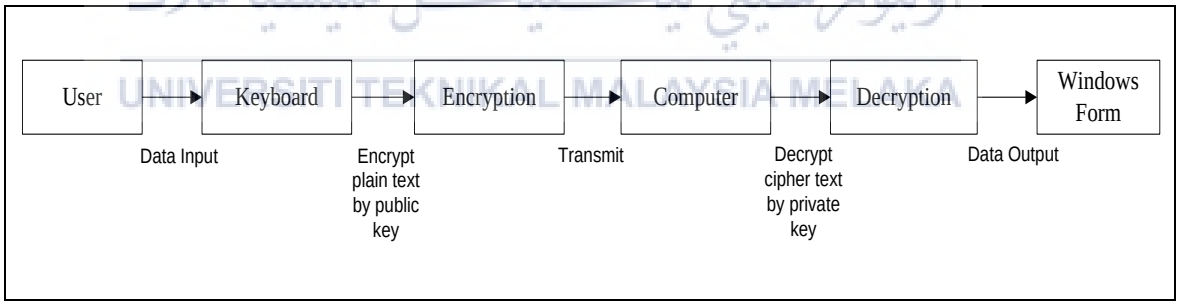


Figure 4.2: Data Flow Diagram

4.3.3. Non-functional Requirement

Non-functional requirement are usually called as a qualities of the system. The quality performance should be done effectively and efficiently. It must exceed the expectations and shown much improvement from the previous system. The qualities and the performance of the system should be done effectively and should run smoothly. The result of encryption and decryption process should be accurate so it will convince the user to use the system.

4.3.4. Others Requirement

Several types of software and hardware are used for implementation of this project. The software that are used in this project are Visual Basic, Microsoft Visio and Microsoft Office Word software meanwhile the hardware that is used in this project is a keyboard, Arduino Leonardo and Lenovo Personal Computer.

List of software :-

i. Visual Basic

   Visual Basic used for writing the coding of decryption.

ii. Microsoft Visio

   Microsoft Office Visio is used to draw diagrams such as flowchart, data flow diagrams and context diagrams.

iii. Microsoft Office Word

   Microsoft Office Word is used to make a report during developing the project.

List of hardware :-

i. Keyboard

User enter plain text and sent it to Arduino Leonardo.

ii. Arduino Leonardo

The Arduino Leonardo is a tool for configuring the encryption of the plain text and transmitting it to the computer for decryption.

iii. Lenovo Personal Computer

Personal computer is used for developing the project. Almost all tasks will be developed by using the computer.

4.4 High-Level Design

High-level view of the project systems structure is being discussed here. High level design explains more details about the process and component involved for the proposed solution. This design takes place in enhancing Arduino based secure keyboard using RSA algorithm. It also studies the architecture that would be used for developing a software.

4.4.1 System Architecture

The Figure 4.3 shows the keyboard encryption and decryption process. The encryption and decryption process used asymmetric RSA algorithm. The RSA Algorithm is used to create a private and public key . It is a type of asymmetric key cryptography. Public and private key must be generated before encryption process .User will input the data using keyboard and send to the Arduino to do the encryption module. The Arduino Leonardo will capture the plain text and encrypt to cipher text.

After the encryption process, the cipher text will be transmitted to the computer for decryption. Decryption process will be using private key to decrypt cipher text to plain text and be shown in Windows Forms ,Visual Basic. Finally, all the data will be save in the text file.

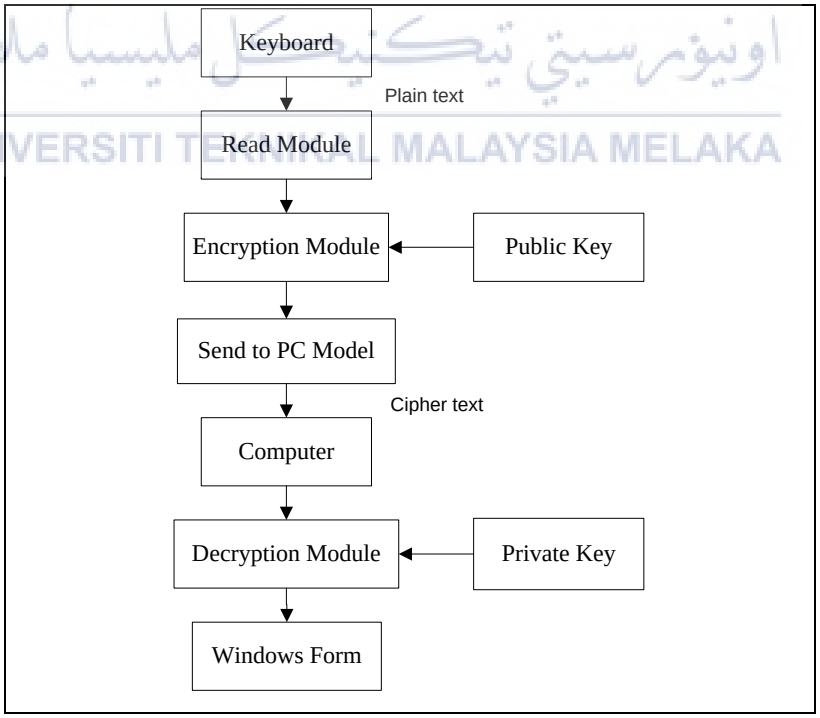


Figure 4.3: Keyboard Encryption and Decryption Process

4.4.2 Interface Design

The navigation design and output design is define here.

4.4.2.1 Navigation design

A keyboard will be used by the user to enter the data to Arduino Leonardo for encryption. When the user presses a key on the keyboard, the keyboard generates data . The keyboard are connected to the Arduino Leonardo. This data is received for encryption process which implement the RSA algorithm and display the cipher text on the computer screen for decryption process . The decryption will use a private key to convert cipher text into plain text. After decryption is done, the plain text will be shown in Windows Forms Application, Visual Basic and then it will save the encrypted and decrypted data in the text file.

4.4.2.2 Output design

The design for the output interface is shown in the Figure 4.4. The encrypted data will only be display on the text box encrypted message once the port is chosen for the decryption process. After decryption is done, the plain text shown in text box decrypted message . The decrypt button is for decryption process and save the data in text file.

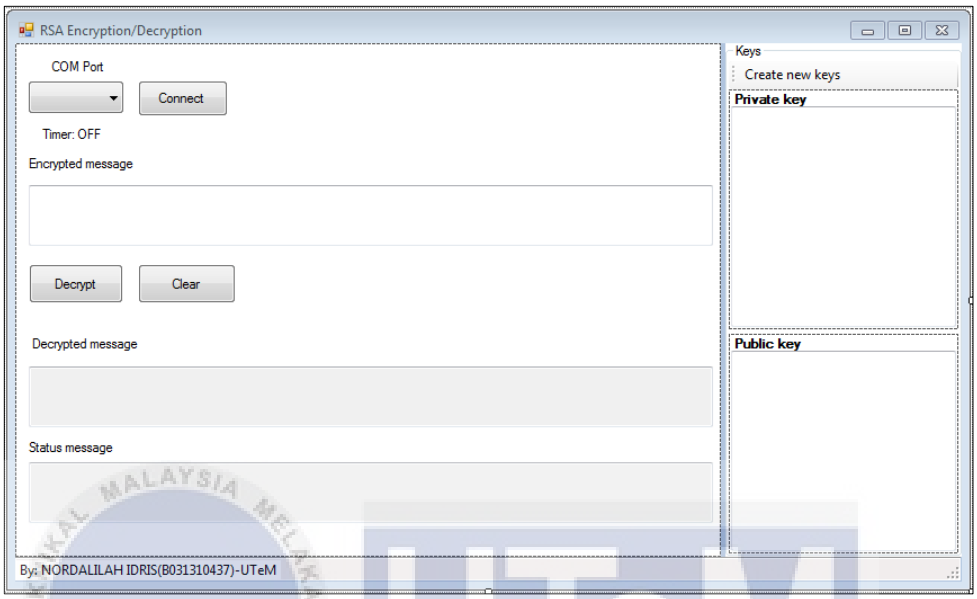


Figure 4.4: Output Design

4.5 Detailed Design

The development of enhancing Arduino based secure keyboard using RSA algorithm involve different key for encryption and decryption . This function shows how the system development of encryption and decryption process will be done.

4.5.1 Software Design

The Figure 4.5 shows the four class diagram of the system. First, user class consists of the name of the user input. Next, the input class which the user enter the plaintext. Then, the process class which is encryption. The process output there are encryption and decryption. Both of it using string. The output will be display in the Windows Form,

Visual Basic and save the encrypted and decrypted data in text file. The operation use the RSA algorithm for encryption and decryption process.

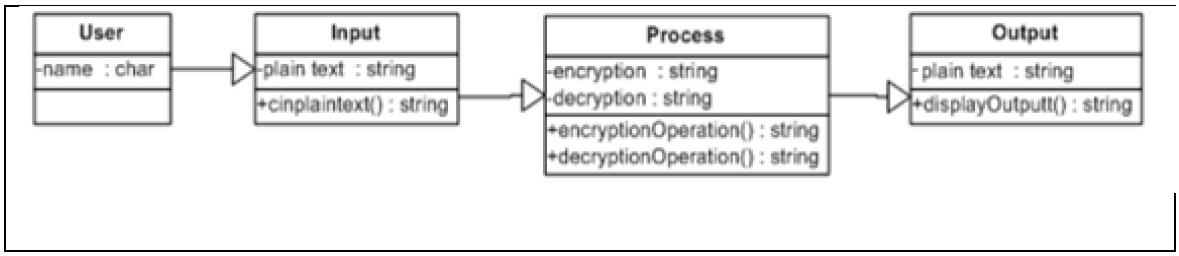


Figure 4.5: Class Diagram

4.6 Conclusion

This chapter mainly discuss about the project design and architecture. The data requirement, functional requirement and other requirement including software and hardware requirement has been explained here. The flow of the project is stated on the flow chart and navigation design diagram. For the next chapter, we will start implementing the process of development system activity. It will give the expected result after the completion of the implementation process.

CHAPTER V

IMPLEMENTATION

5.1 Introduction

This chapter will explain briefly about the implementation of the project on how the development processes take part. The activity involved in the implementation status is encryption and decryption. The implementation phase also is where all the component must be communicated with each other to receive the data that should be encrypted. After completing this phase , the data that have been received can only be decrypt by the private key of an encrypted message through the computer.

5.2 Software Development Environment Setup

Software development environment setup provides a detailed description of the platform that required hardware and software components that is used to implement this project. The tools needed in encryption process are keyboard, computer and the Arduino Leonardo hardware that help to run the project. A program used Arduino 1.6.8 (IDE) to create the programmed in the Arduino Leonardo.

The Arduino 1.6.8 (IDE) need to configure the board used which is Arduino Leonardo board. The programming used in this project is C programming language.

The hardware that involved in decryption process are Arduino Leonardo and computer. The software that have been installed in the computer is Visual Basic .After the encryption module have been made in Arduino, the data will be pass from Arduino to personal computer (PC) for decrypt the encrypted data. Figure 5.1 show the software development environment setup in RSA. The sender will enter the plaintext and undergoing encryption process by generating public key. The cipher text is produced after the plaintext undergo the encryption process. The decryption will be made in Visual Basic. Communication between Arduino and Visual Basic is using serial communication coding . Figure 5.2 shown how the decryption will be done to decrypt the encryption data. The data from Arduino Leonardo will be transfer using serial communication coding in C programming. In the recipient end, the plaintext will be converted to plaintext by decryption process. The decryption process will be using private key, and successful process will produce the right message content. The encrypted data will be done and decrypted data shown in Windows Form ,Visual Basic.

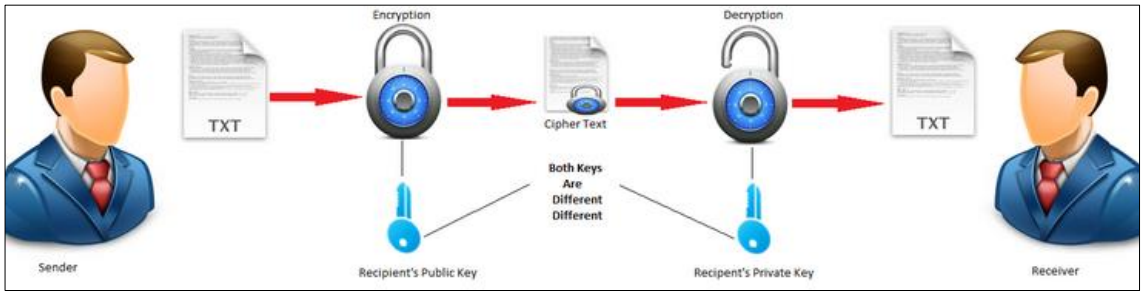


Figure 5.1: Software Development Environment Setup in RSA

Refer to Appendix B for the coding implementation of encryption and decryption.

5.3. Software Configuration Management

In this part this project will thoroughly explain about the design and the setup of the configuration management. This section also explained the software and hardware tool used to support configuration control.

5.3.1. Configuration environment setup

This section describes the implementation of data security system. The implementation of this project started when the Arduino 1.6.8. (IDE) is configured properly for encryption process. As an interaction medium, Arduino Leonardo is will be installed properly via a computer through the USB cable. The Arduino Leonard are programmed using the Arduino Software (IDE).Besides that, the tricky part in the configuration process is that the drivers need to be installed manually in the PC. This only apply for Windows version 7 because the board is not recognized. Serial port is virtual, it disappears when the board is reset. In particular, after initiating the auto-reset of the Leonardo the Arduino software, user must waits for a new virtual (CDC) serial / COM port to appear , one that it assumes represents the boot loader. It then performs the upload on this newly appeared port.

The connection between the keyboard and the Arduino Leonardo need to be programmed so that the Arduino Leonardo can read the data which was sent from the keyboard. The keyboard libraries and USB libraries have to be included in the Arduino Leonardo. Besides that, the developer also need to include the RSA libraries for encryption process.

Refer to Appendix A to configure environment setup. The figure 5.2 below shows the sketch of Arduino Leonardo.

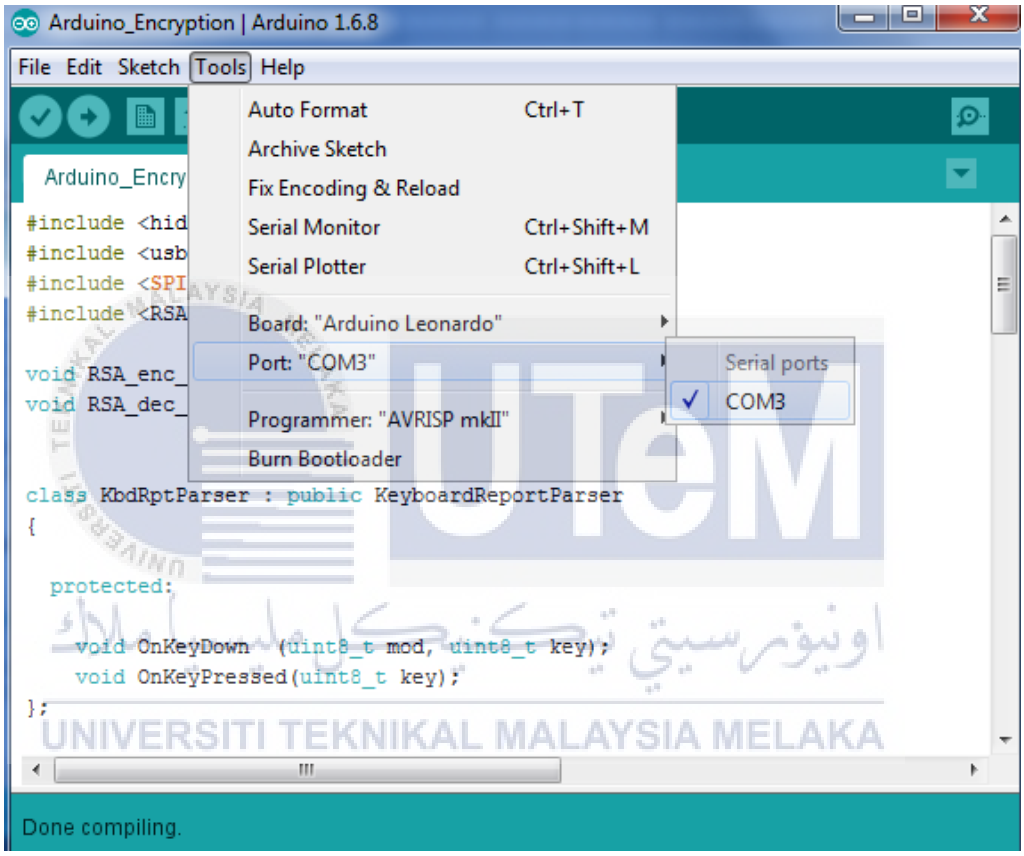


Figure 5.2: The sketch of Arduino Leonardo

Visual Basic installed for decryption process. The path should be accurate to avoid any error during configuration process. Figure 5.3 show the environment variable for Visual Basic . The path of the Visual Basic can be viewed here.

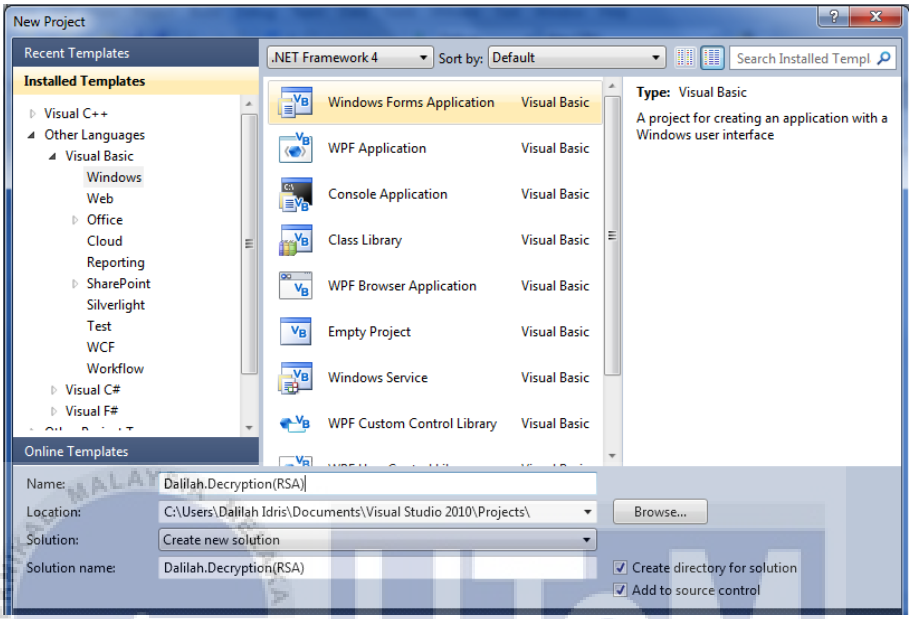


Figure 5.3: The path location in the Visual Basic

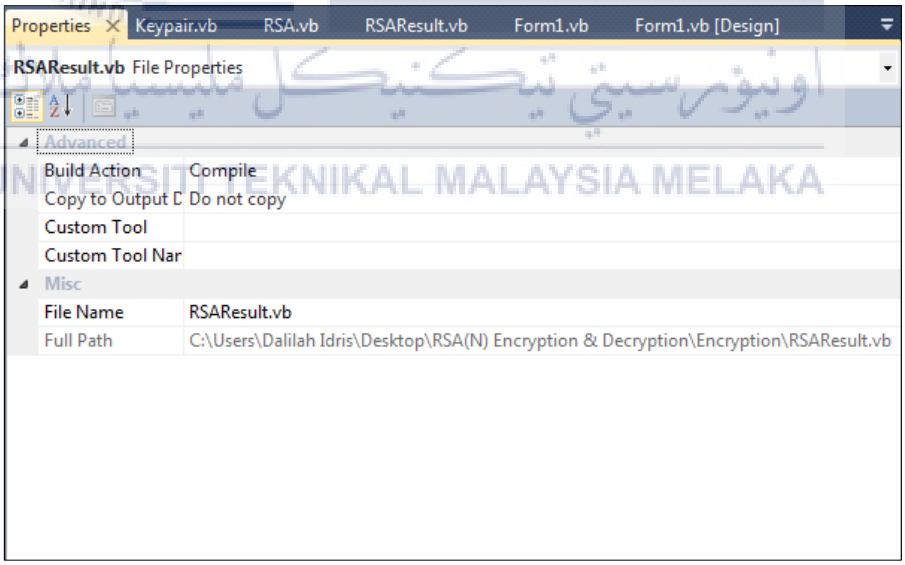


Figure 5.4: The file properties in the Visual Basic

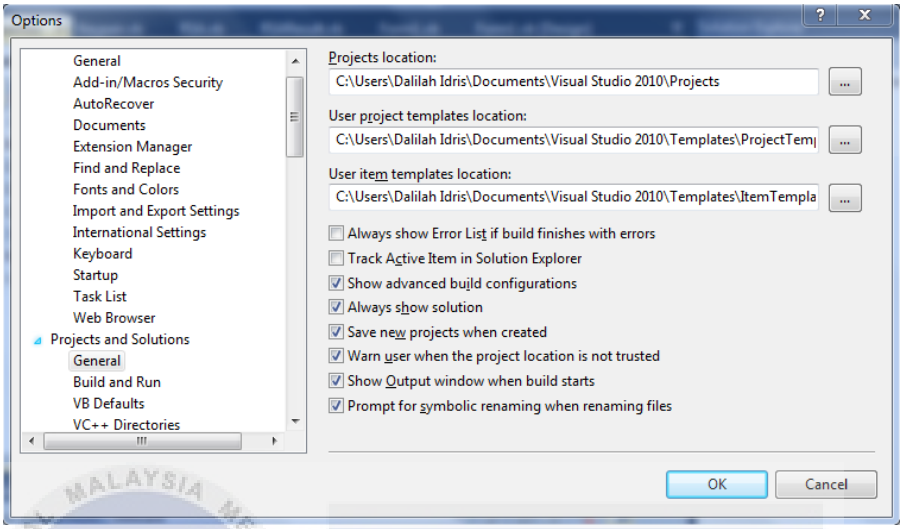


Figure 5.5: The project location in the Visual Basic

5.3.2 Version control procedure

The evaluation process for the system that are being develop is involved in the version control procedure. The Enhancing Arduino based secure keyboard using RSA algorithm for inspecting is the first project documented it is concluded as Version 1.0.

5.4 Implementation status

The progress of the development status is being stated in the Table 5.1. The status of the system is being measured by the module name, description of the module, duration to complete the module and the date for the module completely done.

Table 5.1: Progress of the development status

Module name	Description	Duration	Date completed
Read module	The Arduino Leonardo will read the user input of the keyboard	2 weeks	30 September 2016
Encryption module	The user enter the message and run the encryption process of RSA algorithm.	5 weeks	7 November 2016
Send to computer	The encrypted message will transmit into the computer for display encrypted data and decrypted the data.	2 weeks	18 November 2016
Communication between Arduino and Visual Basic	Serial communication by implementing the coding and to show the encryption module that made in Arduino can be shown in Windows Forms, Visual Basic.	4 weeks	3 March 2017
Decryption module	The decryption is to decrypt the encrypted data and show the plaintext of the encrypted data.	5 weeks	Not completed
Output shown in Windows Forms	The output which is plaintext shown in Windows Forms rather than console.	3 weeks	28 April 2017
Save in text file	Encrypted and decrypted data will save in text file.	2 weeks	12 May 2017

5.5 Conclusion

This chapter explained about the software development environment setup and software configuration management. The product have been implemented according to the designs, problem statement and objectives. The implementation status of the system is also being stated in this chapter. Implementation refers to the process of turning strategies and plans into action in order to achieve the objective of the project. The next chapter will discussed about testing phase and testing strategy of the system to determine if the customization is working properly.

CHAPTER VI

TESTING

6.1 Introduction

Testing is the final phase of this project development cycle. This chapter will discuss about the testing status of the project. In this chapter, this project will define activities involved in the testing phase and the result analysis after completing this phase. There are three important phase in testing module which are the test organization test, environment test and schedule test. This phase will determine whether the project functions achieve the requirement. The testing showed the test result of encryption using the Arduino Leonardo and decryption using Visual Basic.

6.2 Test Plan

There are three phases involved in the test plan that is test organization, test environment and test schedule. Each phase carry different task. The test plan is purposely to identify the testing that implemented and executed before launch the system. Test organization is to determine the user that involve in testing process.

Test environment consists of location or places to carry out the testing process and test schedule is arrangement for the duration and circle during testing process.

6.2.1 Test Organization

Test organization involves people to test the products that have been produced. The organization test is involving the group of people that has different experience in information technology . The people involved in the test organization is the system developer, users and the supervisor. The variety of people involved in testing phase is an advantages for evaluation of the secure keyboard development. Thus, the system can be improved so that the end users can use the system easily.

6.2.2 Test Environment

Test environment describe the location and environment for the testing process take place. This project is fully testing in windows environment. The environment of testing process consists of seven modules. These module are:

- Read module
- Encryption module
- Send module
- Communication between Arduino and Visual Basic
- Decryption module.
- Output shown in Windows Form
- Data save in the text file.

The hardware that required for test environment are listed in table 6.1.

Table 6.1: Component of hardware used

Hardware	Description
Keyboard	Provided by UTEM
Arduino Leonardo	Provided by UTEM
Cable USB	Provided by UTEM
Computer	LENOVO Z470

The software that required for test environment are listed in table 6.2.

Table 6.2: Component of software used

Software	Description
Visual Basic	Version 10
Arduino Leonardo	Arduino Version 1.6.8

6.2.3 Test Schedule

Test schedule was arranged to ensure the testing process can be handled .It is used to guide the developer to make sure the testing can be done in a time given. The purpose of the test schedule is to detect any error or problem of the system before it can be used by the users. The table 6.3 show the test schedule of this project.

Table 6.3: The test schedule

Module name	Duration	Test start date	Test data completed
Read module	2 days	28 September 2016	30 September 2016
Encryption module	5 days	2 November 2016	7 November 2016
Send module	2 days	16 November 2016	18 November 2016
Communication between Arduino and Visual Basic	6 days	27 February 2017	3 March 2017
Decryption Module	5 days	2 April 2017	Not completed
Output shown in Windows Forms, Visual Basic	4 days	24 April 2017	28 April 2017
Data save in the text file	2 days	10 May 2017	12 May 2017

6.3 Test Strategy

In this section, test strategy is an outline to help in facilitating the communication of the process and its effect on the entire project. Data security system will using White-box testing. White-box testing is a software testing that utilizes specific knowledge of programming code to inspect output. The test is exact just if the tester recognizes what the system should do. White box testing does not represent the error created by oversight, and all unmistakable code should likewise be coherent. The advantages of

White-Box testing is it forces test developer to reason carefully about implementation. This testing will reveals errors and mistakes in the code and helps in improving the code. However, this test is expensive as one has to spend both time and money to perform this test and this testing also must have in-depth knowledge about the programming language as this testing required code access.

6.3.1 Classes of Tests

In this section, several user are selected to do the testing based on the modules. Table 6.4 below shows the module for test the project functionality.

Table 6.4: The module and expected result

Module name	Description
Read module	Arduino Leonardo read data from the keyboard
Encryption module	The user enter the data and run the encryption process of RSA algorithm.
Send to computer	The encrypted data will be transmitted into the computer for display.
Communication between Arduino and Visual Basic	Implement serial communication coding in Visual Basic to read and receive the data from Arduino.
Decryption module	The encrypted data from Arduino decrypt to plain text using decryption coding in Visual Basic.
Output shown in Windows Forms Visual Basic	The output which is plaintext shown in Windows Forms rather than console.

Data save in the text file	Encrypted and decrypted data will be save in the text file.

6.4 Test Design

Test design refers to test the reliability of on every systems application from the design perspective. It is a detailed process to ensure all the modules functioning properly.

6.4.1 Test Description

The test description is to show the modules test in this project. The table 6.5 show the modules, test ID, test case and description about the module will be expected output.

Table 6.5: The test id ,module test, test case and description

Test ID	Modules	Test Case	Description
ED_01	Read module	Functional	Arduino Leonardo able to read data from the keyboard
ED_02	Encryption module	Functional	The data input able to encrypt
ED_03	Send to computer	Functional	Able the data encrypted display in serial monitor of computer
ED_04	Communication between Arduino and Visual Basic.	Functional	Serial communication between Visual Basic and Arduino is able to send data
ED_05	Decryption module	Not Functional	The decryption process is to decrypt the encrypted data
ED_06	Output shown in Windows Forms	Functional	The output shown in Windows Forms.

ED_07	Data save in the text file	Functional	Encrypted and decrypted data will be save in the text file.

6.4.2 Test Data

The data is real testing that is used as input for secure keyboard project. Test data used to testing modules of the project. Tables below show the description of all test modules.

Table 6.6: Read Modules

Test ID	Test Case	Tasks	Actual output
ED_01	Functional	Arduino Leonardo able to read the data from the keyboard	The Arduino Leonardo successfully read the data from the keyboard

Table 6.7: Encryption Modules

Test ID	Test Case	Tasks	Actual output
ED_02	Functional	The data input able to encrypt	The user enter the data and run the encryption process of RSA algorithm. The data will be displayed in cipher text.

Table 6.8: Send Modules

Test ID	Test Case	Tasks	Actual output
ED_03	Functional	Enabling the encrypted data to be displayed in serial monitor of computer.	The encrypted data display in serial monitor of computer is successful.

Table 6.9: Communication between Arduino and Visual Basic

Test ID	Test Case	Tasks	Actual output
ED_04	Functional	Serial communication between Visual Basic and Arduino enabling to send data and receive data.	Serial communication between Visual Basic and Arduino is success to send data and receive data.

Table 6. 10: Decryption module

Test ID	Test Case	Tasks	Actual output
ED_05	Not Functional	Decrypt the encrypted data from Arduino.	The decryption cannot decrypt the encrypted data.

Table 6.11: Output show in Windows Forms

Test ID	Test Case	Tasks	Actual output
ED_06	Functional	The output of decryption shown Windows Forms.	The output is successfully shown in Windows Forms.

Table 6.12: Data save in text file

Test ID	Test Case	Tasks	Actual output
ED_07	Functional	Data save in the text file.	The output is successfully save in text file.

6.5 Test Result and Analysis

Test result and analysis explained about test case identification, tester identification, and the result whether the system was success or failed. It consists of expected output and description of user feedback. The result is displayed in table 6.13

Table 6.13: Test Result

Test ID	Tester Identification	Result(Pass/Failed))
ED_01	OK	Pass
ED_02	OK	Pass
ED_03	OK	Pass
ED_04	OK	Pass
ED_05	Not OK	Failed
ED_06	OK	Pass
ED_07	OK	Pass

Analysis on failed test case for decryption module, apparently the module has failed. The coding have been made however the coding of decryption cannot convert the encrypted data. The encrypted data is an unknown data. Research have been made and still the data cannot decrypt to plaintext. The limitation of knowledge about programming and how the Arduino works also is one of the cause the module failed. The information obtained to solve the problem is limited and not all of the information is helpful. It is really hard to find information since this is a new products and not everyone is familiar with Arduino hardware .

6.6 Conclusion

In conclusion, this chapter discuss about the test plan, test strategy, test design and test result of this system. White-Box testing is used as a test strategy in this project because this type of testing will reveals errors and mistakes in the code and helps in improving the code. The test result show that the system is running smoothly without any error. The elements in this chapter are important for the tester to make sure the project meet the entire requirement after the implementation phase. Testing processes identify and verify the weakness and improvement in the system. The next chapter will conclude overall conclusion about this system. The topic that should be discuss is project summarization, project contribution, project limitation and future works.

CHAPTER VII

PROJECT CONCLUSION

7.1 Introduction

This chapter will discuss all the project summarization, project contribution, project limitation, future work and conclusion. Project summarization will be described how the objective has been achieved by integrating the information that have reported in the implementation and testing phase. It is also stated that the intention of this project is to contribute to the university and faculty. The strength and the weaknesses of the project was also being discussed here. Every system that has been developed has its own advantages and disadvantages . Advantages are mainly about the system strengths and disadvantages are about the system weakness.

7.2 Project Summarization

The successfully of a project depends on the objective of the project. This project achieve the objective to enhance Arduino based secure keyboard, to design secure algorithm that can be used to protect information during the transmission and to develop encryption and decryption model of secure keyboard using asymmetric key for secure

data transmission .This system the keyboard received the plain text input from the user. Then, the data input transmitted into the Arduino Leonardo for the encryption process. The key was generated by using RSA algorithms. In this phase, the public key and private key is calculated. Hash value is also being calculated at the same time. After that, the encryption process is done by using the public key. The cipher text will transmit to the computer for display the encrypted data.

For decryption process, user can decrypt the cipher text by using sender private key. Then user will calculate the hash value of the encrypted data and compare it with the hash value of the sender. If the hash value of the receiver same with the hash value of the sender, then the data is safe and have not been modified by other user. Decryption process will be using private key to decrypt cipher text to plain text and be shown in Windows Form ,Visual Basic. Lastly, all data will be save in text file. The decryption part using RSA algorithm. Such cryptosystem will have two different keys to accomplish a secure communication between two parties which one of them is called encryption key and made public while the other called decryption key and made private. This system will enhancing Arduino based secure keyboard using RSA algorithm thus it secure the content of the information from unauthorized user.

7.3 Project Contribution

This system may become a great platform for the user which can protect their keyboard from being captured by other people. Enhancement module for the previous secure keyboard project by applied RSA algorithm in encrypting and decrypting on a secure keyboard . Development of a secure keyboard data input and output in keyboard communication will be encrypted and decrypted. Thus, the user input communication

between the computers will be encrypted and data integrity of user can be protected from other attack especially from key logger attack.

7.4 Project Limitation

The limitation of this project is that the developer cannot handle several things related to this project due to lack of information about the system and time constraint. The project need to be completed as soon as possible however, there is always a problems that come ahead and delay the project from completion.

7.5 Future Works

For the future works, the suggestion that can be made is to build in the Arduino in the keyboard, so it easy to carry anywhere and do not need to assemble one by one. This system may become a great platform if encrypted system was implemented in the keyboard without connected to the Arduino Leonardo. Next, rather than doing the decryption module in separated platform, the decryption module can be made in one platform only which is in Arduino. There is no need to use serial communication to communicate between Arduino and another platform. It just took a longer time to be executed.

7.6 Conclusion

In conclusion, this system provide data security using RSA algorithm. Finally, this project is successfully done. Praise to Allah for His Blessing. Special thanks to my ever patient and dedicated supervisor because the system and report is successfully completed. This system will bring advantage to the user who want to have their data protected. There is no security in this technology era. There is only an opportunity for the hacker to crack and enter the system to destroy and steal crucial information. The only thing that the developer can do is to provide a system that can help the user to secure his or her information. So, both of the objectives of this project was achieved and this system can be improved given time in the near future.

REFERENCES

1. Al-Haija, Q.A. et al., 2014. A tiny RSA cryptosystem based on arduino microcontroller useful for small scale networks. *Procedia Computer Science*, 34(Eicm), pp.639–646.

2. Bernd Grossmann, R.W., 2010. Keyboard and method for secure transmission of data. , (2), pp.2–7.

3. Cheung, F., 2004. Method and system for data encryption and decryption. , pp.1–7.

4. Christopher Reon Gentle, J.J.O., 2001. Method and Apparatus for and encrypting keyboard. , 1(12), pp.1–7.

5. Deshpande, a. M., Deshpande, M.S. & Kayatanavar, D.N., 2009. FPGA implementation of AES encryption and decryption. *2009 International Conference on Control, Automation, Communication and Energy Conservation*, (June), pp.1–6.

6. Eduardo S. Pinheiro, 2010. Secure keyboard. , pp.1–7.

7. Examiner-alan, P. & Richardson, P.C., 1998. METHOD AND SYSTEM FOR AUTHORIZING GENERATION OF ASYMMETRIC CRYPTO-KEYS. , 2(12).

8. Higinio Rubio,Enrique Soriano, R.B., 2015. a Low Cost Lab Monitoring System Based on Arduino Microcontroller and Android. , (NOVEMBER), pp.8014–8022.

9. Lee, J., Piponi, D. & Aminzade, D., 2014. Method and apparatus for secure data input and output. , pp.1–9.

10. Lior Frenkel, A.Z., 2016. Encryption - and decryption - enabled interfaces. , pp.1–12.

11. Martin, L., Torres, L. & Robert, M., 2002. HYBRID CRYPTOGRAPHIC TECHNIQUEUSINGRSA ALGORITHMAND SCHEDULING CONCEPTS. , 42(0), pp.92–100.

12. Meenakshi Shankar, A., 2001. Priority Based RSA Cryptographic Technique. , 345(7), pp.534–535.

13. Nitin V Sarangdhar, J.C., 2015. Protecting keystrokes received from a keyboard in a platform containing embedded controllers. , pp.1–8.

14. Peinado, M. & Benaloh, J., 2007. Secure communication with a keyboard or related device. , pp.1–9.

15. Rahman, M., Saha, T.K. & Bhuiyan, A., 2012. Implementation of RSA Algorithm for Speech Data Encryption and Decryption. , 12(3), pp.74–82.

16. Ravinderpal Singh Sandhu, Oak Hill Va , Desa, C.J., 2010. MULTIFACTOR SPLIT ASYMMETRIC CRYPTO-KEY WITH PERSISTENT KEY SECURITY. , 2(12).

17. Schneier, B., 1996. Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security.

18. Schubert, T.W., D'Ausilio, A. & Canto, R., 2013. Using Arduino microcontroller boards to measure response latencies. *Behavior research methods*, 45(4), pp.1332–46. Available at: http://www.ncbi.nlm.nih.gov/pubmed/23585023.

19. Thakur, J. & Kumar, N., 2011. DES, AES and Blowfish: Symmetric key

cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, 1(2), pp.6–12.

20. Wu, C.H., Hong, J.H. & Wu, C.W., 2001. RSA cryptosystem design based on the Chinese remainder theorem. *Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC*, 2001-Janua(February), pp.391–395.

21. Yongo E., Manyala J.O., K. Kito., Y. Matsushita., Outa N.O., N.J.., 2016. Rsa Cryptography Algorithm Using Linear Congurence Class. *International Journal of Advanced Research*, 4(4), pp.144–149.

APPENDIX A

1. User manual for environment setup of encryption module .
   i. Install the Arduino Leonardo 1.6.8. (IDE) in the computer.
   ii. Configure the board in Arduino 1.6.8 (IDE) which is Arduino Leonardo

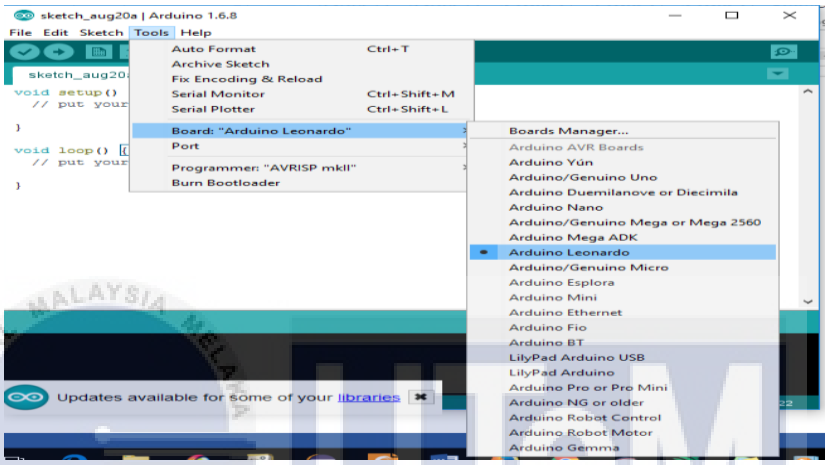


Figure 1: Select the Arduino Leonardo Board

iii. Check the port of Arduino Leonardo used in Device

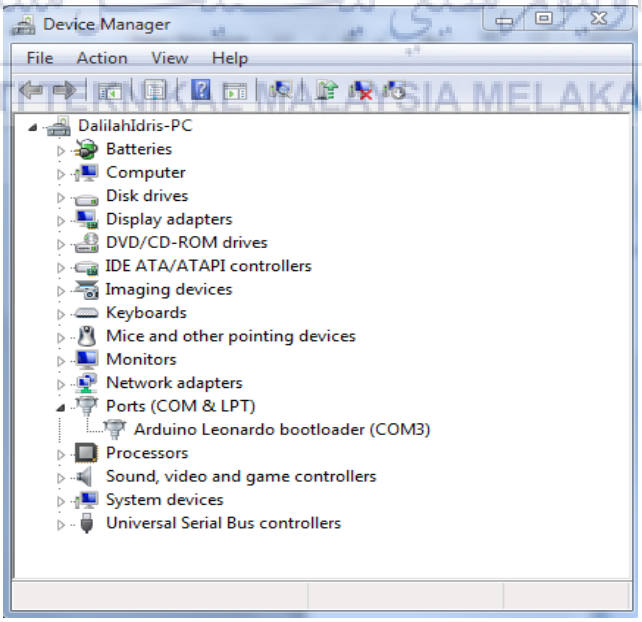


Figure 2: show the port of Arduino Leonardo used

iv. Select the port COM3 for Arduino Leonardo in Arduino IDE

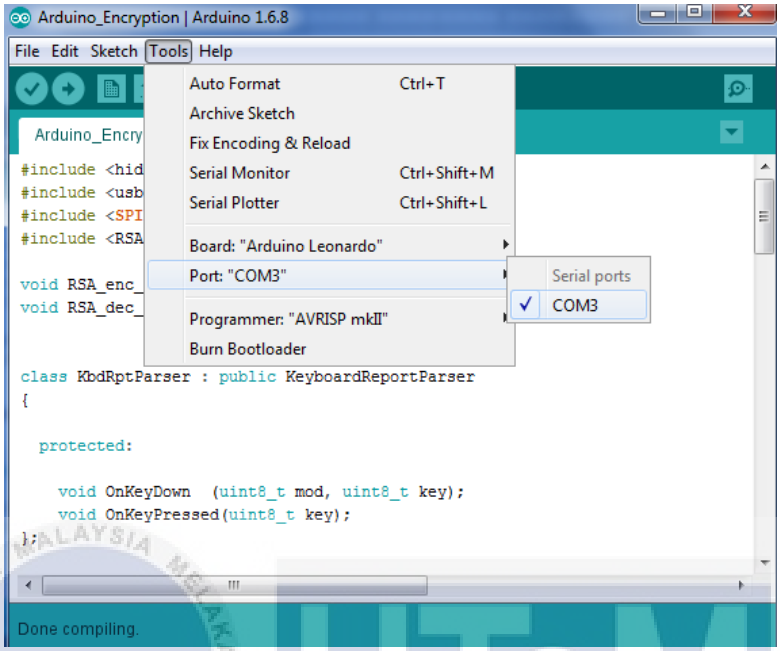


Figure 3: Select the port COM3 of Arduino Leonardo in Arduino IDE

v. Download keyboard library in library Manager of the Arduino Leonardo

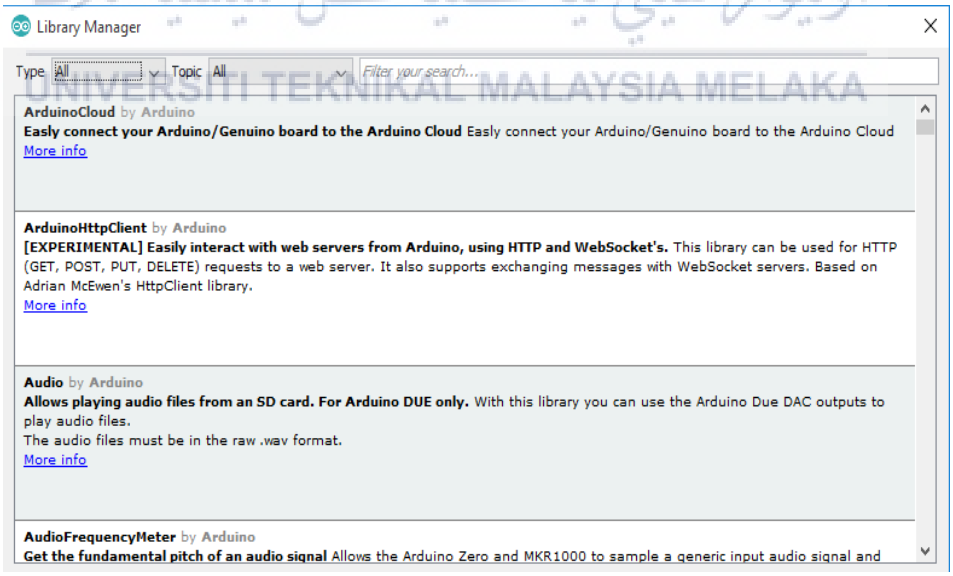


Figure 4 Show library Manager of the Arduino Leonardo

2. User manual for environment setup of decryption module

   i. Connect Arduino Leonardo to the computer.
   ii. Open device manager to see the port that Arduino Leonardo used.
   iii. Open Visual Basic
   iv. Find the port for windows.
   v. Change the port for Arduino Leonardo, example, port 22 in the serial communication coding.
   vi. Run the coding.
   vii. The output of decrypted data shown in the Windows Form Application , Visual Basic.

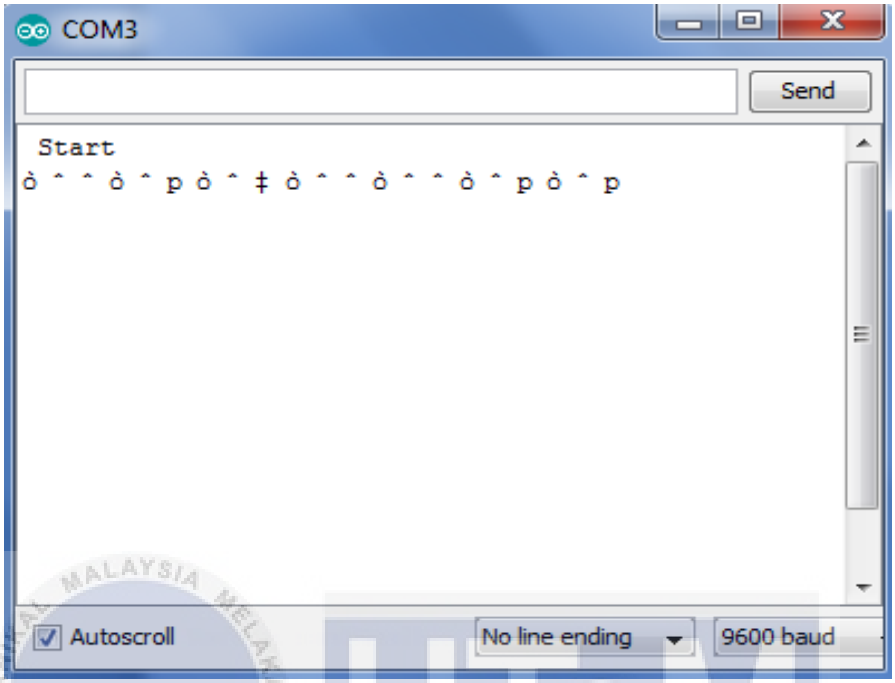
APPENDIX B

1. The source code and implementation of encryption process in Arduino Leonardo.

```
#include <hidboot.h>
#include <usbhub.h>
#include <SPI.h>
#include <RSA.h>

void RSA_enc_single(const uint8_t* key,void* data);
void RSA_dec_single(const uint8_t* key,void* data);

class KbdRptParser : public KeyboardReportParser
{

  protected:

    void OnKeyDown  (uint8_t mod, uint8_t key);
    void OnKeyPressed(uint8_t key);
};


void KbdRptParser::OnKeyDown(uint8_t mod, uint8_t key)
{

  uint8_t c = OemToAscii(mod, key);

  if (c)
    OnKeyPressed(c);
}

void KbdRptParser::OnKeyPressed(uint8_t key)
{

    char plainchar[PLAINTEXT_SIZE];
    String data;
    data=String(key);
    data.toCharArray(plainchar,PLAINTEXT_SIZE);

    char cipher_msg[CIPHERTEXT_SIZE];

    //Keys
    int publicKey[2] = {14351, 11};
    int privateKey[2] = {14351, 1283};
```

```
    //Encrypt code
    rsa.encrypt(plainchar, cipher_msg, publicKey);

    //Encrypted Message :
    for(int i = 0; i < CIPHERTEXT_SIZE; i++)

    //Serial.write
    (cipher_msg[i]);
     Serial.print(cipher_msg);

};

USB     Usb;
//USBHub     Hub(&Usb);
HIDBoot<USB_HID_PROTOCOL_KEYBOARD>    HidKeyboard(&Usb);

KbdRptParser Prs;


void setup()
{
  Serial.begin( 9600 );

#if !defined(__MIPSEL__)
  while (!Serial); // Wait for serial port to connect
#endif
  Serial.println(" Start ");

  if (Usb.Init() == -1)
    Serial.println("OSC did not start.");

  HidKeyboard.SetReportParser(0, &Prs);
}

void loop()
{
  Usb.Task();
}
```

The output for this program :-



2. Coding for serial communication and decryption process in Visual Basic .

```
Imports System.Security.Cryptography
Imports Encryption.RSA
Imports System
Imports System.IO.Ports
Imports System.IO

Public Class Form1

    Dim comPORT As String
    Dim receivedData As String = ""

    Private Sub Form1_Load(
    ByVal sender As System.Object,
    ByVal e As System.EventArgs) Handles MyBase.Load

        CreateNewKeys()

        Timer1.Enabled = False
        comPORT = ""
        For Each sp As String In My.Computer.Ports.SerialPortNames
            comPort_ComboBox.Items.Add(sp)
        Next
    End Sub

Private Sub comPort_ComboBox_SelectedIndexChanged(
ByVal sender As Object,
ByVal e As EventArgs) Handles comPort_ComboBox.SelectedIndexChanged

    If (comPort_ComboBox.SelectedItem <> "") Then
        comPORT = comPort_ComboBox.SelectedItem
    End If
End Sub

Private Sub connect_BTN_Click(
ByVal sender As Object, ByVal e As EventArgs) Handles connect_BTN.Click

    If (connect_BTN.Text = "Connect") Then
        If (comPORT <> "") Then
            SerialPort1.Close()
            SerialPort1.PortName = comPORT
            SerialPort1.BaudRate = 9600
            SerialPort1.DataBits = 8
            SerialPort1.Parity = Parity.None
            SerialPort1.StopBits = StopBits.One
            SerialPort1.Handshake = Handshake.None
            SerialPort1.Encoding = System.Text.Encoding.Default
            SerialPort1.ReadTimeout = 10000
```

```
            SerialPort1.Open()
            connect_BTN.Text = "Dis-connect"
            Timer1.Enabled = True
            Timer_LBL.Text = "Timer: ON"
        Else
            MsgBox("Select a COM port first")
        End If
    Else
        SerialPort1.Close()
        connect_BTN.Text = "Connect"
        Timer1.Enabled = False
        Timer_LBL.Text = "Timer: OFF"
    End If
End Sub
```

```
Function ReceiveSerialData() As String
    Dim Incoming As String
    Try
        Incoming = SerialPort1.ReadExisting()
        If Incoming Is Nothing Then
            Return "nothing" & vbCrLf
        Else
            Return Incoming
        End If
    Catch ex As TimeoutException
        Return "Error: Serial Port read timed out."
    End Try

End Function
```

```
Private Sub COMport_LBL_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles COMport_LBL.Click

End Sub
```



```
Private Sub Timer1_Tick(
ByVal sender As Object, ByVal e As EventArgs) Handles Timer1.Tick
    receivedData = ReceiveSerialData()
    txtMessageEncrypt.Text &= receivedData
End Sub
```

```
Private Sub clear_BTN_Click(
ByVal sender As Object, ByVal e As EventArgs) Handles clear_BTN.Click
    txtMessageEncrypt.Text = ""
End Sub
```

```
Private Sub btnNewKeys_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles btnNewKeys.Click
    CreateNewKeys()
End Sub
```

```
Private Sub CreateNewKeys()
    Dim Keys As Encryption.Keypair = Encryption.Keypair.CreateNewKeys
    txtPrivateKey.Text = Keys.Privatekey
    txtPublicKey.Text = Keys.Publickey
End Sub
```

```
Private Sub EncryptMessage()
    Try
        Dim EncryptedMessage As Encryption.RSAResult = Encryption.RSA.Encrypt(txtMessageEncrypt.Text,
                                                                              txtPublicKey.Text)
        Dim DecryptedMessage As Encryption.RSAResult = Encryption.RSA.Decrypt(EncryptedMessage.AsBytes,
                                                                              txtPrivateKey.Text)
        txtDecryptedMessage.Text = DecryptedMessage.AsString
        txtErrorMessage.Text = "OK"
    Catch ex As Exception
        txtErrorMessage.Text = ex.Message
    End Try
End Sub
```

```
Private Sub Button1_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles btnDecrypt.Click

    EncryptMessage()
    Dim FileWriter As StreamWriter
    Dim results As DialogResult
    results = SaveFileDialog1.ShowDialog

    If results = DialogResult.OK Then
        FileWriter = New StreamWriter(SaveFileDialog1.FileName, False)
        FileWriter.WriteLine("Encrypted Message :")
        FileWriter.WriteLine(txtMessageEncrypt.Text)
        FileWriter.WriteLine("Decrypted Message :")
        FileWriter.WriteLine(txtDecryptedMessage.Text)

        FileWriter.WriteLine("Private Key :")
        FileWriter.WriteLine(txtPrivateKey.Text)
        FileWriter.WriteLine("Public Key : ")
        FileWriter.WriteLine(txtPublicKey.Text)
        FileWriter.Close()
    End If
End Sub
```

```
Private Sub SplitContainer1_Panel1_Paint(
ByVal sender As System.Object,
ByVal e As System.Windows.Forms.PaintEventArgs) Handles SplitContainer1.Panel1.Paint

End Sub

Private Sub txtPrivateKey_TextChanged(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles txtPrivateKey.TextChanged

End Sub
Private Sub ToolStrip1_ItemClicked(
ByVal sender As System.Object,
ByVal e As System.Windows.Forms.ToolStripItemClickedEventArgs) Handles ToolStrip1.ItemClicked

End Sub

Private Sub txtMessageEncrypt_TextChanged(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles txtMessageEncrypt.TextChanged

End Sub

Private Sub Label4_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles Label4.Click

End Sub

Private Sub txtEncryptedBase64_TextChanged(
ByVal sender As System.Object,
ByVal e As System.EventArgs)

End Sub

Private Sub Label5_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles Label5.Click

End Sub

Private Sub txtDecryptedMessage_TextChanged(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles txtDecryptedMessage.TextChanged

End Sub

Private Sub Label6_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles Label6.Click

End Sub
```

```
Private Sub txtErrorMessage_TextChanged(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles txtErrorMessage.TextChanged

End Sub
```

```
Private Sub SplitContainer2_SplitterMoved(
ByVal sender As System.Object,
ByVal e As System.Windows.Forms.SplitterEventArgs) Handles SplitContainer2.SplitterMoved

End Sub
```

```
Private Sub ToolStripStatusLabel1_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles ToolStripStatusLabel1.Click

End Sub
```

```
Private Sub StatusStrip1_ItemClicked(
ByVal sender As System.Object,
ByVal e As System.Windows.Forms.ToolStripItemClickedEventArgs) Handles StatusStrip1.ItemClicked

End Sub
```

```
Private Sub Label2_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles Label2.Click

End Sub
```

```
Private Sub txtPublicKey_TextChanged(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles txtPublicKey.TextChanged

End Sub
```

```
Private Sub Label1_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles Label1.Click

End Sub
```

```
Private Sub SplitContainer1_SplitterMoved(
ByVal sender As System.Object,
ByVal e As System.Windows.Forms.SplitterEventArgs) Handles SplitContainer1.SplitterMoved

End Sub
```

```
Private Sub GroupBox1_Enter(
ByVal sender As System.Object,
ByVal e As System.EventArgs) Handles GroupBox1.Enter

End Sub
```

```
Private Sub Label3_Click(
ByVal sender As System.Object,
ByVal e As System.EventArgs)

End Sub
```

```
    Private Sub btnDecrypt_Click(
    ByVal sender As System.Object,
    ByVal e As System.EventArgs) Handles btnDecrypt.Click

    End Sub

    Private Sub btnEncrypt_Click(
    ByVal sender As System.Object, ByVal e As System.EventArgs)

    End Sub
End Class
```

The output for this program : -