UNIVERSITI PUTRA MALAYSIA

KEY TRANSFORMATION APPROACH FOR RIJNDAEL SECURITY

MEK RAHMAH BINTI SULONG.

FSKTM 2008 3

KEY TRANSFORMATION APPROACH FOR RIJNDAEL SECURITY

By

MEK RAHMAH BINTI SULONG

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in fulfillment of the Requirements for the Degree of Master of Science

February 2008

Dedicated to my honorable supervisor; Associate Professor Ramlan Mahmod, my supportive co-supervisor; Mrs. Zaiton Muda, my friends, and my beloved family.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science

KEY TRANSFORMATION APPROACH FOR RIJNDAEL SECURITY

By

MEK RAHMAH BINTI SULONG

February 2008

Chairman: **Associate Professor Ramlan Mahmod, Phd.**

Faculty: **Computer Science and Information Technology**

Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen in 1999. It is a combination of security, performance, efficiency, implementability and flexibility that makes it the best selection for Advanced Encryption Standard (AES). However, the 128-bit Rijndael Key Schedule does not satisfy the frequency (bit confusion) test for majority of Subkeys and does not satisfy the avalanche (bit diffusion) test for any Subkeys. These contribute to some attacks in the Key Schedule. Thus, a new transformation method which is called "ShiftRow" is proposed into the 128-bit Rijndael Key Schedule based upon information principles (bit confusion and diffusion properties). The new method shifts the rows of the Rijndael Subkey after the RCon function is being applied to the Subkey. This method improves the security of Rijndael Key Scheduling by increasing

the bit confusion and diffusion of the Rijndael Subkey. The new method has shown positive results in terms of the bit confusion and diffusion of Subkey and it has increased bit confusion and diffusion compared to the Subkey of the original Rijndael Key Schedule.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

PENDEKATAN KUNCI TRANSFORMASI UNTUK KESELAMATAN RIJNDAEL

Oleh

MEK RAHMAH BINTI SULONG

Februari 2008

Pengerusi: **Professor Madya Ramlan Mahmod, Ph.d.**

Fakulti: **Sains Komputer dan Teknologi Maklumat**

Rijndael adalah sebuah blok cipher yang telah direkabentuk oleh Joan Daemen dan Vincent Rijmen pada tahun 1999. Ia merupakan suatu kombinasi keselamatan, persembahan, keefisyenan, perlaksanaan dan kesesuaian menjadikannya sebagai pilihan yang terbaik untuk Advanced Encryption Standard (AES). Bagaimanapun, Penjadualan Kunci Rijndael tidak berjaya melepasi ujian frekuensi (pengeliruan bit) bagi kebanyakan Sub-Kekunci dan tidak berjaya melepasi ujian avalanche (pencampuran bit) bagi sebarang Sub-Kekunci. Hal ini akan menyumbang kepada pencerobohan ke atas Penjadualan Kunci. Oleh itu, satu kaedah transformasi baharu yang dinamakan "ShiftRow" telah diajukan untuk ditambah ke dalam Penjadualan Kunci Rijndael yang mana ianya berdasarkan prinsip maklumat (ciri-ciri pengeliruan dan pencampuran bit). Kaedah baru ini menganjak baris Sub-Kekunci Rijndael setelah fungsi RCon

diaplikasikan pada Sub-Kekunci. Kaedah ini memperelokkan keselamatan bagi Penjadualan Kunci Rijndael dengan meningkatkan pengeliruan dan pencampuran bit pada Sub-Kekunci Rijndael. Kaedah baru ini telah menunjukkan keputusan yang positif dari segi pengeliruan dan pencampuran bit bagi Sub-Kekunci dan ianya telah meningkatkan pengeliruan dan pencampuran bit dibandingkan dengan Sub-Kekunci Jadual Kunci Rijndael asal.

ACKNOWLEDGEMENT

Praise to Allah S.W.T. for giving me the strength, patience, and motivation to complete this research.

My deepest appreciation and gratitude is dedicated to the research committee lead by Associate Professor Ramlan Mahmod and Mrs. Zaiton Muda for their motivation, guidance, encouragement, support, and assistance throughout the research.

My deepest thank go to my family and colleagues at the Faculty of Computer Science and Information Technology, UPM, for their supports during the process of completing this research.

As for financial support, I am grateful to PASCA for giving me the scholarship while I was completing this research. Thank you all and may God bless all these individuals for their kindness.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ALGORITHMS

LIST OF ABBREVIATIONS

NIST	-	National Institute OF Standards and Technology
AES	-	Advanced Encryption Standard
DES	-	Data Encryption Standard
GF	-	Galois Field
XOR	-	Exclusive XOR
NBS	-	National Bureau of Standard
DEA	-	Data Encryption Algorithm
RSA	-	Rivest Shamir Adlemen
IEEE	-	Institute of Electric Electronic Engineering
ANSI	-	American National Standards Institute

CHAPTER 1

INTRODUCTION

1.1 Introduction

Cryptography is the science of encoding and decoding secret messages (Alex Brennen V., 2004). The term *cryptanalysis* is the study of cryptographic algorithms or resulting Ciphertext in order to determine their strengths and potential weaknesses. Often such analysis is performed to break an encryption algorithm or in order to perform key recovery (Alex Brennen V., 2004). *Cryptology* is the science of making and breaking secure codes. *Cryptosystem* is a protocol or method of performing encryption (Alex Brennen V., 2004). There are two types of cryptosystems: symmetric and asymmetric key. Both encrypt messages use computer algorithm and provide users with the secrecy through the use of cryptographic keys but still, there are differences in the way the keys are being used. A symmetric cryptosystem has a single key (see Figure 1.1), which is used for both encrypting and decrypting messages. Mathematical process is used in an algorithm to transform Plaintext into Ciphertext and vice versa, with each transformation depending on the value of the key.

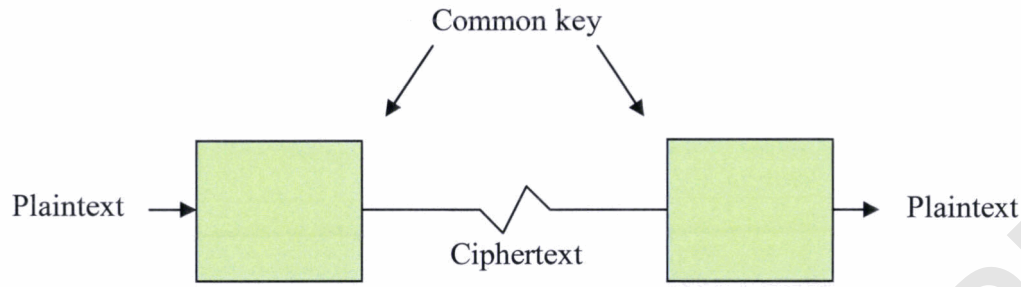

Figure 1.1: A Symmetric Cryptosystem

Data Encryption Standard (DES) is a well-known example of symmetric cryptosystem. Others are Triple DES, IDEA, RC2, RC4, RC5, and Blowfish. In contrast to symmetric cryptosystem, public-key cryptosystem uses complementary pair of keys to separate the process of encryption and decryption as shown in Figure 1.2. One key is considered a pair, with the private key kept secret while the other is made public. However, this research focuses on symmetric-key cryptosystem only. Hereinafter, detailed description for both cryptosystems will be explained in Chapter 2.

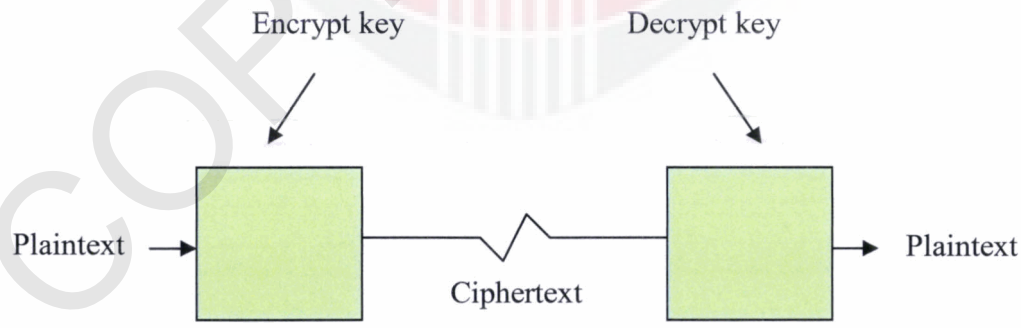

Figure 1.2: A Public-Key Cryptosystem

The growth of cryptology has made the variety of algorithms, including DES being exposed to various types of attack. In 1997, the National Institute of Standards and

Technology (NIST) US (an agency of the US Department of Commerce's Technology Administration), initiated a process to select a symmetric-key encryption algorithm to be used to protect sensitivity (unclassified) of Federal information in furtherance of NIST's statutory responsibilities and to be adopted as Advanced Encryption Standard (AES).

In the same year, NIST announced the acceptance of fifteen candidate algorithms and requested assistance of the cryptographic research community in analyzing the candidates. NIST reviewed the results of the preliminary research and selected Rijndael, Twofish, RC6^{TM}, MARS and Serpent as finalists. Having reviewed further public analysis of the finalists, NIST has decided to propose Rijndael as the Advanced Encryption Standard (AES) (Nechvatal et. al., 2000). Rijndael is a block cipher designed by Joan Daemen and Vincent Rijmen. According to Nechvatal et. al. (2000), it is a combination of security, performance, efficiency, implementability and flexibility that makes it an appropriate selection for AES for the purpose of usage in the current and future technology.

There are many other further analysis and improvements that have been done on Rijndael (Daemen et. al., 1999). McLoon W. et. al. (2001) proposed Field Programmable Gate Arrays (FPGAs) Rijndael encryption design, utilizes look-up tables to implement entire Rijndael round function. In the same year, Jing et. al. (2001) derived a new algorithm for computing inverse in GF(2^m) on the standard basis. Sklavos et. al. (2002) designed alternative architectures and VLSI implementation designs. These designs operate for both encryption and decryption processes in the same device. Xinmiao et. al. (2002) addressed various approaches for efficient hardware