TEXT ENCRYPTION AND DECRYPTION SOFTWARE USING MICROCONTROLLER

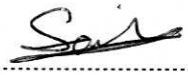
MOHD SAIFUL AZIM BIN KHAIRUL ANUAR

This report is submitted in partial fulfillment of the requirements for the award of Bachelor of Electronic Engineering (Telecommunication Electronics) With Honours

Faculty of Electronic and Computer Engineering
Universiti Teknikal Malaysia Melaka

May 2008

"I hereby declare that this report is the result of my own work except for quotes as cited in the references."

Signature : 

Author :Mohd Saiful Azim Bin Khairul Anuar

Date : 12/5/08

"I hereby declare that I have read this report and in my opinion this report is sufficient in terms of the scope and quality for the award of Bachelor of Electronic Engineering (Telecommunication Electronics) With Honours."

Signature : .....

Supervisor's Name :En. Imran Bin Mohd Ibrahim

Date : 12/5/08

DEDICATION

I would like to dedicate this thesis to my late- mother..... I loved you and I missed you so much..... I would also like to dedicate this thesis to my beloved father, my step- mother and to all my family members.

ACKNOWLEDGEMENT

First and foremost, thank to Allah for giving me the strength to complete this project and this thesis report. I would also like to show my gratitude to En. Imran, my project supervisor for all the guidance and advice he has given me in completing this project and this thesis report. A big thank you also goes out to my family and friends who have supported me and also to those who have contributed directly or indirectly in my completion of this project and thesis report. Thank you all.

ABSTRACT

This project is about building a text encryption and decryption software using the microcontroller. Encryption is a process of masking a message so that it is unreadable. Encryption is important to avoid other people to read certain information. The only way to read the information is to know the method on how the message is being masked, in this case knowing the algorithm used to encrypt the message. In this age of information technology and with the fast advancement of computer technology, the need to secure information especially digital information has become immense. Nowadays, most encryption and decryption processes are done by the computer. The main objective of this project is to build a text encryption and decryption software that will run on a microcontroller. Then, the microcontroller will be used as an external means to encrypt text. As mentioned earlier, most encryption processes nowadays are done by the computer, so by having a hardware that does the encryption externally, we can take the load of encrypting the text from the computer and also remove the hassle of installing encryption software on the computer. The objective of this project is to write an encryption and decryption program for the microcontroller and use the STK 500 development board and Atmega 8515 microcontroller as an external encryption and decryption platform and the computer will be used as the interface platform between the user and the microcontroller. Programming language that is used to write the program is C language and the GUI will be designed using MFC software.

ABSTRAK

Projek ini adalah bertujuan untuk menghasilkan sebuah perisian enkripsi teks dengan menggunakan *microcontroller*. Enkripsi adalah satu proses menukarkan sesuatu perkataan yang boleh difahami kepada bentuk yang tidak boleh difahami. Tujuan menukarkan perkataan kepada bentuk yang tidak boleh difahami adalah untuk menyembunyikan sesuatu informasi supaya tidak mudah dibaca oleh orang lain terutama sekali jika informasi itu adalah penting dan perlu dirahsiakan daripada orang lain. Perkembangan teknologi maklumat pada masa kini dan juga perkembangan teknologi komputer yang pesat, menyebabkan keperluan untuk mengengkripsikan data adalah satu kemestian. Pada masa kini, kebanyakkan proses enkripsi dilakukan menggunakan komputer. Tujuan utama projek ini adalah untuk menghasilkan perisian enkripsi yang mampu digunakan pada *microcontroller* dan *microcontroller* itu akan diaplikasikan sebagai satu platform luaran untuk melakukan proses enkripsi. Dengan adanya platform luaran ini, beban kepada komputer dapat dikurangkan dan tidak perlu lagi bersusah- payah memasukkan perisian enkripsi ke dalam komputer. Objektif utama projek ini adalah menghasilkan peirisian enkripsi untuk *microcontroller* dan menggunakan STK500 *development board* dan *microcontroller* Atmega8515 sebagai platform enkripsi luaran. Bahasa komputer yang akan digunakan untuk menulis perisian tersebut adalah *C language* than aplikasi *MFC* pula akan digunakan untuk menghasilkan *GUI*.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

GUI - Graphical User Interface
MFC - Microsoft Foundation Class
AES - Advanced Encryption Standard
DES - Data Encryption Standard
3DES - Triple- DES
BF - Blowfish
ASCII - American Standard Code for Information Interchange
USB - Universal Serial Bus

LIST OF APPENDIX

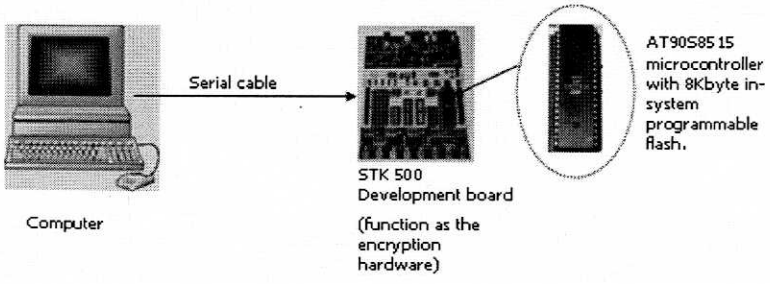
CHAPTER I

INTRODUCTION

In this chapter, a brief introduction on the project is given. The objective of the project, scope of work and problem statement is also discussed in this chapter.

1.1 Introduction

The idea of this project is to build a text encryption and decryption program for the microcontroller. The microcontroller will then be implemented on an embedded system. The embedded system suggested is the Atmel STK500 development board and the microcontroller used is the Atmega 8515 flash microcontroller. The development board will then be interfaced and connected to the computer externally via RS-232 9-pin serial cable. The development board will serve the purpose of an encryption and decryption hardware.



1.2 Objective

One of the objectives of this project is to write and produce a text encryption and decryption using microcontroller. Another objective is to learn about microcontroller and embedded system since the microcontroller working together wit the development board is an embedded system. Moreover, the objective of this project is also to use the microcontroller and the STK 500 development board as a hardware.

1.3 Scope of work

Scope of work is the work that is done in order to complete this project. This includes the work limitations, equipment used and work description.

1.3.1 Research

The scope of the research is research on microcontroller, embedded system, programming language and also embedded system. The source of the research will be journals, articles, books, user guides, datasheets and also thesis.

1.3.2 Programming Work

The scope of the programming wok will be to write a C language encryption and decryption program that will run on the microcontroller and also produce a GUI application for the computer.

1.3.3 Hardware

The scope of the hardware work is to integrate the hardware with the computer and to make it so that the microcontroller together with the development can be used as an external encryption/ decryption hardware. The work involves only using the hardware. No hardware development work is required.

1.4 Problem Statement

It is known that software encryption programs can demand a lot from the computer. There is also the hassle of installing encryption software. So, to take the load from the computer and remove the hassle of installing encryption software, it is ideal to have an encryption hardware that does the encryption externally.

Moreover, having the encryption program on the computer can be dangerous in term of security. Computers can be hacked and once the computer is hacked, the hacker will have access to the computer including the encryption program installed in the computer. One way to overcome this is by having the encryption to be done externally.

CHAPTER II

LITERATURE REVIEW

2.1 Background study

In this chapter, the history of cryptography and how cryptography came about are discussed. Also discussed in this chapter is the necessity of data encryption or in other words why encryption is done in the first place.

2.1.1 History of cryptography

The word "cryptography" is derived from the Greek words kryptos, meaning hidden, and graphien, meaning to write[1][2]. Historians believe Egyptian hieroglyphics, which began about 1900 B.C.E., to be an early instance of encipherment. Encipherment originally involved pen-and-pencil calculations. Mechanical devices were introduced to speed up encipherment in the eighteenth century, and they in turn were replaced by electromechanical devices. In those days, encryption started using character substitutions and transpositions to make data irrelevant.[3]

When two parties communicate over an open or insecure network, each needs to be certain of the identity of the other. Webster's dictionary defines authentication as "a process by which each party to a communication verifies the identity of the other."[3]. The term IFF, for identification, friend or foe, was an authentication protocol introduced during World War II to protect U.S. airspace from intrusion by enemy aircraft. The identity of a plane entering U.S. airspace was authenticated using a challenge– response pair; the correct response is determined by a cryptographic function of the challenge.[4]

One main element of cryptography is the encryption algorithm. Encryption algorithm is very important in cryptography because cryptography uses encryption algorithm to provide security and privacy. There are three classes of encryption algorithm, symmetric, asymmetric and digest algorithm. Encryption is the process of disguising a message in such a way as to hide its substance and meanings. The process of encrypting a message (plain text) is called encryption and the process of decrypting ciphertext back into plain text is called decryption.[1] [3][4][8].

The proliferation of computers and communication systems in 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services. Furthermore, computers allowed for the encryption of any kind of data that is represented by computers in any binary format, unlike classical ciphers which only encrypted written language texts, dissolving the utility of a linguistic approach to cryptanalysis in many cases. Many computer ciphers can be characterized by their operation on binary bit sequences (sometimes in groups or blocks), unlike classical and mechanical schemes, which generally manipulate traditional characters directly. However, computers have also assisted cryptanalysis, which has compensated to some extent for increased cipher complexity[3][4][5][6][8].

In today's modern world, modern cryptography is very important issue for providing security and privacy for e- commerce, which is conducted electronically. Moreover, it is very important in securing personal information which is stored on computer and transmitted over computer networks[1][3][4][6].

The three principal applications of cryptography are secrecy, authentication, and access control. Secrecy intends to deny information contained in text by disguising its form, for example,

a) In order to prevent an eavesdropper from learning the content of the communication when two users communicate over an open or insecure network; and
b) To hide information stored.

2.2 The necessity of data encryption

Today, the term "information highway" has become a household phrase. Anywhere and everywhere millions of people are using various form of electronic information exchange for numerous applications. It is fast, it is easy and it has become an integral part of our lives. However, there is always the question is communicating electronically secure?

Stories about hackers with malicious intents penetrating computers systems are abundant. Electronic thefts and the fraudulent use of electronic data are exploding. People are becoming more aware that when they use their ATMs at the local supermarket, pay bills with electronic fund transfers, chat with colleagues on a national bulletin board, share a file over e-mail, or send personal data in a fax, the information may be intercepted and read by people they never intended to see it[13].

Below are some of evidence of the seriousness of electronic theft[16]:

a) In the United States during 2001, the Internet Fraud Complaint Centre, organised by the United States Department of Justice and the Federal Bureau of Investigation, received 49,711 complaints relating to Internet fraud, 16,775 of which were referred to other authorities for further action. The average (median) monetary loss per referred complaint was US$435.00, with 43% of complaints relating to auction fraud.

b) The Federal Trade Commission's fraud database 'Consumer Sentinel', which compiles identity theft and consumer fraud data from United States and Canadian agencies, recorded over 200,000 complaints in 2001. This compares with 18,600 complaints in 1999, and 8,000 in 1998.

c) In a telephone survey of 1,006 online consumers conducted for the National Consumers League in the United States between April and May 1999, 24% said they had purchased goods and services online. However 7%, which represents 6 million people, said that they had experienced fraud or unauthorized use of credit card or personal information online.

d) One of the most recent studies of identity fraud in Australia was conducted by the Australian Bureau of Criminal Intelligence in 2002. In the pilot study, 23 law enforcement and other public sector agencies, and one private sector organization provided information relating to identity fraud offenders, fraudulent identities and victims of identity takeovers known to them. The study found that between 25 February 2002 and 23 August 2002, 1,195 fraudulent identities were identified relating to 597 suspects and involving 1,404 documents. 1,183 cases involved fraudulent identities, 12 cases involved identity takeovers, and 12 involved known identity fraud offenders. In all, 1,404 offences were identified in which $2,639,797 had been obtained and a further $239,532 attempted to be stolen.

This is where data encryption and cryptography comes into play. Encryption techniques can be used to mask electronic information and make it unreadable. Only by doing the decryption techniques can the information be converted back to readable format.

2.3 Literature review

In this section, the various application of encryption used today is discussed and also the pros and cons of doing encryption internally and externally. Also shown in this section are other similar technologies or products that are similar with the project or share the same basic concept as the project.

Moreover, the specification or background research on Caesar Cipher, the STK 500 development board and the Atmega 8515 microcontroller are also included in this section.

2.3.1 Common uses of encryption

As mentioned before, encryption has been used in many ways to ensure that the information is secure and safe. Below are the common uses and applications of encryption:

2.3.1.1 Authentication

Authentication is the process of logging in, signing on or in other words, presenting information or oneself in a manner that proves his or her identity[17]. The most common example of authentication is the use of a username and password to gain access to a system, network or websites. The username and password combination is often referred to as a person's credentials and it is frequently sent over networks. Encryption is used to protect these credentials. If no encryption is used to protect such information as it sent over the network, and attacker could capture those information and assume the identity of the originator.