DEVELOPING SECURE KEYBOARD USING ARDUINO LEONARDO; ENCRYPTION MODULE

NAFEESA HUSNA BINTI ABDUL RAUB

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS TESIS*

JUDUL : Developing Secure Keyboard using Arduino Leonardo; Encryption Module

SESI PENGAJIAN: 2015/2016

Saya __ NAFEESA HUSNA BINTI ABDUL RAUB___________

(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 14,jalan 6b/11 seksyen
16,43650 bandar baru bangi

Tarikh : 23/8/2016

(TANDATANGAN PENYELIA)

MOHD ZAKI BIN MAS'UD

(Nama Penyelia)

Tarikh : 23/8/2016

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

DEVELOPING SECURE KEYBOARD USING ARDUINO; ENCRYPTION MODULE

NAFEESA HUSNA BINTI ABDUL RAUB

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

2016

DECLARATION

I hereby declare that this project report entitled

DEVELOPING SECURE KEYBOARD USING ARDUINO LEONARDO; ENCRYPTION MODULE

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

STUDENT : ______________________________ Date: 23/8/2016

(NAFEESA HUSNA BINTI ABDUL RAUB)

SUPERVISOR : ______________________________ Date : 23/8/2016

(MOHD ZAKI BIN MAS'UD)

DEDICATION

This thesis is dedicated to my beloved family who never failed to give me financial and moral support, for giving all my need during the time I am developing my system. A lot of thanks for teaching us that even the largest task can be accomplished if it is done one step at a time.

Without their patience, understanding, support, and most of all love, the completion of this project would not have been possible.

This dedication is also dedicated for all colleagues who help on giving advices and their point of views during the system developed.

Thank you

ACKNOWLEDGEMENT

I like to thank my supervisor, Mr Mohd Zaki bin Mas’ud for giving me a support, guidance and encouragement to complete my project. Special thanks also to my graduate friends, especially to my classmate for sharing the literature and invaluable assistance. Not forgetting to my best friends who always been there. Thank you for giving me inspiration, motivation and endless support.

I would also like to thank to Universiti Teknikal Malaysia Melaka for giving permission to borrow the hardware that need for my project needed. This accomplishment would not have been possible without them.

Thank you for my family who had given me all the supports that I need not only to complete this project but also from the very beginning of my life in Universiti Teknikal Malaysia Melaka

ABSTRACT

In this project, the system defines the secure keyboard The development of this project is using an additional hardware which is Arduino Leonardo and the keyboard for user input The keyboard input will be transmitted and implemented into Arduino Leonardo and were sent to the computer. Besides that, the system also used the Advanced Encryption Standard (AES) algorithm to encrypt the data from the keyboard. The secure keyboard by encryption helps to protect the communication between the input keyboard and the computer. The non-secure keyboard communication can easily be attacked. .An example of the attacked is an attack from a key logger. A key logger function is to capture each human interface device input and monitor it. Therefore, the process for development of the system follows as Rapid Application Development (RAD) method and Joint Application Development (JAD) methods to accelerate system development.

ABSTRAK

Dalam projek ini, sistem ini mentakrifkan keselamatan papan kekunci Projek ini menggunakan perkakasan tambahan iaitu Arduino Leonardo dan papan kekunci untuk masukkan data pengguna. Input papan kekunci akan menghantar dan melaksanakannya ke Arduino Leonardo dan seterusnya menghantar ke komputer . Selain itu, sistem ini juga menggunakan algoritma Advanced Encryption Standard (AES) untuk penyulitan data. Papan kekunci selamat dengan penyulitan dan membantu melindungi komunikasi antara kemasukan data dan komputer. Komunikasi papan kekunci tidak selamat dan boleh diserang dengan mudah.Contoh serangan adalah seperti serangan dari keylogger. Fungsi keylogger adalah untuk memerangkap setiap input perkakasan antaramuka manusia dan memantaunya. Oleh itu, proses untuk pembangunan sistem ini dengan menggunakan kaedah Pembangunan Aplikasi Rapid (RAD) dan kaedah Pembangunan Aplikasi Bersama (JAD) untuk mempercepatkan pembangunan sistem.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

CHAPTER I

INTRODUCTION

1.1 Introduction

A safe keyboard giving secure keyboard communications in a computer system. The assurance is even accessible when the computer being assault, such as the key logger. The attacker capture each human interface device input and monitor it. The attacker can frequently find important data from the client.

The project of secure keyboard is developed by encrypting the data input by the user input that bypassed through Arduino Leonardo and transmit the encrypted data onto computer. It displays the encryption data and sort a decryption process. .Arduino Leonardo is a microcontroller board for building digital devices and interactive object that can sense and control physical devices.

The highest levels of this security are available when an advanced cryptographic standard (AES) the symmetric-key algorithm is used for both encrypting and decrypting the data. This algorithm can help to protect the sensitive information especially in transaction information or financial transactions. Subsequently, it conceivable other spyware to catch the information.

1.2 Problem statement

There are some problem statement had been identified on the system. The Problem Statement (PS) is shown as below in Table 1.2:

Table 1.2 Summary of Problem Statement

PS	Problem Statement
PS 1	The data input is not encrypted before passing to the computer
PS 2	The threat to keyboard such as keylogger

1.3 Project Question

The Project Question (PQ) are discussed from the Problem Statement (PS) in Table 1.2. The Table 1.3 below shown the Summary of Project Question (PO).

Table 1. 3. Summary of Project Question

PS	PQ	Project Question
PS 1	PQ 1	How to developed secured keyboard?
PS 2	PQ 2	How can Arduino Leonardo will help to encrypt the data from keylogger?

1.4 Project Objective

The Project Objective (PO) are developed based on Problem Statement and Project Question. The Table 1.4 below shown the Summary of Project Objective.

Table 1. 4. Summary of Project Objective

PS	PQ	PO	Project Objective
PS 1	PQ 1	PO 1	To define secure keyboard
PS 2	PQ 2	PO 2	To design an encryption tool component for secure keyboard
		PO 3	To develop encryption model of secure keyboard

1.5 Project Scope

1. The developer who develop a secure keyboard encryption
2. The users who input data through keyboard communication will be encrypted.
3. The Arduino Leonardo device that used to encrypt the data input from user to the computer.

1.6 Project Contribution

The Table 1.6 below shown the Summary of Project Contribution

Table 1. 6. Summary of Project Contribution

PS	PQ	PO	PC	Project Contribution
PS 1	PQ 1	PO 1	PC 1	Proposed suitable programming language for Arduino Leonardo
PS 2	PQ 2	PO 2	PC 2	Proposed an algorithm for encrypting the data input
		PO 3	PC 3	Proposed data input in keyboard communication will be encrypted

1.7 Thesis Organization

Chapter 1: Introduction

This chapter will discuss the explanation the background of this project why we need to develop this system. In this chapter also will include problem statement about this project and the objective to achieve when doing this project. Furthermore, in this chapter will discuss the scope of this project and an explanation about the scopes. Chapter 1 are discuss briefly on the background this project.

Chapter 2: Literature Review

This chapter review 20 articles that related to the research done on this project. We need to discuss issues that related to project for example its function, process, architecture, algorithm and others. Compare the article about their methodology used to complete the research. The hardware, software, parameters and the attribute also need to do some comparison between the 20 articles that related to our title.

Chapter 3: Methodology

Chapter 3 discuss more in the method that we used to develop the project for an example the software that we needed to develop it. This also will determine what approaches we need to use to complete the project within the time. Milestones about the project need to be prepared in this chapter. Explain every stage on the milestone. This is all about in chapter 3.

Chapter 4: Analysis and Design

Chapter 4 discuss the design of the project and the requirement analysis. This will also include the problem analysis that we need to investigate and describe current system scenario/situation. For the requirement analysis, we need to specify the data requirement, functional and non-functional requirement. The detailed about design of user-interface, database and system architecture. Software and physical design also will be including in this chapter.

Chapter 5: Implementation

Chapter 5 describes the implementation status of the project and the software development environment setup, software configuration management that is include the configuration environment setup and version control procedure and the implementation status.

Chapter 6: Testing

Chapter 6 describes the activity involved in testing phase and what is testing strategy to be adapted in the project. The test plan and test designs are explaining more in this chapter. 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

Chapter 7 conclude all the project summarization, project contribution, and the project limitation. Project summarization will be described how the objective has been achieved by integrating the information that had reported to implementation and testing phase. State also the project contribution to the university/faculty/company/individual. Project limitation needs to be stated while doing this project until the progress was done.

1.8 Conclusion

In conclusion, this chapter introduce the problem statement, objective and contribution of this project. The problem state the issues to create the project and how to solve the problem. The research question and objective laid out the foundation concept of this project. The contribution present the outcomes of the project. The next chapter is chapter II which is literature review. The chapter review 20 articles that related to the research done on this project.

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

A secure keyboard combines a human interface device (HID), application programs stored in nonvolatile memory, and encryption technologies into a single package (Examiner.P and Cain.D,2010). 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 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 (Bernd.G,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 (Cardoso.D,2007).All confidential information is converted into secure forms, such as by encryption by an encryption key retrieved from a memory location of the hardware token (Christopher D,2005).

Arduino is the name of a group of microcontroller board. The boards are a mix of an ATMEL chip including RAM, streak memory, and information/yield channels. Accordingly, these board has the same general structure as basic computer, however their execution is obviously just a small amount of those. These board associates with standard exploratory programming utilizing a USB association and a virtual serial port. The Arduino measures reaction latencies subsequent to being signaled begin of a trial and conveys the inertness and reaction back to the PC over a USB association (Schubert, Ausilio.AD, Canto.R, 2013).

Symmetric encryption techniques utilize the same enter to both encryption Also unscrambling. Such symmetric routines incorporate the well-¬known des (Data encryption Standard) and AES (Advanced encryption Standard) calculations. On deviated encryption methods, for example, those RSA (Rivest Shamir Adelman) algorithm, a workstation that is will get encrypted information generates integral open Also private keys Furthermore transmits people in general magic of the sender. Following the. Sender need encrypted the information utilizing people in general key, just the holder of the private key camwood unscramble it. (F.Lior,2010).

2.2 Related Work/Previous Work

According to Us.B & Boyington (2014), M. the strategy might incorporate getting to an administration by means of a computer. The computers might be coupled to a programmable human data gadget. The programmable human information gadget might be arranged to specifically get client data from a human client and stores no less than one encryption key. The strategy might incorporate encoding, by the programmable human information gadget, client private data utilizing an encryption key connected with the administration and put away inside of the programmable human info gadget. The strategy might likewise incorporate transmitting the scrambled client classified info to the administration by means of the PC, wherein the PC is not designed to decide the decoded client secret data from the encoded client private information.

However, Deshpande, a. M., Deshpande, M. S., & Kayatanavar, D. N.(2009) said that advanced Encryption Standard (AES) is an approved cryptographic algorithm that can be used to secure electronic information. The AES can be modified in programming or worked with pure hardware. The AES algorithm is a symmetric block cipher that can encrypt and decrypts information. Encryption converts data to the form that called ciphertext. Decryption of the ciphertext converts the data back into its original form, which is called plaintext. The AES computation is fit for using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt information in pieces of 128 bits. The equipment execution of the Rijndael algorithm can give either superior or ease for particular applications. At backbone communication channels is not possible to lose processing speed, which drops the efficiency of the overall system while running cryptography algorithms in software.

Besides that, an article from Cardoso, D (2007) show the protected information system give technique information transmitted between a data gadget, for example, a console and a destination gadget, for example, a computer (PC). A first secure module is utilized for blocking information transmitted by the keyboard to the PC that works on the information to create protected output. A second secure module is utilized for getting the protected output from the principal secure module and giving back the protected output to its unique structure. The first type of the information might then before sent by the second secure module to the computer for use along these lines. The framework empowers a safe correspondence channel between the keyboard and the PC without requiring extra drivers or programming to arrange the computer to acknowledge such ensured information.

Then, an article from Honma, T., & Cited, R. (2001) shows the technique and keyboard for protecting 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 strategy 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 Schubert, T.W., D'Ausilio, A. & Canto, R. (2013), they propose to do latencies of button presses are a staple of intellectual science paradigms. They use the Arduino microprocessor platform as an alternative to keyboards and standard response boxes. They recommend utilizing open-source Arduino microcontroller boards a reasonable and adaptable option. These boards connect to standard test programming utilizing a USB association and.An virtual serial port, or by emulating a keyboard. The Arduino measures response latencies after being signaled and begin of a trial communicates the latency and response back to the PC over a USB connection. They similarly demonstrate to interface an Arduino to standard reaction time modifying (utilizing E-Prime) and report how correct those estimation may be contrasted with standard response boxes. It also sketch how utilizing the Arduino platform permits extending the experimental toolbox to include other measures beyond key presses. Subsequently, they depict how the Arduino can be utilized as a platform for measuring latencies of various kinds.

2.3 Critical Review of Current Problem and Justification

The Table 2.3 shows the critical review of current problem and justification in different method, advantages and disadvantages.

Table 2. 3 Critical Review of Current Problem and Justification

Method	**Description**	**Advantages**	**Disadvantages**
Comprising encryption module	Obtain a keyboard input from the keyboard, encrypting the keyboard input comprises an encryption key and passing the encrypted input to the computer	Data information input is secure	Require an appropriate key in order to decrypt the data.
The secure information that connected to server via a network	A strategy for protecting by a server 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.	Transaction important information across the network more secure.	Have software can interpreting the data to get the information.
Data processing terminal device on-line connected to the host computer, between which encrypted data is transferred	Processing the encrypted Journal data to modified data.	The data are encrypted	Need secret key to decrypt

Secure keyboard input terminal	It provide protected information where mechanical assembly being furnished with intends to associate the characters with the keys in a random and to present to the user after effects of such association in a helpful structure while information is being input.	The data are encrypted	Need secret key to decrypt
Secure keyboard using encrypted method	An encryption keyboard, including a panel and a control board, characterized in that it has a sealed flexible circuit board between the panel and the control board, the sealed flexible circuit board has a built in anti-spy detection circuit to achieve self-destructive feature electrically connected through the circuit	The data are encrypted	Need secret key to decrypt
Rolling key function	A method comprising storing a current copy of the key. The key is simultaneously updated at each secure module using a respective clock. It comprising resetting clock during power on to resynchronize said key. It	Have automatic updated encryption key	Not easily to decrypted by unauthorized person

	also comprising encrypting data according to 3DES.		
Having an encrypted and a digitizer for receiving an input and generating an output supplied to encrypt.	Coupling the encrypted to the digitizer in such a manner as to guarantee that a given cipher text is the encryption, generated by the encrypted of an output, generated by the digitizer.	Digitalized generated the encrypted 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 button presses by using Arduino microcontroller boards	Arduino microprocessor platform as an alternative to keyboards and standard response boxes. It shows how to connect an Arduino to standard reaction time software (using E-Prime), and report how precise the measurement is compared to standard response boxes.	Report how precise the measurement is compared to standard response box	Can change the measurement

Android Application to Recommend Home Security Threats	A home mechanization framework is intended for remotely controlling and checking the home environment and it additionally suggests the home security dangers. The system consists of an application created utilizing the Android stage and Arduino microcontroller. The Arduino microcontroller is the heart of the system that has the smaller scale web-server and performs the essential activities that should be done.	Threat can detected faster	Limit to certain threat
Arduino experiments in psychological and neurophysiological settings	It requires the exact control of various info and output signals. These signals are often generated or recorded via computer software and external dedicated hardware. It requires extra programming to control its behaviors. The Arduino afford to load the experimental script on the board's memory and let it run without interfacing with computers or external software, thus granting complete independence, portability, and precision.	Require extra programming to be function	Monitor without interface

2.4 Proposed Solution

The review on the previous research has given requirement to create the development of secure keyboard. The development of secure keyboard provides more secure communication in a computer system. The process development of secured keyboard is involved a keyboard, Arduino Leonardo and computer.

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 more recent Arduino Leonardo board uses the Atmel ATmega32u4 microprocessor that has built-in USB communication and in this way does not require an extra converter chip. 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 the code is written in a simplified 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 a computer or work standalone. A few components make the Arduino fascinating tool as a measurement platform. As a matter of first significance, it interfaces 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

The highest levels of security are available when an advanced cryptographic standard, such as the symmetric encryption is used because it has a same unique key pair for encrypted and decrypted. AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively. It uses 128 bit blocks, and AES supports larger key sizes than 3DES and faster in both hardware and software. AES is more secure. AES is the successor of DES as standards symmetric encryption algorithm. It is less susceptible to cryptanalysis than 3DES

DES is the previous data encryption standard. It key size is a really short for legitimate security. Previously, triple DES (3DES) is a basic name to those triple information encryption calculation. 3DES is very slow especially in software implementations because DES was designed for performance in hardware.

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 to define what is secured keyboard, how the design encryption tool component for secure keyboard and how to develop encryption model of secure keyboard. The problem statement stated which are the data are not encrypted and exposed to the key logger attack which a main threat to keyboard.

2.5 Conclusion

In conclusion, from this chapter, minimum 20 related article/journal about the secured keyboard have been review. They are several techniques and methods used to secure the communication between keyboard and computer. All the techniques have their own advantages and disadvantages. 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 detail about the method of this project. The activity for every stage described based on the project flow. The project tools for the secure keyboard is using Arduino Leonardo and encryption will explain the process how to test the simulation and to implement encryption in Arduino Leonardo and decryption in the computer.

3.2 Methodology

Methodology explains the methods and principles that are used for doing a particular kind of work. In this case, this chapter will define the step that will be taken during the completion of this project. This project will be carried out following “Rapid application Development” methodology.

Rapid application development (RAD) in the figure organized methodologies those information-driven information planning with prototyping methods and joint application improvement (JAD) methods to accelerate system development. RAD require the intelligent utilization of organized strategy and prototyping to characterize user requirement and design the final system.

Joint Application Development, or JAD, is a process for improvement in the quality of the final product by concentrating on the in advance part of the improvement lifecycle so as to reduce the likelihood of errors or required changes that are timely and expensive to correct later on. JAD also results in a shortening of the total life cycle time that it would otherwise take to complete a project.

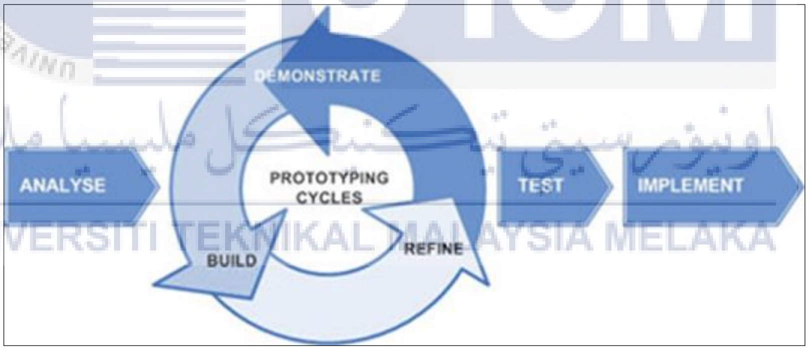


Figure 3. 1 Rapid Application Development

3.2.1 Phase 1: Analyze

This is the first phase to conduct this project in which the problem statement, scope, and project goal are defined as been explained in Chapter I. This phase, all required data and material for this project are collected and organized as presented in Chapter II. In order to make sure that this project works as planned, a Gantt chart and Milestone are constructed. These tools state the activities that are done and period took for each activity in order to accomplish this project. The objective of this phase, is to design encryption tool for the keyboard.

3.2.2 Phase 2: Prototyping cycle

3.2.2.1 Build

This step will start to develop the tools to secure the keyboard by using Arduino Leonardo in encryption module. The keyboard are connected to the Arduino Leonardo which implement the AES encryption and display the cipher text on the computer screen.

3.2.2.2 Refine

This phase shows the improvement of the tools if there are any problems occur.

3.2.2.3 Demonstrate

This phase demonstrate how the tools work. It shows the output of encryption in the computer when typing using the keyboard.

3.2.3 Phase 3: Test

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

3.2.4 Phase 4: Implement

In this step, 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.

3.3 Project Milestones

Project milestones explain the activities and duration date 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. The aim of Gantt chart is 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 3.3.1 shows the milestone of the project.

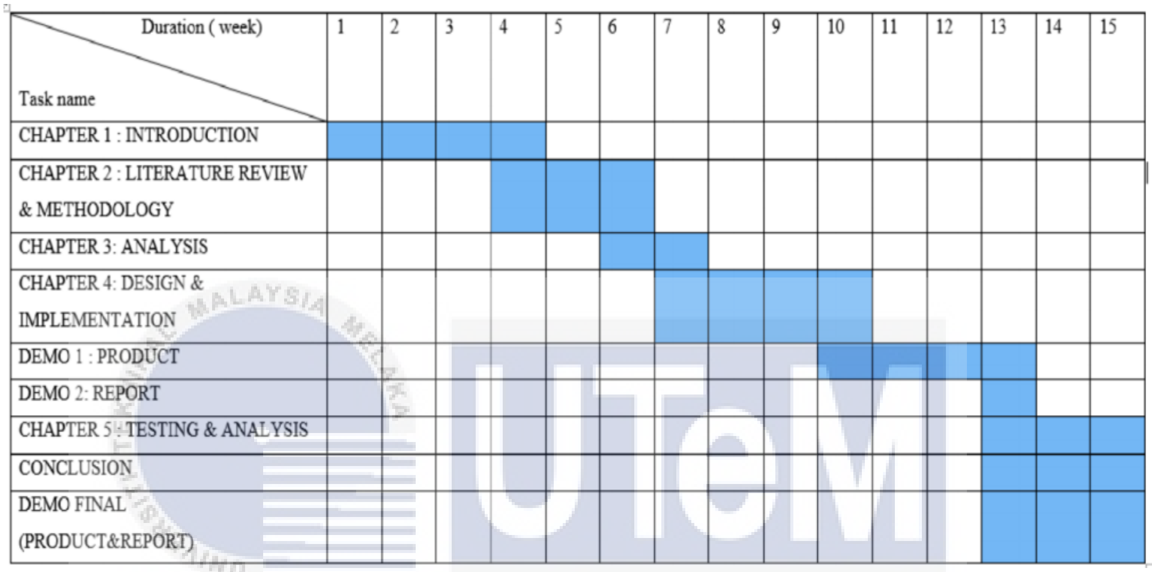
Table3.3.1 Milestones

Week	**Activity**	**Note / Action**
1 22-26 Feb	Proposal PSM Submission & Presentation	Deliverable – **Proposal** Action – Student
		Deliverable – **Proposal Presentation (PP)** Action – Student
	Proposal assessment and verification	Action – Supervisor, Evaluator
2 29 Feb -4 Mar	Proposal Correction/Improvement Chapter 1	Action – Student
	List of supervisor/title	Action – AJK PSM/PD
3 7-11 Mar	Chapter 1 (System Development Begins)	Deliverable – **Chapter 1** Action – Student, Supervisor
4 14-18 Mar	Chapter 1 & Chapter 2	Action – Student
5 21 - 25 Mar	Chapter 2	Action – Student
6 28 Mar -1 April	Chapter2 Chapter3	Deliverable – **Chapter 2** **Progress Presentation 1 (Pembentangan Kemajuan(PK 1))** Action – Student, Supervisor
	Student Status	Action – AJK PSM/PD,Supervisor Warning Letter 1

7 4-8 April	Project Demo & Chapter 3 Chapter 4	Action – Student
8	**MID SEMESTER BREAK**	
9 18-22 April	Project Demo & Chapter 4	Deliverable – **Chapter 3** Action – Student, Supervisor
10 25 - 29 April	Project Demo & Chapter 4	Deliverable – **Progress Presentation 2 (Pembentangan Kemajuan ,(PK) 2)** Action – Student, Supervisor
	Student Status	Action – AJK PSM/PD, Supervisor Warning Letter 2
11 2 - 6 May	Project Demo	Action – Student
	Determination of student status(Continue/Withdraw)	Action –PSM/PD Committee, Supervisor(submit student status to AJK)
12 9 – 13 May	Project Demo & PSM Report	Action – Student, Supervisor, Evaluator
13 16 - 20 May	Project Demo & PSM Report	Action – Student, Supervisor, Evaluator
	Presentation Schedule	AJK PSM/PD
14 23 - 27 May	Project Demo & PSM Report	Deliverable – **PSM Report** Action – Student, SupervisoR
15 30 May -3 June	**FINAL PRESENTATION (PA)**	Action – Student, Supervisor, Evaluator

The table below shows the Gantt chart of this project.

Table 3.3.2 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, the project methodology describe how the project is implemented. Project planning involves analyzing, build, refine and demonstrate, test and implement the project. 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 of the development system that implemented. In order to develop a new system the analysis process is important step in order to create a good and efficient system. By doing the analysis on the current project, the project get some information therefore the system can be developed successfully and meet user requirements.

The design for this system is the user input of the keyboard encrypt by through the Arduino Leonardo and passed to the computer. Then, the computer display and decrypt the user input. The system used the advanced cryptographic standard the symmetric-key algorithm, which the same key is used for both encrypting and decrypting the data which it is the highest level of the security

4.2 Problem Analysis

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.

The figure 4.2 shows the transmit data for current system. The system is about when the user have entered data using the keyboard is directly to the computer. Thus, there is no protective to the data along the transmission to the computer. The non-protective kf data means the data are not encrypted and can be trace by other people which they can steal the important information of the user.

Besides that, the keyboard that not encrypted are exposed to the threat such as key logger. Key logger 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.

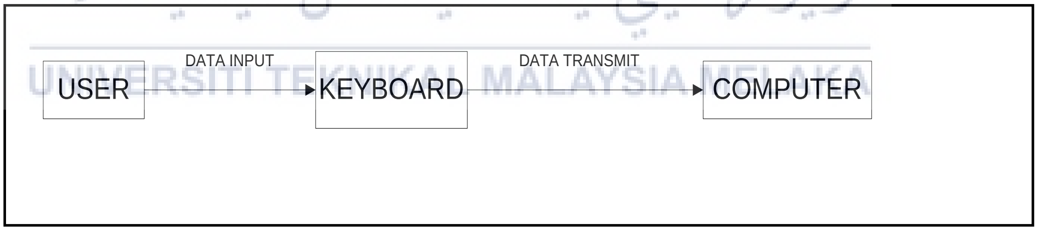


Figure 4. 1 Transmit Data for Current System

Hence, there is a system that could protect the user input. The system is encrypt the user input of the keyboard by using Arduino Leonardo then transmit the data to the computer. The encryption process of data can prevent the key logger attack.

4.3 Requirement analysis

4.3.1 Data Requirement

The figure shows the flow chart diagram for the system. The keyboard receive the data input from the user. Then, the data input transmitted into the Arduino Leonardo for the encryption process. The cipher text or encrypted data will transmit to the computer which then display the encrypted data.

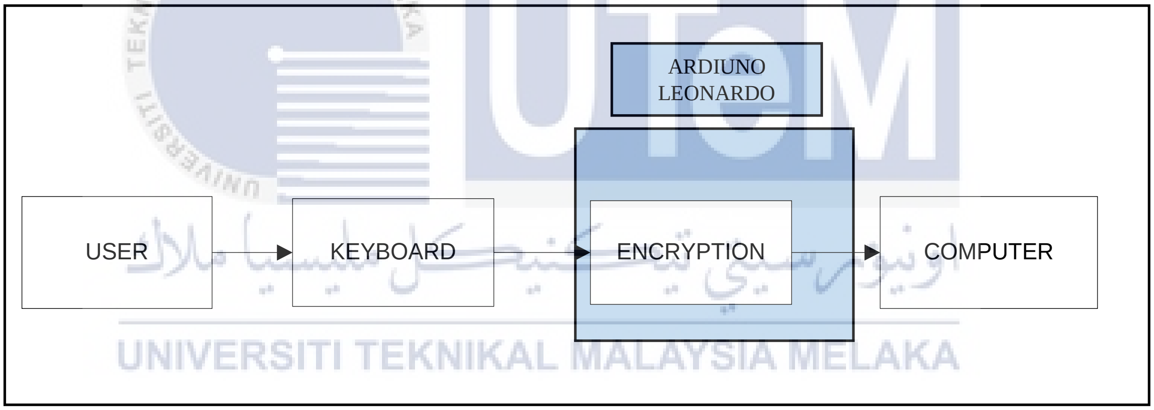


Figure 4.3. 1 Flow Chart Diagram

4.3.2 Functional Requirement

Functional requirement described an interaction between the system and its environment. It described how the system should behave and what was user expected from the system. This requirement is used to design the system modules or functions.

The system are defined a safe keyboard which giving a secure keyboard communications in a computer system. The secured keyboard implement the data input from the keyboard to be encrypted through the Arduino Leonardo and sent to the computer for decryption. The encrypted data also prevent key logger attack that capture the keystroke of the keyboard by user input. The encrypted data will provide data integrity.

The figure 4.3.2 below shows the data flow diagram. This system encrypt the data that user have entered using the keyboard.When the data have entered,the data will encrypt into 16 chars using the aes algorithm which used the sama public key for encrypt and decrypt.The program will be transmit to the computer for display the encrypted data and decryption of data.

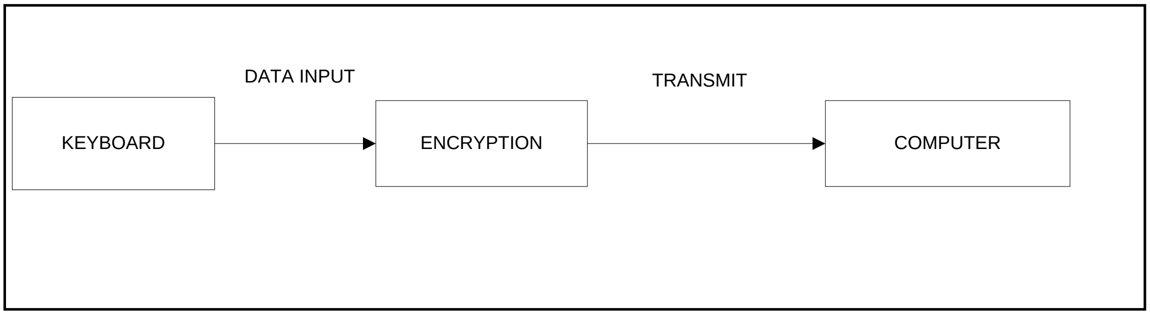


Figure 4.3.2 Data Flow Diagram

4.3.3 Non-functional Requirement

Non-Functional requirement is a requirement that specifies criteria to judge the operation of a system. Non-functional requirement are often called qualities of a system. The qualities and the performance of the system are should be done in effectively and run smoothly.

4.3.4 Others Requirement

Software

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

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

Hardware

i. Arduino Leonardo
The arduino Leonardo are tool for configure the encryption of the plain text and transmit to the computer for the decryption.

ii. Personal Computer ASUS/Computer

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

iii. Printer Canon

Printer is used to print project reports

4.4 High-Level Design

High Level Design means a high level design that discusses an overall view of how something should work and the top level components that will comprise the proposed solution. It also studies the architecture that would be used for developing a software. This part consists of system architecture, user interface design, conceptual and logical database design.

4.4.1 System Architecture

System architecture refer to the conceptual design and logical design of a system and its components structure.

The figure shows the keyboard encryption process. The input data will transmit to the Arduino Leonardo for encryption process. The Arduino Leonardo will capture the plain text and encrypt to cipher text. The encryption process used advanced cryptographic standard (AES), symmetric-key algorithm, which the same key is used for both encrypting and decrypting the text. In this encryption method, the ten keys will be set as encrypted key. After the encryption process, the cipher text will transmit to the computer for display the encryption text and decrypt the encrypted text.

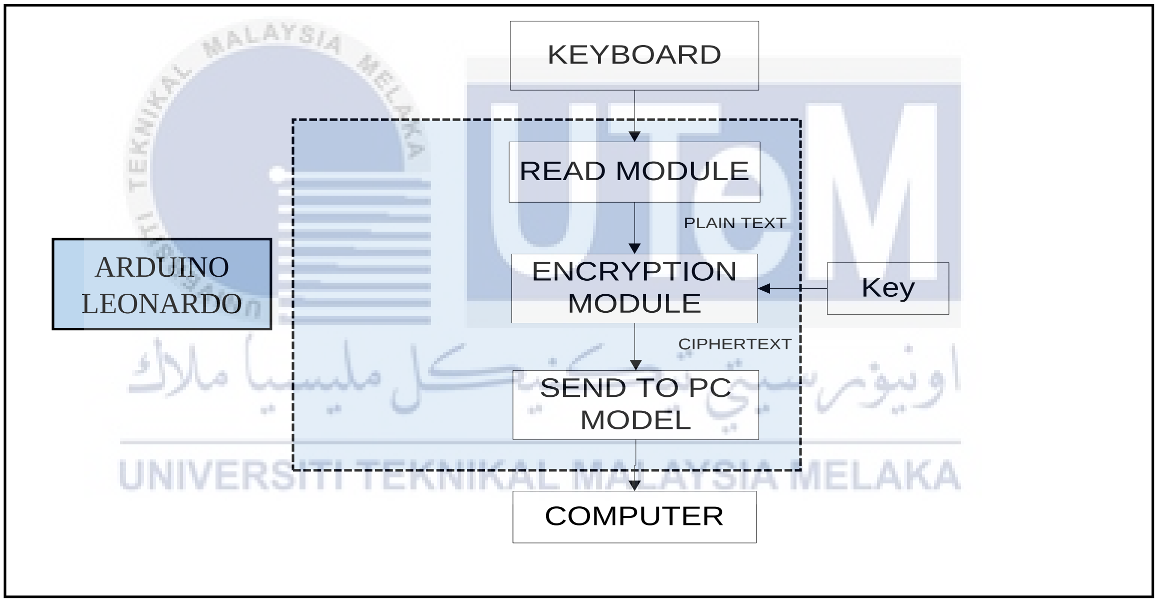


Figure 4.4. 1 Keyboard Encryption Process

Encryption of AES algorithm

The Advanced Encryption Standard (AES) is a symmetric-key encryption standard AES is based on a design principle known as a substitution permutation network. The standard comprises AES-128, block ciphers. Each of these ciphers has a 128-bit block size, with key sizes of 128.In this section, it provide a brief overview of the AES algorithm and the working of its major constituent computations.

The AES algorithm consists of following phases:

1. **Key Expansion**

   Round keys are derived from the cipher key

2. **Initial Round.AddRoundKey**

   Each byte of the state is combined with the round key using a bit-wise operation.

3. **Middle Rounds.**

   Repeatedly perform the following transformations:

4. **SubBytes**

   A non-linear substitution step where each byte is replaced with another according to a lookup table.

5. **ShiftRows**

   A transposition step where each row of the state is shifted cyclically a certain number of steps.

6. **MixColumns**

   A mixing operation which operates on the columns of the state, combining the four bytes in each column.

7. **AddRoundKey**

   Each byte of the state is combined with the round key using a bit-wise operation.

The figure below shows the AES algorithm encrypt the data input of user.

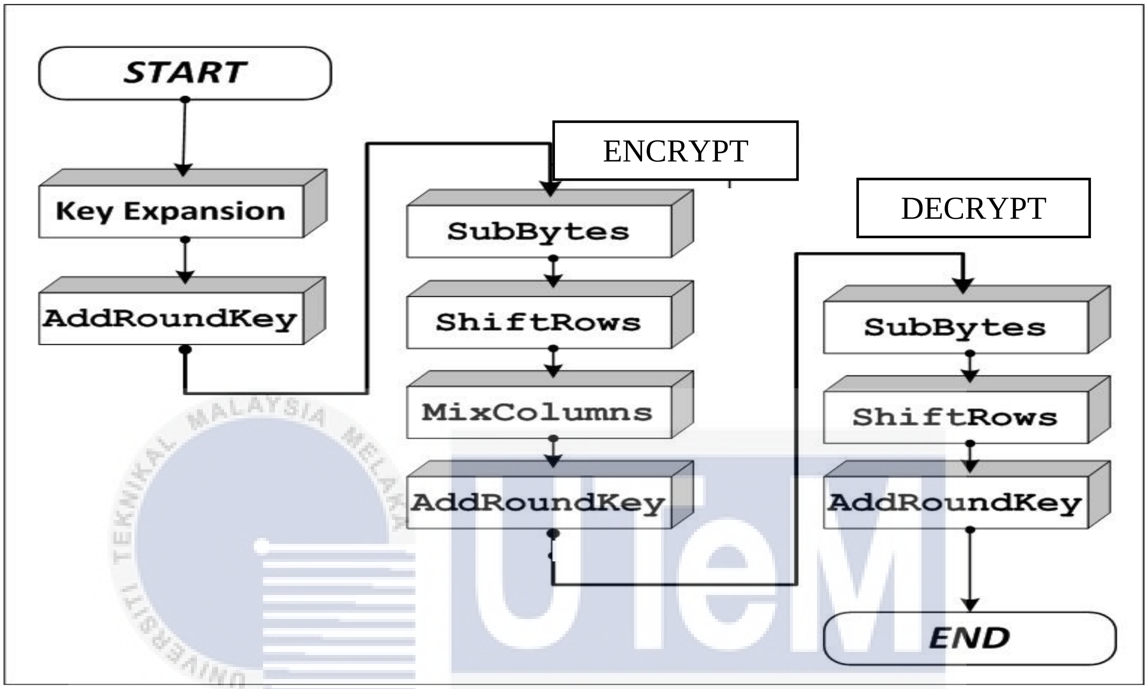


Figure 4.4.2: Show the step of AES algorithm

4.5 Detailed Design

This system function for the system development is how the encryption process will be done and output the encrypted data should be correct.

4.5.1 Software Design

The Figure 4.5.1 shows the four class diagram of the system. First, user class consists of the name of the user input. Secondly, the input class which the user enter the plaintext .Then, the process class which is encryption. The encryption operation using the AES algorithm to encrypt the input plain text. The output will be display in the notepad.

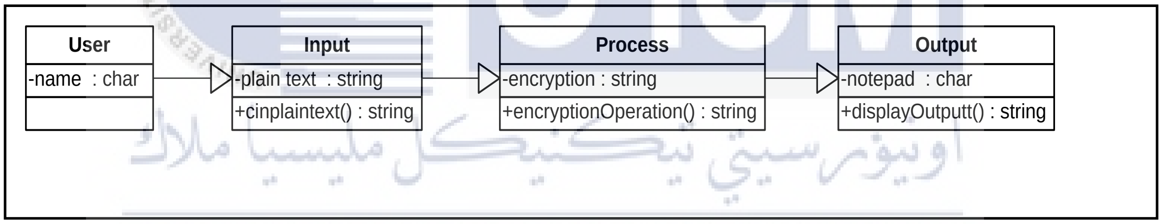


Figure 4.5. 1 Class Diagram

4.6 Conclusion

This chapter mainly discuss about the analysis and design of the system. This chapter discuss the process of the current system, the improvement of the new system development, and the process of the system work using the data model, data flow, navigation design and the class diagram. For the next chapter, the implementation process for the development system activity is involved and it give the expected output after completed the implementation process.

CHAPTER V

IMPLEMENTATION

5.1 Introduction

This chapter discuss about the implementation status of the project and the software development environment setup, software configuration management that is include the configuration environment setup and version control procedure and the implementation status. The activity involved in the implementation status is encryption. After completing this phase, the data should be encrypted and can only be decrypted 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 on the platform that required hardware and software components that used to implement in this project. The tools needed in this environment setup are keyboard, computer and the

Arduino Leornardo hardware that help to run the project. A program used Arduino 1.6.8 (IDE) to create the programed in the Arduino Leonardo. The Arduino 1.6.8 (IDE) need to configure the board used which is Arduino Leonardo board. Then, configure the port used for the Arduino Leonardo hardware used. The programming used in this project is C programming language. This configuration is very important to run the project. Besides that, need a computer to send the encrypted data for the decryption process. Refer Appendix B for the coding implementation of encryption.

5.3. Software Configuration Management

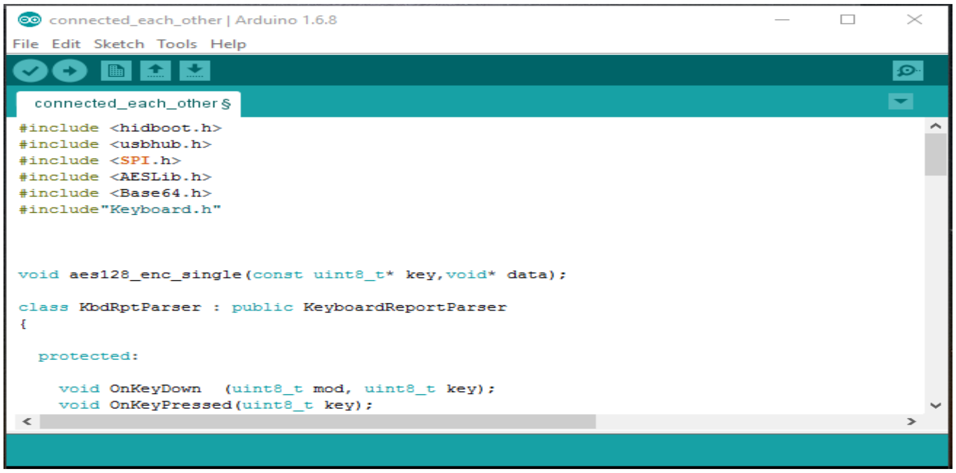
Software configuration management explain about the design and setup the configuration management of this project. This section also explained the software and hardware tool used to support configuration control.

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. As an interaction medium, Arduino Leonardo is will be installed properly via a computer through the USB cable. The Arduino Leonardo signal is send and received when Arduino Leonardo is connected to keyboard and computer. This project run when the user input the data using the keyboard and the data send to Arduino Leonardo for the AES encryption and transmit the data to the computer and display the encrypted data in the serial monitor of the Arduino Leonardo platform.

The configuration environment setup also describe the difficulties involved in implementation of secure keyboard. The connection between the keyboard and the Arduino Leonardo need to be programmed thus the Arduino Leonardo can read the data pass from the keyboard. The keyboard libraries and USB libraries have to include to make the Arduino Leonardo read the data pass to it. Besides that, the difficult thing is the AES encryption program apply. The developer need to change the data from the integer to char array so that the program can read the encryption data in 16 char. Furthermore, the developer also need to include the AES libraries to encrypt the data.

The secure keyboard have good strength as noted in the previous chapter. This system will encrypt the data that user have entered using the keyboard.When the data have entered, the data will encrypt into 16 chars using the aes algorithm which used the public key for encrypt.The keys and encrypted data in 16 chars shows the attacker had difficult to expect what the data are being transfer. This gives the data are more secure.Refer to appendix A to configure environment setup. The figure below shows the sketch of Arduino Leonardo


connected_each_other | Arduino 1.6.8
File Edit Sketch Tools Help
connected_each_other §

```
#include <hidboot.h>
#include <usbhub.h>
#include <SPI.h>
#include <AESLib.h>
#include <Base64.h>
#include"Keyboard.h"



void aes128_enc_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);
```

Figure 5.3. 1 Shows the sketch of Arduino Leonardo

5.3.2 Version control procedure

The evaluation process for the system that are being develop is involved in the version control procedure. The secure keyboard 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 Table5.4. 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 4 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 week	31 May 2016
Encryption module	The user enter the message and run the encryption process of AES algorithm.	4 week	18 July 2016
Send to computer	The encrypted message will transmit into the computer for display encrypted data and decrypted the data.	1 day	1 August 2016

5.5 Conclusion

In conclusion, this chapter discuss about the software development environment setup and software configuration management. The implementation status of the system is also being stated in this chapter. This is to make sure the system is function properly. The next chapter will discussed about testing phase and testing strategy that is need to be adopted in the project.

CHAPTER VI

TESTING

6.1 Introduction

This chapter will discuss about the testing status of the project. This chapter will discuss about the plan, design, result and analysis of testing project. The testing showed the progress of developed of encrypted user input using the Arduino Leonardo.

6.2 Test Plan

The test plan is purposely to identify the testing that implemented and executed before launch the system. In the test plan it consists of three phase of planning which are test organization, test environment and test schedule. 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

The organization test is involving the group of people that has different experience in information technology .The variety of people involved in testing phase is an advantages for evaluation of the secure keyboard development. People chosen for testing phase are system developers and students. System developer is a person who is fully in charge to test and evaluating the secure keyboard project. Students are those who study in different course of information technology in Universiti Teknikal Malaysia Melaka (UTEM).

6.2.2 Test Environment

Test environment is consisting of the location and environment for the testing process take place. There are several type of environments with regard of the secure keyboard system testing. The environment of testing process consists of three modules. These module are:

- Read module
- Encryption module
- Send module

The component used for test environment are listed in table 6.2.2

Table 6.1.2 Component of hardware used

Hardware	**Description**
Keyboard	Provided by UTEM
Arduino Leonardo	Provided by UTEM
Cable USB	Provided by UTEM
Computer	ASUS A450L

6.2.3 Test Schedule

The test schedule is a guide to be followed by the system developer. The purpose is to detect if any problem occur during the testing. The table 6.2.3 show the test schedule of this project.

Table 6.2.2 Show the test schedule

Module name	**Duration**	**Test start date**	**Test data completed**
Read module	2 days	1 July 2016	2 July 2016
Encryption module	5 days	19 July 2016	23 July 2016
Send module	1 days	2 August 2016	2 August 2016

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. White box testing is uses specific knowledge of programming code to examine outputs. The test is accurate only if the developer knows what the program is supposed to do. Black box testing is testing without knowledge of the internal working software being tested. The developer only know the legal input and what the expected output should be but not how the program actually arrives at those output.

6.3.1 Classes of Tests

In this section, several user are selected to do the testing based on the modules. Table 6.3.1 below shows the module for test the project functionality.

Table 6.3.1 Show 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 AES algorithm The data will display encrypted text in 16 char.
Send to computer	The encrypted data will transmit into the computer for display the encryption data.

6.4 Test Design

Test design is refer 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 6.4.1 show the modules, test ID, test case and description about the module will be expected output.

Table 6.4.1: Show the module test, test id test case and description

Modules	Test ID	Test Case	Description
Read module	AD_01	Functionality	Arduino Leonardo able to read data from the keyboard
Encryption module	AD_02	Functionality	The data input able to encrypt
Send to computer	AD_03	Functionality	Able the data encrypted display in serial monitor of computer

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. Table 6.4.2 shows the description of all test modules.

Table 6.4.2.1: Read Modules

Test ID	Test Case	Tasks	Actual output
AD_01	Functional	Arduino Leonardo able to read data from the keyboard	The Arduino Leonardo successfully read data from the keyboard

Table 6.4.2.2: Encryption Modules

Test ID	Test Case	Tasks	Actual output
AD_02	Functional	The data input able to encrypt	The user enter the data and run the encryption process of AES algorithm. The data will display encrypted text in 16 char.

Table 6.4.2.3: Send Modules

Test ID	Test Case	Tasks	Actual output
AD_03	Functional	Able the data encrypted display in serial monitor of computer	The encrypted data display in serial monitor of computer is succesfull.

6.5 Test Result and Analysis

Test result and analysis consists of expected output and description of user feedback.

Module: Read Module

Test Case: Functionality

Test Start Date: 1 July 2016

Test End Date: 2 July 2016

Duration Cycle: 2 days

Test ID	Tester Identification	Result(Pass/Failed))
AD_01	OK	Pass

Module: Encryption Module

Test Case: Functionality

Test Start Date: 19 July 2016

Test End Date: 23 July 2016

Duration Cycle: 5 days

Test ID	Tester Identification	Result(Pass/Failed))
AD_02	OK	Pass

Module: **Send Module**

Test Case: Functionality

Test Start Date: 2 August 2016

Test End Date: 2 August 2016

Duration Cycle: 1 days

Test ID	Tester Identification	Result(Pass/Failed))
AD_03	OK	Pass

6.6 Conclusion

In conclusion, this chapter describe test plan, test environment, test schedule, test strategy, testing design and result and analysis. These are important contents in the testing phase that should be covered by a tester. Testing process is a process to identify and verify the weakness and strength in the system. It very important because it can help system developer to verify whether the system is success or not. The result of testing process shows the complement of secure keyboard project that can be used by end user. The output for testing chapter will be used an input in the next chapter, Project Conclusion.

CHAPTER VII

PROJECT CONCLUSION

7.1 Introduction

This chapter will conclude all the project summarization, project contribution, and the project limitation. Project summarization will be described how the objective has been achieved by integrating the information that have reported in the implementation and testing phase. The stated also are the project contribution to the university and faculty.

7.2 Project Summarization

The succesfully of a project depends on the objective of the project.This project achieve it objective to define the secure keyboard. The project define a secure communication in a computer system. The data input by the user were send to the computer had been encrypted. Second objective is to design an encryption tool component for secure keyboard. This project used Arduino Leonardo medium to encrypt the data from the keyboard and transmit it to display to the computer AES algorithm is used to encrypt the data input from the keyboard. Third objective is to develop encryption model of the secure keyboard.This project encrypt the data that user have entered using the keyboard.When the data have entered,the message will encrypt into 16 chars using the AES algorithm which used the public key for encrypt and decrypt The program transmit it to the computer in order to for display the encrypted data and decrypted it.

The development of this project have their own weakness. The secure keyboard have the static password to encrypt and decrypt the data. It used a 10 keys system to encrypt in AES algorithm. The weakness of the keys is it can give other people chance to guess the keys. Besides that, encrypted data displayed the same encrypted if someone enter a same data. This weakness make it possible for other people to guess the input data.

The strength of this project is it can encrypt the data user input by the keyboard and display the 16 chars of encrypted data. The long encrypted chars make it difficult for other people to guess the data. The encrypted data also prevent key logger attack which can capture the keystroke of the keyboard by user input. The encrypted data gave the data more integrity or strength to the data.

7.3 Project Contribution

This system may become a great platform for the user which can protect their keyboard from captured by other people. The system used C programming language for encryption data in Arduino Leonardo. It also used AES algorithm which the data will be encrypt into 16 char of data input.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

During the project development process the developer had limitation of sources, configuration of AES encryption and timing to complete the task.

7.5 Future Works

This system may become a great platform if encrypted system was implemented in the keyboard without connected to the Arduino Leonardo. Besides that, the password of the encrypted keyboard can be save by owner itself. It gives the authentication of user to decrypt it data. The encrypted output should be different because if same output it easily the other people guess the value of data.

7.6 Conclusion

The system of secured keyboard using Arduino Leonardo, encryption module is achieve the goal of objective of this project. The data of user input had been encrypted by connected the keyboard to Arduino Leonardo and display the encrypted data at the monitor of Arduino Leonardo. The previous chapter had test the project. Thus, the project is successfully complete the project.

CONCLUSION

In the introduction, it defined the background of the project which is the secure keyboard using Arduino Leonardo in encryption module, problem statement,objectives and scope to let user know the system overview. In chapter literacture review, at least 20 articles have been reviewing that related to this project. The related article can be compared such as methodology, function, process, hardware and software to this project. Furthermore, the method for this project follow as Rapid Application Development (RAD) and this project need to finished in 15 week. Besides that, this project explained the requirement needed and detailed about design of architecture of this project.

In chapter implementation, it describe implementation status of the project and the software development environment setup, software configuration management that is include the configuration environment setup and version control procedure and the implementation status. The activity involved in the implementation status is encryption. In testing phase, it describe about testing plan phase. Every system is testing to ensure the system is function.

Finally, the project is successfully done and thank to Allah with His Blessing and supervisor because the system and report successfully done. This system will bring advantages to the user who want to protect their data secure.

REFERENCES

1. S.Pinheiro, E., 2010. Secured keyboard. *Paten US7835521*, pp. 1-7

2. Bernd Grossmann, R. W. (19 May 2010). Keyboard and method for secure data transfer. *EP 2187331 A1*, 1-7.

3. Cardoso, D., (21 Jun 2007). Encrypted keyboard. *US 20070143593 A1*, pp. 1-5.

4. Christopher Gentle, J. O. (24 march 2005). Method and apparatus for an encrypting. *US 20050066186 A1*, 1-9.

5. Lior Frenkel, A. Z. (4 November 2010). Encryption and decryption enabled interfaces . *US 9268957 B2*, 1-12.

6. Masaki Kyojima, R. (14 August 2001). Decryption method and device, and access right authentication method and appratus. *US 6275936 B1*, 1-22.

7. Naguib, N. N. (22 May 2008). Apparatus, and associated method, for providing secure data entry of confidential information. *US 20080120511 A1*, 1-8.

8. Honma, T., & Cited, R. (2008). Method and Apparatus for an encryption keyboard US 7366916 B2 *pp* 1–7.

9. Boyington, M. (2 September 2014). Cryptography secure input device, *US 8826028 B1*, 1–12.

10. 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), 1–6.

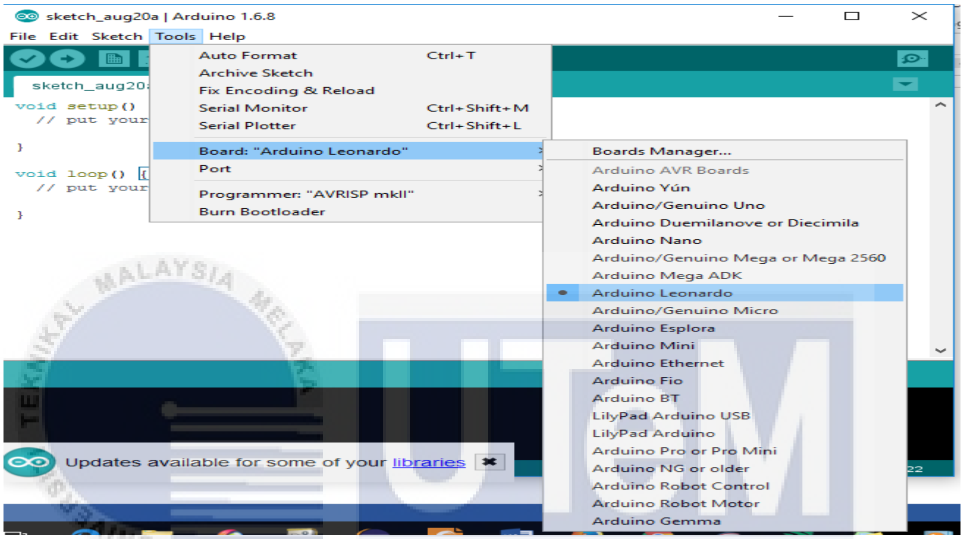
11. Schubert, T. W., D’Ausilio, A., & Canto, R. (2013). Using Arduino microcontroller boards to measure response latencies. *Behavior Research Methods*, *45*(4), 1332–46. http://doi.org/10.3758/s13428-013-0336-z

12. Silvio. (12 Mar 1996) Natural input encryption and method of use US 5499296 A, pp 1–8.
13. Angelo, M.F., 2016. Method and apparatus for allowing access to secured computer resources by utilizing a password and an external encryption algorithm US 5949882 A , pp.1–16.
14. Cheung, F. & Cheung, F., (2016). Method and system for data encryption and decryption. , pp.1–7.
15. Jadhav, P., Bankhele, T., Nikalje, P., & Chintawar, P. (2016). Android Application to Recommend Home Security Threats, *2*(2), 2–5.
16. Agarwal, M., Mehra, M., Pawar, R., & Shah, D. (2011). Secure authentication using dynamic virtual keyboard layout. *Proceedings of the International Conference & Workshop on Emerging Trends in Technology - ICWET '11*, (Icwet), 288. http://doi.org/10.1145/1980022.1980087
17. Clark, J. I., Eckert, A. B., & David, M. (3 Feb 1987). System for the printing and reading of encrypted messages *US 4641346 A* ABSTRACT, 1–16.
18. Nitin V.Sarangdhar, Jasmeet Chhabra(10 Feb 2015). Protecting keystrokes received from a keyboard in a platform containing embedded controllers, *US 8954747 B2* 1–8.
19. Chi-Pei Wang, Chen Chang, Kai-Hsiang Chou (31 July 2014). Device for preventing logging of clients input data in a computer system, 2–4.
20. Wang, C. P. (4 June 2009). Method For Anit Keylogger, *US 20090144558 A1*, 1–13.
21. Gardner, G. A. (13 Oct 1998). Data encryption for product information and access *US 5822428 A* ABSTRACT, 1–5.
22. Oh Chung Geon, Choi Kwang Wol, Sung Kwi Chul, Kim Dae Hyeong, Kim Seong Il (11 Aug 2015). Computer security apparatus and method using security input device driver, *US 20050177649 A1*,1–10.
23. Dereck D. Clark (29 Sept 1998). Methods and apparatus for securely encrypting data in conjunction with a personal computer *US 5815577 A*, (1), 1–23

APPENDIX A

ENVIRONMENT SETUP OF ARDUINO LEONARDO

1. Install the Arduino Leonardo 1.6.8. (IDE) in the computer.
2. Configure the board in Arduino 1.6.8 (IDE) which is Arduino Leonardo



```
void setup()
  // put your
}

void loop() {
  // put your
}
```

Figure 1: Select the Arduino Leonardo Board

3. Check the port of Arduino Leonardo used in Device

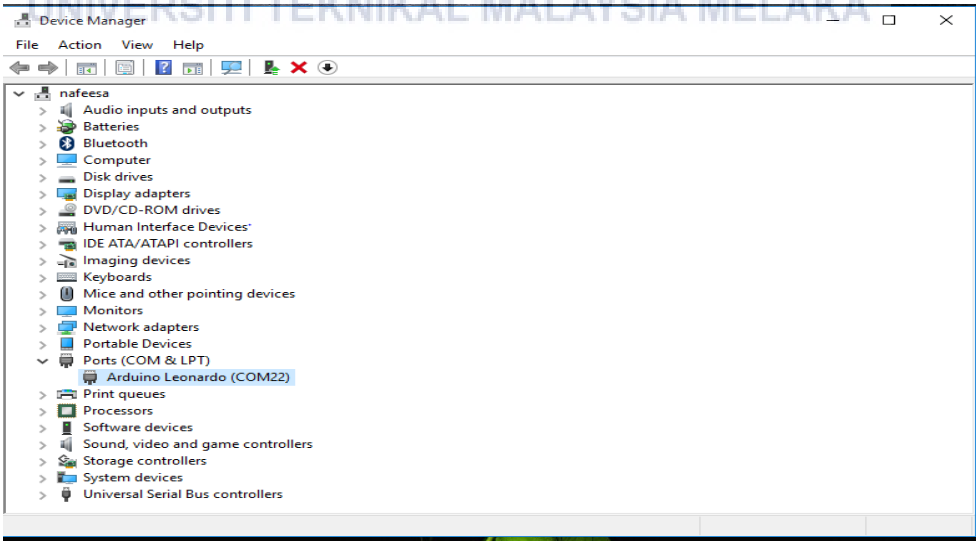
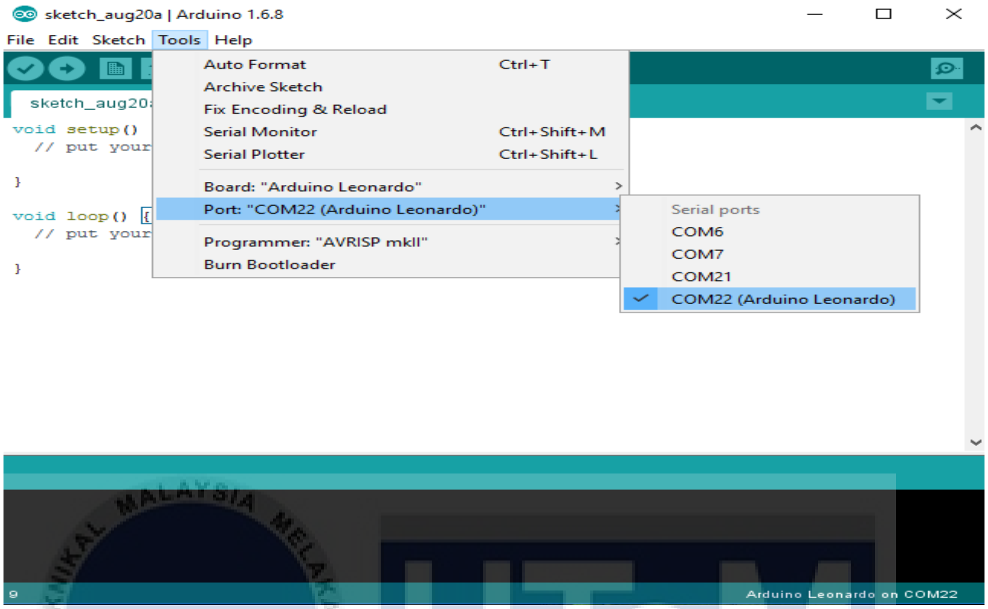


Figure 2: show the port of Arduino Leonardo used

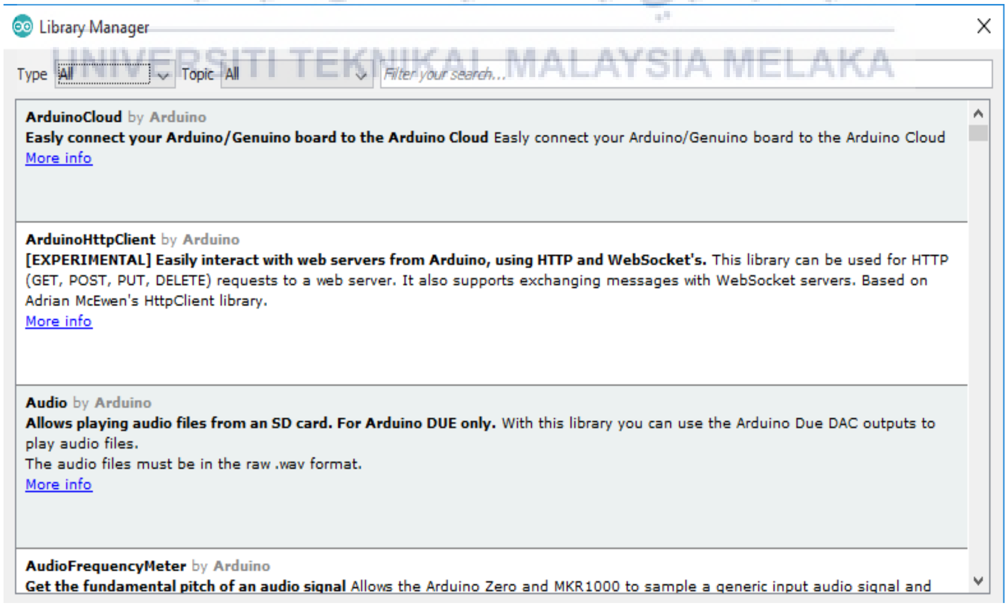
4. Select the port COM22 for Arduino Leonardo in Arduino IDE


sketch_aug20a | Arduino 1.6.8
File Edit Sketch Tools Help
sketch_aug20
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
Board: "Arduino Leonardo"
Port: "COM22 (Arduino Leonardo)"
Programmer: "AVRISP mkII"
Burn Bootloader
Serial ports
COM6
COM7
COM21
COM22 (Arduino Leonardo)
9
Arduino Leonardo on COM22

```
void setup()
  // put your

}

void loop() {
  // put your

}
```

Figure 3: Select the port COM22 of Arduino Leonardo in Arduino IDE

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



ArduinoCloud by Arduino
Easly connect your Arduino/Genuino board to the Arduino Cloud Easly connect your Arduino/Genuino board to the Arduino Cloud
More info

ArduinoHttpClient by Arduino
[EXPERIMENTAL] Easily interact with web servers from Arduino, using HTTP and WebSocket's. This library can be used for HTTP (GET, POST, PUT, DELETE) requests to a web server. It also supports exchanging messages with WebSocket servers. Based on Adrian McEwen's HttpClient library.
More info

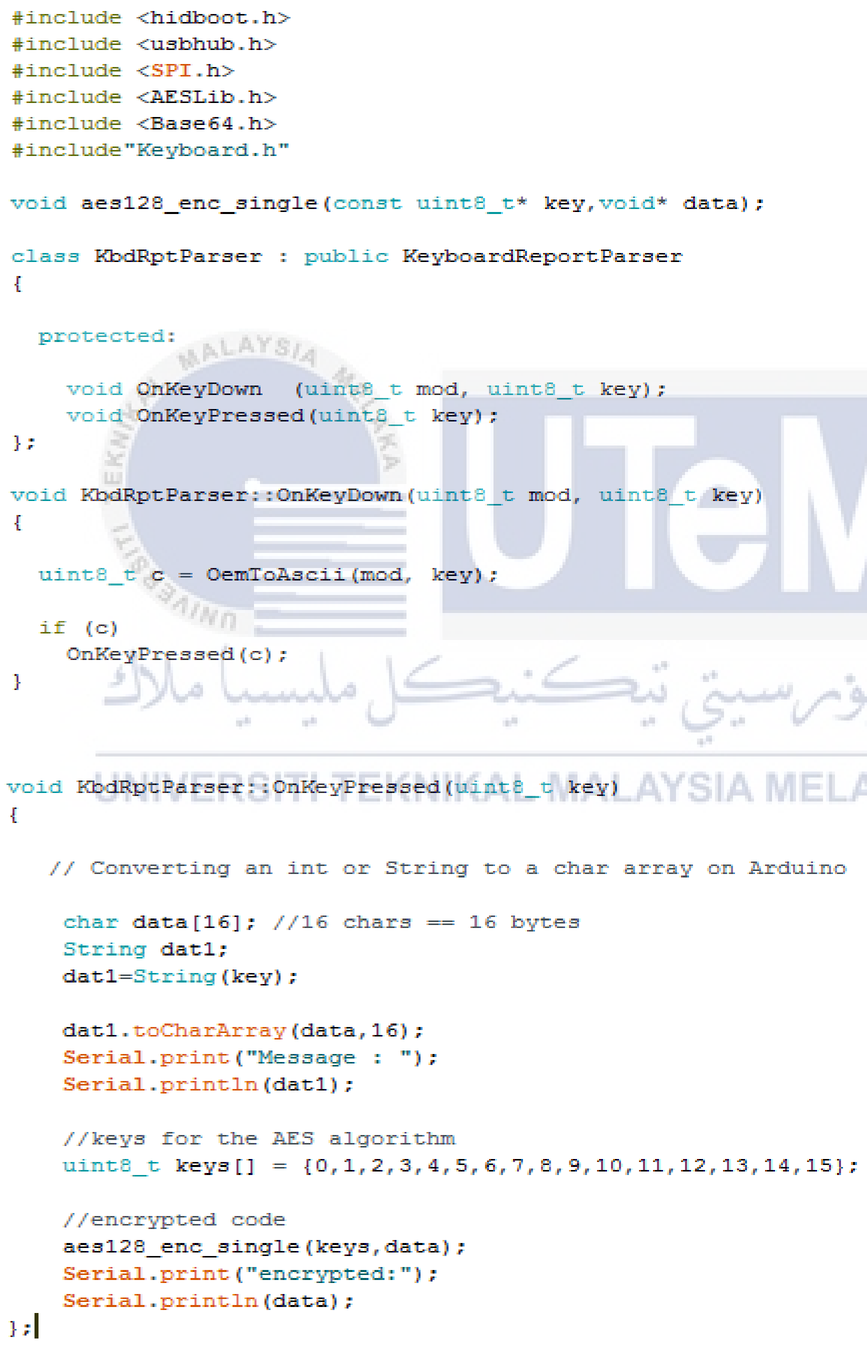
Audio by Arduino
Allows playing audio files from an SD card. For Arduino DUE only. With this library you can use the Arduino Due DAC outputs to play audio files.
The audio files must be in the raw .wav format.
More info

AudioFrequencyMeter by Arduino
Get the fundamental pitch of an audio signal Allows the Arduino Zero and MKR1000 to sample a generic input audio signal and

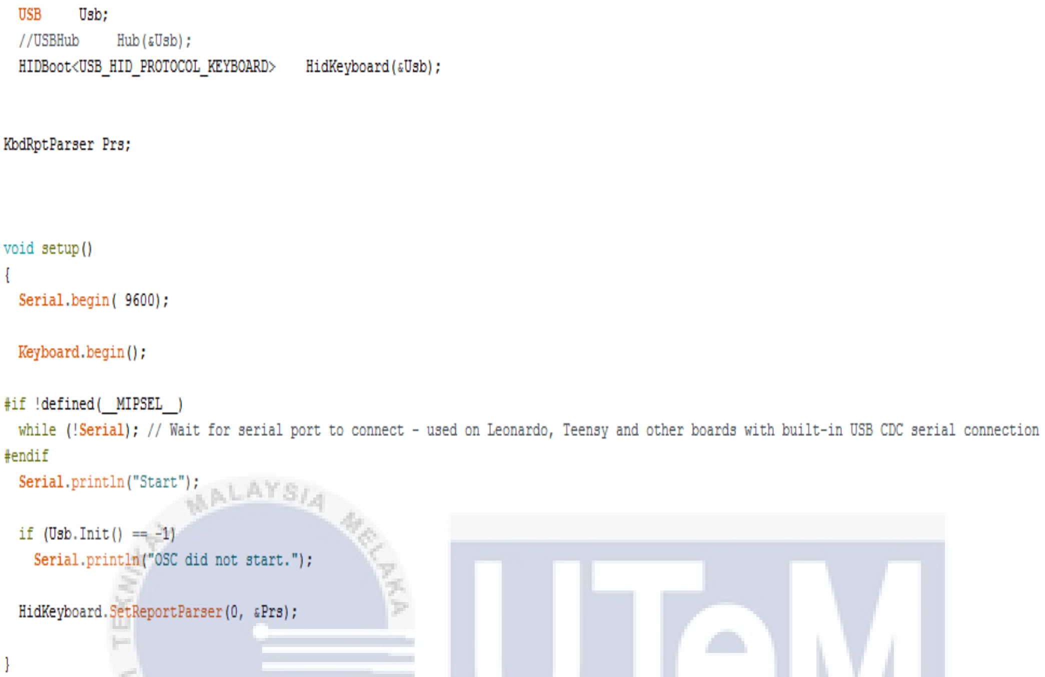
Figure 4 Show library Manager of the Arduino Leonardo

APPENDIX B

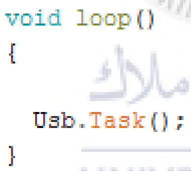
The coding for the read from the keyboard and encryption in arduino Leonardo



```
#include <hidboot.h>
#include <usbhub.h>
#include <SPI.h>
#include <AESLib.h>
#include <Base64.h>
#include"Keyboard.h"

void aes128_enc_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)
{

   // Converting an int or String to a char array on Arduino

    char data[16]; //16 chars == 16 bytes
    String dat1;
    dat1=String(key);

    dat1.toCharArray(data,16);
    Serial.print("Message : ");
    Serial.println(dat1);

    //keys for the AES algorithm
    uint8_t keys[] = {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15};

    //encrypted code
    aes128_enc_single(keys,data);
    Serial.print("encrypted:");
    Serial.println(data);
};
```

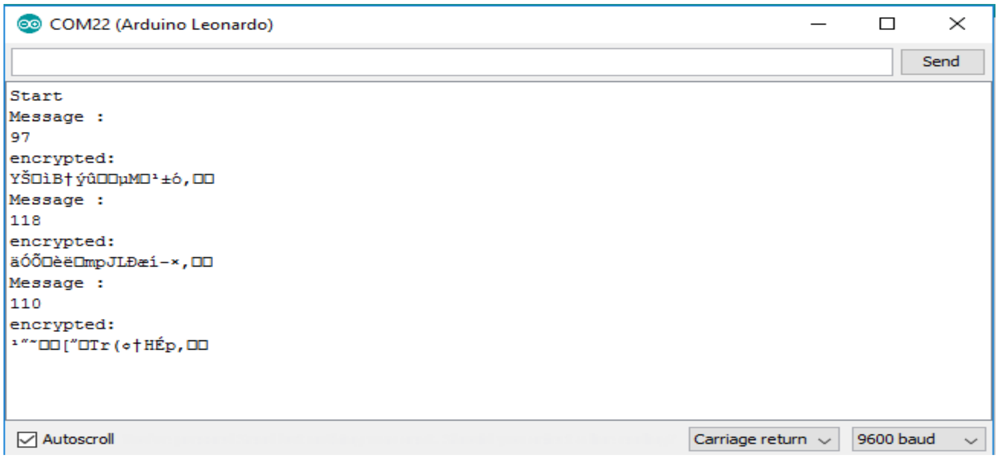


```
  USB     Usb;
  //USBHub     Hub(&Usb);
  HIDBoot<USB_HID_PROTOCOL_KEYBOARD>    HidKeyboard(&Usb);


KbdRptParser Prs;



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

  Keyboard.begin();

#if !defined(__MIPSEL__)
  while (!Serial); // Wait for serial port to connect - used on Leonardo, Teensy and other boards with built-in USB CDC serial connection
#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



```
Start
Message :
97
encrypted:
YŠ□iB†ýû□□µM□¹±ó,□□
Message :
118
encrypted:
äÓÕ□èë□mpJLÐæí–×,□□
Message :
110
encrypted:
¹″˜□□[″□Tr(∘†HÉp,□□
```