UNIVERSITI PUTRA MALAYSIA

IMPROVING THE RANDOMNESS OF OUTPUT SEQUENCE FOR THE ADVANCED ENCRYPTION STANDARD CRYPTOGRAPHIC ALGORITHM

SHERIF ABDULBARI ALI.

IMPROVING THE RANDOMNESS OF OUTPUT SEQUENCE FOR THE ADVANCED ENCRYPTION STANDARD CRYPTOGRAPHIC ALGORITHM

By

SHERIF ABDULBARI ALI

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

December 2005

Dedicated to my parents

Abstract of thesis presented to the Senate of Univeristi Putra Malaysia, in fulfilment of the requirements for the degree of Master of Science

IMPROVING THE RANDOMNESS OF OUTPUT SEQUENCE FOR THE ADVANCED ENCRYPTION STANDARD CRYPTOGRAPHIC ALGORITHM

By

SHERIF ABDULBARI ALI

December 2005

Chairman: **Associate Professor Ramlan Bin Mahmod, PhD**

Faculty: **Computer Science and Information Technology**

Rijndael, the Advanced Encryption Standard (AES) is an encryption standard uses ByteSub, Shiftrow, Mixcolumn and KeyExpansion functions which are the principle of generating a random and pseudorandom numbers. AES has larger S-boxes, but a very simple algebraic description that make it particularly vulnerable. Attacks against simplified variants of the AES algorithm have been reported for 128-bit keys, 7 rounds out of 10 have been attacked; for 192-bit keys, 7 rounds out of 12 have been attacked; for 256-bit keys, 9 rounds out of 14 have been attacked. NIST stated that AES appears to offer an adequate security margin. It is estimated that attacks in the indicated number of rounds above would result in a heavy cost to resources. Thus, it may be some time before malicious hackers have the ability to break AES in its original form. However, the rapid growth of computer technology and its resources may make this time shorter than NIST estimated time to break the algorithm. This research proposes a transformation function to be added to the AES algorithm. The new transformation function is shifting the columns of the AES state after the

Mixcolumn function is applied to the state. This transformation function improves the security of the AES algorithm by increasing the randomness of the AES output sequence. The new approach has shown positive result in terms of the randomness of output sequence. The approach has increased randomness in comparison to the output sequence of the original AES algorithm.

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

MEMPERBAIKI KERAWAKAN JUJUKAN OUTPUT BAGI ALGORITMA KRIPTOGRAFIK ADVANCED ENCRYPTION STANDARD

Oleh

SHERIF ABDULBARI ALI

December 2005

Pengerusi: **Profesor Madya Ramlan Mahmod, PhD**

Fakulti: **Sains Komputer dan Teknologi Maklumat**

Rijndael yang dikenali sebagai Advanced Encryption Standard (AES) adalah satu piawaian enkripsi yang menggunakan fungsi ByteSub, Shiftrow, Mixcolumn dan KeyExpansion yakni prinsip di atas penjanaan nombor rawak dan separa rawak. AES mempunyai Kotak-S yang lebih besar tetapi penerangan algebra mudah yang menyebabkannya mudah diserang. Serangan ke atas varian-varian yang dipermudahkan telah dilaporkan untuk kunci 128-bit, 7 pusingan dari 10 telah diserang; untuk kunci 192-bit, 7 pusingan dari pada 12 telah diserang; untuk kunci 256-bit, 9 pusingan dari pada 14 telah diserang. NIST menyatakan bahawa AES memberikan margin keselamatan yang mencukupi. Adalah dianggarkan bahawa serangan pada bilangan yang disebutkan di atas akan menyebabkan kos yang tinggi terhadap sumber, oleh kerana itu mungkin masa yang panjang diperlukan sebelum pengodam mempunyai kemampuan untuk memecahkan AES dalam bentuk asalnya. Walaubagaimanapun, perkembangan panatas teknologi komputer dan sumber berkaitan mungkin memendekkan masa yang dianggarkan oleh NIST untuk

memecahkan algoritma tersebut. Kajian ini mencadangkan penambahan fungsi tranformasi pada algoritma AES. Fungsi tranformasi yang baru ini menganjak lajur keadaan AES setelah fungsi Mixcolum diaplikasikan pada keadaan. Fungsi transformasi ini memperelokkan keselamatan dengan penambahan kerawakan pada jujukan output AES. Pendekatan yang baru ini telah menunjukkan keputusan yang positif dari segi kerawakan pengeluaran jujukan output. Pendekatan ini telah menambah kerawakan pengeluaran jujukan output dibandingkon dengan jujukan output algoritma AES asal.

ACKNOWLEDGMENTS

First and foremost, I thank God for His endless guidance, help, blessings and motivation to complete this research work.

I also extend my heartfelt gratitude to the research committee lead by *Prof.Madya Dr. Ramlan Mahmod, Prof.Madya Dr. Abdul Azim Abd.Ghani* for providing me their virtuous guidance, support, help and encouragement throughout this research.

My sincere gratitude also goes to my family who is always there, supporting me. Thank you for your prayers.

For financial support, I'm grateful to Sana'a Community College (SCC) in Republic of Yemen for giving me the scholarship while I was carrying out this research. Thank you all and may God bless all these individuals for their kindness.

I certify that an Examination Committee met on 9th of December 2005 to conduct the final examination of Sherif Abdulbari Ali on his Master of Science thesis entitled "Improving the Randomness of Output Sequence for the Advanced Encryption Standard Cryptographic Algorithm" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Univeriti Pertanian Malaysia (Higher Degree) Regulation 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Hj. Mohd Hasan Selamat
Associate Professor
Faculty of Computer Science and Information Technology
Univeriti Putra Malaysia
(Chairman)

Azmi Bin Jaafar, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Univeriti Putra Malaysia
(Internal Examiner)

Mohamad Rushdan Md. Said PhD
Associate Professor
Institute for Mathematical Research
Univeriti Putra Malaysia
(Internal Examiner)

Abdullah Mohd Zin, PhD
Associate Professor
Faculty of Information Science and Technology
Univeriti Kebangsaan Malaysia
(External Examiner)

HASANAH MOHD. GHAZALI, PhD
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date : 16 FEB 2006

This thesis submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfillment of the requirements for the degree of Master of Science. The members of the Supervisory Committee are as follows:

Ramlan Mahmod, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

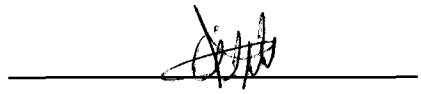
Abdul Azim Abd.Ghani, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

AINI IDERIS, PhD
Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date : 09 MAR 2006

DECLARATION

I hereby declare that the thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UPM or other institutions.



SHERIF ABDULBARI ALI

Date: 10/02/2006

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard
NIST	-	National Institute Standards and Technology
NBS	-	National Bureau Standards
NSA	-	National Security Agency
DES	-	Data Encryption Standard
GF	-	Galois Field
DFA	-	Differential Analysis Attack
PES	-	Proposed Encryption Standard
IPES	-	Improved Proposed Encryption Standard
IDEA	-	International Data Encryption Algorithm
RSA	-	Rivest Shamir Adlmen
DEA	-	Data Encryption Algorithm
FIPS	-	Federal Information Processing Standards
RNG	-	Random Number Generator
PRNG	-	Pseudo Random Number Generator

CHAPTER 1

INTRODUCTION

1.1 Background

In this days and age, for security purposes, some installations recognize computers and their data as valuable and vulnerable resources and have applied appropriate protection. An exposure is a form of possible loss or harm in a computing system; examples of exposures are unauthorized disclosure of data, modification of data, or denial of legitimate access to computing. A vulnerability is a weakness in the security system that might be exploited to cause loss or harm. The major assets of computing systems are hardware, software and data. There are four kinds of threats to the security of a computing system: interruption, interception, modification and fabrication. The four threats all exploit vulnerabilities of the assets in computing systems. Cryptographic techniques can be used to defend these data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.

Cryptography means hidden writing which is basically the practice of using mathematics to conceal data. Cryptography is concerned with keeping communications private so we can store information or transfer it across any insecure means that cannot be read by others except the intended recipient. A cryptographic algorithm is a mathematical function used in the encryption and decryption process. A cryptographic algorithm works in combination with a key word, number, or phrase

to encrypt the plaintext. The same plaintext encrypts to different ciphertext with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key.

In conventional cryptography, also called secret-key or symmetric key encryption, one key is used for both encryption and decryption. The Data Encryption Standard (DES) in an example of a conventional cryptosystem that has been widely deployed by the U.S. Government and the banking industry. Triple DES (3DES), IDEA, Blowfish, RC2 and AES are other examples of symmetric key encryption. Triple DES is simply the DES repeated 3 times with a separate key for each stage. The alternative to DES and Triple DES is IDEA (International Data Encryption Algorithm). IDEA which is the one of the best symmetric encryption algorithms currently available. This encryption is not only secure but also fast. This algorithm was developed in Zurich at the start of the 1990s by cryptographers Xuejia Lai and James Massey (Xuejia and James, 1991). They proposed a secret-key block cipher. It is a Feistel network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be at any length up to 448 bits. Although there is a complex initialization phase that is required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. The RC symmetric encryption algorithm is a cipher with variable key length; it has been developed by Ron Rivest. The RC family has several members RC2, RC4, RC5 and RC6 which are equally important to symmetric encryption algorithms.

In 1997, NIST announced the initiation of an effort to develop the AES and NIST announced the acceptance of fifteen candidate algorithms and requested the

assistance of the cryptographic research community in analyzing the candidates. Rijndael is one of the five finalist algorithms in the NIST Advanced Encryption Standard (AES) project. The AES is (Bellare and Rogaway, 2001) a new block cipher design, with a 128-bit block size, and key sizes in 128, 192, or 256 bits. Fifteen design teams from around the world submitted candidate algorithms when NIST asked for competitive public submissions in 1996. NIST selected the best five of them in 1998 which were Twofish, Serpent, Rijndael, RC6, and MARS.

NIST selected the winner from these five excellent algorithms. All of the top five AES finalists have received intense cryptanalytic scrutiny from the best cryptographers in the world, many of whom have AES submissions of their own that compete with the others. In October 2000, NIST selected Rijndael as the proposed Advanced Encryption Standard (AES), replacing the data encryption standard (DES), which has been the standard since 1977.

The AES, Rijndael. Joan Daemen and Vincent Rijmen's algorithm AES uses 8-bit S-boxes as its source of nonlinearity and simple XOR (exclusive-or) operations. Due to its simple operations and byte orientation, AES is fast in hardware and on 8, 32 and 64-bit microprocessors. AES was the only finalist that adjusts the number of rounds needed for each key size, improving performance for the 128-bit size. AES's combination of security, performance, efficiency, implementability and flexibility made it an appropriate selection for the Advanced Encryption Standard (AES), and as for use in the technology of today and in the future (Nechvatal et. al., 2000), (William, 2003).

1.2 Problem Statement

Randomness of the algorithm's output is required for cryptographic algorithm, where the randomness of the output is one factor of measuring security (Rukhin A et al, 2001). The NIST evaluation criteria of the cryptographic algorithm were divided into three major categories: Security, Cost and Algorithm and Implementation Characteristics, where the security was the most important factor in the evaluation (Nechvatal et al, 2000). The AES algorithm security depends only on the key's secrecy. The goal of a strong symmetric key encryption algorithm is that there is no way to decrypt the data except by knowledge of the key and there is no better way to find out that key than key exhaustion (William, 2003). The AES algorithm have been reported for 128-bit keys, 7 rounds out of 10 have been attacked; for 192-bit keys, 7 rounds out of 12 have been attacked and for 256-bit keys, 9 rounds out of 14 have been attacked by the Related-Key and Differential cryptanalysis attacks (Jamil, 2004), (Hee J et al, 2002), (Kim J et al, 2003) and (Ferguson N et al, 2001). This research proposed a modification on AES algorithm by adding a function to the algorithm. This function is used to increase the randomness of the AES algorithm output.

1.3 Objective

The main objective of this research is to improve the security of the AES algorithm by increasing the randomness of the numbers generated by the algorithm.

1.4 Methodology

The following points provide an explanation of how this research was carried out.

1.4.1 The Identification of the problem

The first step of in this research is to review and study current related papers about the Advanced Encryption Standard to understand the algorithm's process, current status of the AES and the latest Advances of the AES. After reviewing the related research, it was found that there is a security vulnerability in the AES algorithm. This is the area where the problem statement is derived from. It was reported that seven and nine rounds of the AES algorithm rounds have been attacked (Jamil, 2004), (Hee J et al, 2002), (Kim J et al, 2003) and (Ferguson N et al, 2001).

1.4.2 The Input Requirement

The inputs that have been used in this experiment can be divided into three types; plaintext, cipher key and key length. The plaintexts can be divided into two types, 128-bit plaintext means simple message (e.g. pin code 1234, this is a test etc) and long plaintext (text files with size 10KB, 20KB, 40KB etc). Where 128-bit plaintext is a minimum requirement for the block size (Nechvatal et al, 2000). The cipher key allows encryption of the plaintext, which must be kept secret, there are three different standard key sizes 128, 192 and 256 bits used to testify the two types of the plaintexts (Federal Information Processing Standards Publication, 2001).

1.4.3 Randomness Measurement

Statistical randomness measurements have been used in this experiment. (Rukhin et al, 2001) Various statistical tests will be applied to a sequence to attempt to compare and evaluate the output sequence to a truly random sequence. Randomness is a probabilistic property; that is, the properties of a random sequence that can be characterized and described in terms of probability value.

1.4.4 Design and Implementation

There are more than 60 experiments that have been done to achieve the objective of this research. The first experiment is to write the AES algorithm source code by using Visual Basic language and to ensure that the output is the expected output from original AES algorithm, which was tested by using the same cipher example input used in (Federal Information Processing Standards Publication (FIPS) 197, 2001) publication. The next step is to implement the new approach, which is a transformation function that shifts the columns of the state to be added to the AES algorithm; the new approach will be discussed in detail in chapter 4.

Next experiment is to run the input with AES and the new approach algorithm. The same plaintext, cipher key and key length were used for both algorithms. In the sample plaintext experiment 10 plaintext with 128-bit block length were used as inputs. Each plaintext has been tested by using three standard sizes of key length, which are 128,129 and 256 bits (Nechvatal et al, 2000). For the long plaintext experiment 10, text files with different sizes in kilo bytes were used as inputs. Each