UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DESIGN AND ANALYSIS SAFEST ENCRYPTION TELEVISION SIGNAL DISTRIBUTION

This report submitted in accordance with requirement of the Universiti Teknikal Malaysia Melaka (UTeM) for the Bachelor Degree of Engineering Technology
(Type your Department's course here) (Hons.)

by

NURFARAHIZZAH BINTI ABDULLAH
B071310932
921010-04-5090

FACULTY OF ENGINEERING TECHNOLOGY
2016

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN PROJEK SARJANA MUDA

TAJUK: **Design and Analysis Safest Encryption Television Signal Distribution**

SESI PENGAJIAN: **2016/17 Semester 1**

Saya **NURFARAHIZZAH BINTI ABDULLAH**

Mengaku membenarkan Laporan PSM ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka (UTeM) dengan syarat-syarat kegunaan seperti berikut:

1. Laporan PSM adalah hak milik Universiti Teknikal Malaysia Melaka dan penulis.
2. Perpustakaan Universiti Teknikal Malaysia Melaka dibenarkan membuat salinan untuk tujuan pengajian sahaja dengan izin penulis.
3. Perpustakaan dibenarkan membuat salinan laporan PSM ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (✓)

☐	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia sebagaimana yang termaktub dalam AKTA RAHSIA RASMI 1972)
☐	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)
☑	TIDAK TERHAD	

Disahkan oleh:

Alamat Tetap:

BATU 18, KAMPUNG PAYA MAS,

84900 TANGKAK,

JOHOR.

Tarikh: 3/1/2017

Cop Rasmi:

CHAIRULSYAH WASLI
Pensyarah Kanan
Jabatan Teknologi Kejuruteraan Elektronik dan Komputer
Fakulti Teknologi Kejuruteraan
Universiti Teknikal Malaysia Melaka

Tarikh: 3-1-17

** Jika Laporan PSM ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan PSM ini perlu dikelaskan sebagai SULIT atau TERHAD.

DECLARATION

I hereby, declared this report entitled "DESIGN AND ANALYSIS SAFEST ENCRYPTION TELEVISION SIGNAL DISTRIBUTION" is the results of my own research except as cited in references.

Signature : .....

Author's Name : NURFARAHIZZAH BINTI ABDULLAH

Date : 3/1/2017

APPROVAL

This report is submitted to the Faculty of Engineering Technology of UTeM as one of the requirement for the award of Bachelor's Degree of Electronic Engineering Technology (Telecommunications) with Honours. The following are the members of supervisory committee:

(Supervisor)

ABSTRACT

This project proposes the design, analysis and animation of encryption television signal then compare the result of technique and simulation. The basic principle to design safest encryption television signal is cryptography technique. This project is mainly focused on understanding about encryption and decryption operations with the design the safest one. The design includes the animation and geographical user interfaces (GUI) MATLAB. To do the comparison between the techniques is use and simulation by using the geographical user interface software to analyse the result. The project outcome is to overcome the lack of understanding about television signal encryption in FTK.

ABSTRAK

Projek ini mencadangkan reka bentuk, analisis dan animasi tentang penyulitan isyarat televisyen dan kemudianya membandingkan hasil perhitungan, simulasi dan pengukuran. Prinsip rekaan keselamatan penyulitan isyarat televisyen ini adalah berdasarkan kiptografi teknik. Projek ini sebahagian besarnya fokus pada fahaman tentang operasi penyulitan and penyahsulitan dengan mereka yang paling selamat. Reka bentuk termasuk animasi dan antara muka pengguna (GUI) geografi MATLAB. Lakukan perbandingan antara teknik parameter dan simulasi dengan menggunakan perisian antara muka pengguna yang geografi untuk menganalisis keputusan. Hasil projek adalah untuk mengatasi dari kekurangan persefahaman tentang penyulitan isyarat televisyen dalam FTK.

DEDICATIONS

Alhamdulillah, praise to the Almighty Allah S.W.T

This thesis is dedicated to:

To my mom,

Arah binti Tawil

For raising me become who I am today.

To beloved siblings,

My Supervisor,

My lecturers,

And all my friends.

Thanks for their encouragement and supported.

ACKNOWLEDGEMENTS

Alhamdulillah, thanks to Allah because of His blessing, I finally complete and finish my final year project successfully.

During the process to complete my project objective, I do a lot of research either by using internet, reading past year thesis, reference books and journal. With the guidance and support from peoples around me, I finally complete the project due to the time given. Here, I want to give credit to those who helped me to achieve what I had achieved in my final year project.

First and foremost, I would like to express my deepest gratitude to my project's supervisor, En. Chairulsyah bin Abdul Wasli for giving me an opportunity working under his supervision throughout this project. The project would not be completed under the time frame without their supervision. He always gives me the wisdom to think and work independently.

I would also like to thank other lecturers for giving me the advices and the opportunity to handle this project as well as their encouragement. Thanks also to my friends to had been providing me remarkable ideas to improve the project. At last but not least, I would like to express my gratitude to both of my parents who had provided me with financial support and encouragement throughout my course of studies. May Allah bless and reward them for their sincere, endeavour and contribution in the way of knowledge.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

LIST OF SYMBOLS AND ABBREVIATIONS

AES	-	Advanced Encryption Standard
AM	-	Amplitude Modulation
ATM	-	Automated teller machine
CATV	-	Cable TV
CCD	-	Charged-coupled Device
CFB	-	Cipher feedback
CW	-	Continuous Wave
DES	-	Data encryption standard
DTH	-	Direct to home
FM	-	Frequency Modulation
HBO	-	Home box office
IF	-	Intermediate Frequency
RF	-	Radio Frequency
RSA	-	Rivest, Shamir and Adleman
SSH	-	Secure Sockets Layer
SSL	-	Secure Socket Layer
TLS	-	Transport Layer Security
UHF	-	Ultra-High Frequency
VHF	-	Very High Frequency

CHAPTER 1
INTRODUCTION

1.0 Introduction

This chapter provides an introduction of safest encryption television signal distribution. This chapter introduces the project with its background, problem statement, objectives, scopes and project significance, to provide a sense of purpose and reasons to proceed with this project.

1.1 Background

The data or information security technology is one of the key technologies support for the new media of radio and television industry. Encryption television signal refers to as scrambling whereby to protect or prevent TV signal from hackers. In another word, encryption is to prevent or keep any sensitive information from being stolen and utilized for illegal purposes. Techniques of scrambling with respect to encryption technology. Besides that, encryption is utilized to control access to pay television services, usually applied to cable or satellite television services. Cable and satellite television services typically encrypt or scramble the signal of channels that the subscriber has not purchased therefore only people who paid for the service will receive and view it. This project will design and analyse the theoretical of encryption TV signal, animation, and simulation aspect. To show how the system of this project functionally by creating an animation with used an Adobe Flash Player. In order to design and analyse, the technique and simulation use Geographical User Interface (GUI) MATLAB simulation is to be prepared. The parameter such as substitution

technique and another parameter will be affected by it. The task is study literature, design, animation, technique, and simulation.

1.2 Problem Statement

There is a few problem of this research, first is rare and lack of understanding about TV signal encryption in FTK. This is because topic about the encryption television signal does not cover in any of the subjects in FTK and less disclosed to students. Therefore, we need to study and research about this topic. Second, an encryption technique is still not widely applied. The reason is people less concern about encryption system, so the system is rarely used in anywhere. Even though, encryption is a very important topic to understand. As we know, security is one of the most important factors in life. It can be useful anywhere anytime. It also helps protect your data, your interactions, and your access even when attackers make and runs around software defences. It is also critical to use properly because, in a public network, there are still opportunities for data to leak out, even if your software is standing guard effectively. Lastly, data hacker's case still happens. This is because nowadays hackers are increasingly rampant. Therefore, we need to take action to reduce hacker using the encryption system.

1.3 Objectives

The main objectives of this research is deeply concentrated on aspect as listed below:

I. To understand encryption system in television transmission signal.
II. To design the technique of safest encryption television signal.
III. To analyse the finding result.

1.4 Project Scope

This project will focus on the study of literature about encryption television signal. Other than that, it also involves in design, animation, technique and simulation. Besides that, this project needs to present the animation that shows how the system functioning and result will be attractive and effective. In addition, this project also involves in finding parameter and create the simulation part to show the technique that be used. The comparison between simulation and technique will also take place. MATLAB software is an instrument that can be used to simulate the results. Moreover, all the data will be analysed after finding the experiment result. Lastly, when all the process is completed, all information is arranged and starts writing a final report.

1.5 Project Significance

The report overall consists of five chapter. Following is an each chapter description in this thesis.

Chapter 1 is delivering term of design safest encryption television signal distribution. It also contains objective, scopes of work and problem statement of this project.

Chapter 2 is a literature review on theoretical concepts applied in this project. The chapter consists explanation about an overview of transmission of a television signal, encryption systems, an application that are related and etc. This chapter also present the design of encryption system within of television signal is to protect television signal from hackers and to prevent any sensitive information from being stolen.

Chapter 3 is Methodology. It is an important part of the whole project because it shows out how the project's activity is developed for Chapter 3.

In Chapter 4, all the analysis result from the animation and GUI MATLAB software. Expected result also will be explained in this chapter. Lastly, write the discussion from the analysis result.

Chapter 5 is the last chapter that will be the summary of the whole project. The problem facing during work progress also will be discussed in this chapter. Besides it also concludes with some recommendation that can be implemented in future.

CHAPTER 2
LITERATURE REVIEW

2.0 Introduction

This chapter provides understandings of theories and previous researches that are related to this final year project. This also includes an overview of transmission of a television signal, cryptography technique, encryption and decryption systems, and an application that are related and so on. Nowadays, security is one of the most important factors in life. It can be useful anywhere and anytime. This chapter also present the design of encryption system within of television signal is to protect television signal from hackers and to prevent any sensitive information from being stolen. In a television signal, the encryption system is utilized to control access to pay television services usually applied to cable or satellite television services. Therefore, only people or subscribers who paid for the service will receive and view the signal of television that displayed on the TV screen.

2.1 Encryption system

In an era where security breaches seem to be regularly making the news. There are many aspects to security and in applications, between secure commerce and payments to private communications and also to protect the passwords. Therefore, encryption is a very important topic to understand. It helps protect your data, your interactions, and your access even when attackers try to hack around software defenses.

Encryption is a control system that can reduce the risks and costs of the incidents while providing protection for data. The encryption system is a translation of signal code and is the most effective way to achieve data security. Therefore, the encryption also means scrambling data in such a way that only someone who has a secret code or key can access and read it. In other words, the main purpose of encryption is to prevent any sensitive information from being stolen and used for illegal purposes. Today, encryption is much better, but it functions as the common purpose of sending a secret message or information from one place to another without anyone can read it. For example, encryption is one of the most important for e-commerce as it allows private information such as details of the credit card to be sent safely to the online shop that is visiting. An encryption method referred as Secure Socket Layer (SSL) is utilized in Web browsers to encrypt purchase details. Besides that, encryption also is used to protect data in transit sent from all sorts of devices across all sorts of network, not just the internet but every time someone uses an automated teller machine (ATM) or buys something online with a smartphone, the encryption system is utilized to protect the information being relayed. (Josefson, 2000)

2.1.1 Encryption and Decryption Technique

Encryption is a component and some algorithms that are known as a cipher to hide the information which is called a secret code. Some code or password is needed to make information accessible and the process useful. Therefore, by using encryption algorithms process, it can change the information into incomprehensible symbols. Encryption includes the text, number, and images, audio and so on. However, encryption is the process of translating plain text data known as plaintext into something that random data and more complex known as ciphertext, while decryption is the process of converting ciphertext back to plaintext. (Tunga et al., 2014)

2.1.2 Ciphers

Ciphers is a mathematical function utilized for encryption or decryption. In most cases, two related functions which are one for encryption and the other for decryption are employed. Therefore, many categories of ciphers advanced over time.

Ciphers will be changed in the digital era. There are generally based on two types of algorithms, one using the same key to encrypt and decrypt, and another one using different keys to encrypt and decrypt. These two types also called as symmetric and asymmetric key algorithms with respectively. The one that uses symmetric keys falls into private-key cryptography while asymmetric key algorithms fall into public-key cryptography. Two methods that used in the symmetric key algorithm, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) are two well-known of ciphers while RSA (Rivest, Shamir, and Adleman) is a well-known cipher based on asymmetric key algorithms. (Takeya, 1989)

Example of encryption and decryption process are shown in Figure 2.1 below.

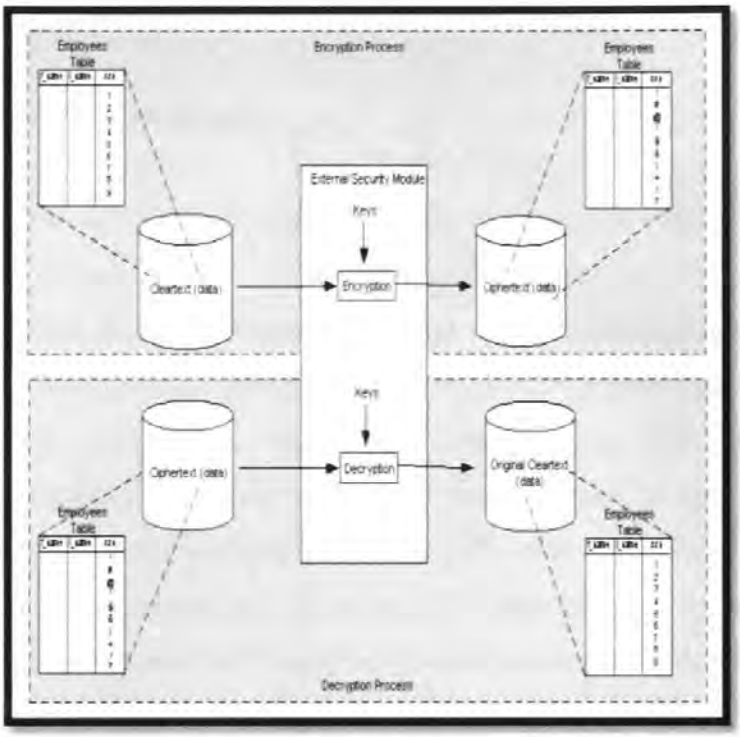

Figure 2.1: Example of encryption and decryption process

2.2 Introduction of Cryptography

Cryptography is the study of secret information or information hiding and to prevent disclosure of their contents through signal interception using codes, ciphers, and other methods, data can be encoded with verification that concerns the ways in communication. Therefore, only certain people can see the real message. It includes security to prevent unauthorized to access private information.

In telecommunications, cryptography is required when communicating over any untrusted medium, which includes any network. Besides, the principles of cryptography can be applied to the encryption of the television and computer network