CHAPTER 1

INTRODUCTION

1.1 Project Overview

Security in computing focuses on confidentiality, integrity, authenticity and non-repudiation. Confidentiality ensures that patient's information is accessible only by authorized parties. Strong user and computer authentication ensures that the origin of a message is correctly identified. Integrity protects against unauthorized modification of data. Access control provides protection against unauthorized use of resources. Non-repudiation requires that neither the sender nor the receiver of a message be able to deny the transmission of data.

This project introduces a new encryption algorithm. It is a block cipher with a 128-bit block size and a 256-bit key. For many applications, the Data Encryption Standard algorithm is nearing the end of its useful life because of its 56-bit key size. This project is a preliminary into the practical and theoretical aspects in designing a block cipher. The philosophy behind the design of the block cipher is the simplicity of the design of algorithm, which is more amenable to analysis than a more complex design. The design strategy divides the block cipher into major components, each with well-defined functionalities and properties.

The block cipher is an iterated block cipher, using a standard substitution-permutation network, which has undergone cryptanalysis over many years. It uses algorithmic substitution boxes generated using mathematical principles such that it is proven to be secure against linear and differential cryptanalysis. The permutation

layer uses a combination of linear mixers that possess highly diffusive properties. The algorithm uses a table lookup and simple Boolean operations to achieved optimized performance. The design produces a block cipher with good security level and performance.

1.2 Project Objective

Cryptography has been of interest primarily to the military and diplomatic communities. Today, however, several factors have combined to stimulate great interest in commercial applications. The rise of data crime in recent years has emphasized the need for techniques to protect information [1]. Cryptographic systems can be classified into two groups: private key cryptosystems and public key cryptosystems. Private key cryptosystem, such as DES (Data Encryption Standard) provides a practical solution for a variety of applications. Today, the cryptographic community is quite aware of the fact that breaking DES has become much more feasible than it was previously thought because of its small key size. This project intends to develop an encryption algorithm that is not only secure, but one that has good performance and is suitable for hardware and software implementations. The objective is to analyze the properties of a secure block cipher and design a block cipher that has good security features and optimum performance.

1.3 Project Scope

This project covers the full cycle of the development of a block cipher, i.e. research of encryption algorithms, analysis and design of a new block cipher and testing of the block cipher developed. The studies of encryption algorithms include

mathematics preliminary required for encryption algorithm, various cryptographic properties of block cipher

1.4 Significance of Study

This dissertation focuses on a private-key cryptosystem. We categorize a block cipher into three components and analyze various cryptographic properties of each component as well as the structure of a block cipher. Based on the analysis performed, we introduce a new block cipher cryptosystem with a block length of 128 bits and key length of 256 bits. It consists of a uniform Substitution Permutation Network with the advantage that the same network can be used to perform both the encryption and the decryption operations. It uses nonlinear algorithmic S-Boxes, which are based on mathematical theory and contains no trapdoors. Unlike DES which has bit-oriented permutation, the proposed cipher has a linear mixer with uniform and good diffusion properties. The linear mixer uses byte-oriented operations that makes the cipher suitable for both hardware and software implementations. The nonlinear and highly diffusive key schedule immunizes the key schedule against related-key attacks. Its 256-bit key length solved the short key length problem faced by DES and should be sufficiently large enough for critical applications in future.

The principle goal of designing a private-key cryptosystem must be security. In the real world, however, performance is always of concern. The proposed private-key cryptosystem is designed to improve the overall performance by using table lookup and simple Boolean operations in its algorithm. This contributes to the speed of the algorithm compared to other algorithm that uses key-dependent S-Boxes,

variable rotation, etc. This is important to ensure that the proposed cryptosystem can be implemented efficiently in a variety of cryptographic applications.

1.5 Dissertation Organization

This dissertation is organized as follows: Chapter 2 focuses on the private-key cryptosystem, which is the main objective of this research. The discussion covers the basic concepts used in a cryptosystem, Data Encryption Standard (DES) and the problems of DES. This chapter also investigates other alternatives to DES, including some well-known block cipher as well as multiple encryption, a technique to strengthen DES. Analysis is performed to determine the reasons of designing a new block cipher.

Chapter 3 analyses the requirements for block cipher design. This includes the common cipher structures, the different components of a block cipher and the important cryptographic properties of each components and ways to increase block cipher's strength against attacks.

Chapter 4 covers the design phase of the block cipher, which includes a description of the major design principles underlying the proposed block cipher, an overview of the basic building blocks of the block cipher, the design strategy used and the design rationale of the various components of the block cipher, including the structure of the cipher, S-Boxes, diffusion layer and key scheduling.

Chapter 5 describes the testing methods of the important cryptographic properties of the block cipher, and analyses the results.

Finally, Chapter 6 summarizes the entire development process by discussing the motivation for this research, significance of the research, future enhancements and an overall conclusion of the project.