Journal of Theoretical and Applied Information Technology
20th April 2016. Vol.86. No.2
© 2005 - 2016 JATIT & LLS. All rights reserved·

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVEMENT KEYS OF ADVANCED ENCRYPTION STANDARD (AES) RIJNDAEL_M

[1,2] MOHANAAD SHAKIR, [2] ASMIDAR BIT ABUBAKAR, [2] YOUNUS BIN YOUSOFF, [3]MUSTEFA SHEKER
[1]Alburaimi University Collage(BUC), Oman, [2]University Tenaga National(UNITEN) ,[3]National University of Malaysia(UKM)
E-mail: [1]mohanaad@buc.edu.om , [2]asmidar@uniten.edu.my,[3]Yunusy@uniten.edu.my,
[4]alnaser.mustafa@yahoo.com

ABSTRACT

Rijndael is a specification for the encryption of electronic data that considered as a collection of ciphers with distinct block and key sizes. This study aims to develop the key of Rijndael cipher in order to enhance the level of confusion and diffusion. The tools of analysis, design, implementation, testing, and evaluation have been applied by using the model of software system development life cycle (SDLC). The results of the study show that adding keys to the Rijndael will increase its security level and promote widely use in the organizations.

Keywords: *Information System Security, Cipher Algorithm, AES.*

1. INTRODUCTION

As defined by the U.S. National Institute of Standards and Technology (NIST) in 2001, the Advanced Encryption Standard (AES), originally referenced as Rijndael [1], [2], is a specification for the encryption of electronic data [3]. AES is based on the Rijndael cipher code designed by two cryptographers from Belgium, Joan Daemen and Vincent Rijmen, who proposed their project to NIST [4]. Rijndael is also considered as a collection of ciphers with distinct block and key sizes. For AES, three members of the Rijndael family were chosen by NIST, each with a block size of 128 bits with three different lengths for the key: 128, 192 and 256 bits. AES coming after its predecessor, the Data Encryption Standard (DES) [5] which was published in 1977, is the ultimate standard adopted by the U.S government. As described by AES, the algorithm is basically a symmetric-key code, i.e.: the same key is used for both encryption and decryption processes of the data. It is worth mentioning that on November 26, 2001, AES was announced by the NIST as U.S. FIPS PUB 197 [3]. Among the fifteen competing designs that were showcased, the Rijndael cipher was chosen as the most suitable and appropriate. AES was officially adopted as a federal government standard on May 26, 2002 following the approval of the Secretary of Commerce. Also, AES is available in many various encryption formats, and is the first open cipher source that is publicly accessible and approved by the National Security Agency (NSA) for top secret information. AES code design is based on a principle known as a substitution-permutation network. This principle is essentially a combination of both substitution and permutation which is fast for implementation under both software and hardware [6]. Unlike DES, AES is not based on a Feistel network. Another specification of the Rijndael is that it is specified with block and key sizes that may be multiples of 32 bits but with the requirement that both must be with a minimum of 128 and a maximum of 256 bits. AES operates on a 4×4 column-major order bytes matrix of, known as the *state*, and most AES calculations are performed in a specific finite field. The key size used for an AES cipher code determines the number of transformation repetitions required to convert the input (i.e.: plaintext), into the output (i.e.: cipher text).

The number of repetition cycles are organized as follows:

- 10 repetition cycles for 128-bit keys.
- 12 repetition cycles for 192-bit keys.
- 14 repetition cycles for 256-bit keys.

Each repetition round is composed of several processing steps, each one contains 4 similar stages, including one that is dependent on the encryption key itself. A set of reverse repetition rounds are applied to convert the cipher code text back into the original plaintext utilizing the same encryption key.

2. RELATED WORK

An extended version of Rijndael block cipher was designed by a research group in 2002[13]. The new expanded version of Rijndael (AES) is based on the same basic concepts and general structure of the original form. Consequently, it provides a stronger resistance against standard, previously known attacks. The main difference between this version and the original is that each word in the state array consists of 8-bytes (64-bits) instead of 4-bytes (32-bits). Other significant changes is that each column of the state is considered as an eight term polynomial with a single coefficient in Galois Field GF(28) and a multiplied modulo x8 +1 of static polynomials rather than 4-term polynomials with coefficient in GF(24) and multiplied modulo x4 +1 [7]. In 2003 another research group proposed an alternative version called the `Baby Rijndael` which essentially takes into consideration a new variant of AES with a smaller form factor that performs the encryption and decryption processes with block and key size of 16-bits. This cipher code was used as a homework assignment for the cryptography graduate course at Iowa State University. The goal was to utilize this cipher code to help the students learn how to implement Rijndael on a smaller scale and a more manageable degree. It is worth mentioning that all the parameters were significantly reduced in Baby Rijndael, while its original structure is maintained. However, this cipher was intended to be used for educational purposes and it is not considered appropriate for actual applications [8]. In 2004, a new variation of AES algorithm was introduced by another research group. This algorithm has the capability of generating a random pool of ciphering code keys. The algorithm selects the ciphering keys randomly from the pool of keys during the encryption process which means that the key expansion in ciphering and deciphering processes is redundant. Moreover, only the key length plus the index of the schedule key of keys pool is sent by the sender. By utilizing this information, the decipher code is extracted by the receiver without the need to any re-expansion [9]. Another simplified AES was proposed in 2005 by a research group. The proposed algorithm simply encrypts and decrypts with block and key size of 16-bits which also considers a reduced form of Rijndael cipher. It is worth mentioning that his cipher code is also intended for educational purposes which facilitates the understanding of the original version of Rijndael. It is worth noting here that this version is very simplistic in which examples could be worked out by hand, without the need of a computer [10]. In 2007 a research group from China introduced a technique known as Affine Power Affine (APA) for designing good S-box with enhanced resistance to algebraic attacks. The role of the S-box is to increase the complexity of algebraic expression and inherits desirable characteristics from AES S-Box with the APA structure. The algebraic complexity of the improved AES S-box is increased by an impressive factor [from 9 to 253], while its inverse S-box is maintained at 255. Additionally, other desirable cryptographic characteristics of AES S-box are acquired [11]. Another new variation of AES cipher by based on the concepts of the original cipher was proposed in 2008, in fact, it is very similar to Rijndael. The major difference is that the Rijndael algorithm starts with 128-bits block size, and performs encryption along the block column by column, while the proposed algorithm starts with 200-bit instead. Hence, each word in the state array consists of 5-Bytes (40-bits) instead of 4-Bytes (32-bits). Consequently, the proposed algorithm provides enhanced security but reduced efficiency compared to the original one [12]. Accordingly, the main purpose of this study is to develop the key of Rijedael cipher in order to enhance the level of confusion and diffusion.

3. METHODOLOGY:

In this study, the model of SDLC has been adopted to encompass and execute the research tools, analysis, design, implementation, testing, and evaluation as shown in figure (1). Firstly, the analysis tool has been used to analyze the Rijndeal key structure and to determine the need to develop the multi key encryption. Secondly, the tool of design has been implemented to develop the Rijndael key through improving its algorithm and programming it by the use of language Visual C#. Finally , the implementation research instrument included the test of Rijndeal M as well as evaluating the Rijndeal M by comparing it to the standard Rijndeal key.

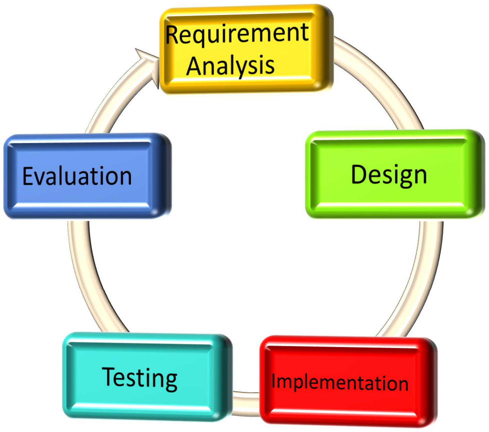
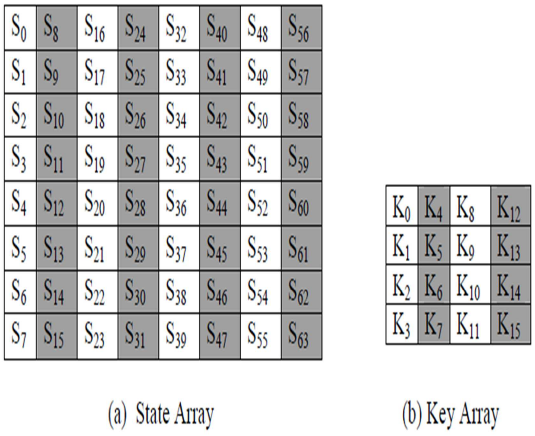


Figure (1) Methodology Framework

4. STRUCTURE AND IMPLEMNTATION OF RIJNDAEL-M

The plaintext block for input is 512-bits, which is represented as a matrix with a dimension of 8 x 8 while the key is represented by a matrix with a dimension of 4 x 4 and comes with 128-bits, as shown in the table below. In the case of message encryption using Rijndael-M, the original plaintext is divided into blocks of 512- bits.



S_0	S_8	S_{16}	S_{24}	S_{32}	S_{40}	S_{48}	S_{56}
S_1	S_9	S_{17}	S_{25}	S_{33}	S_{41}	S_{49}	S_{57}
S_2	S_{10}	S_{18}	S_{26}	S_{34}	S_{42}	S_{50}	S_{58}
S_3	S_{11}	S_{19}	S_{27}	S_{35}	S_{43}	S_{51}	S_{59}
S_4	S_{12}	S_{20}	S_{28}	S_{36}	S_{44}	S_{52}	S_{60}
S_5	S_{13}	S_{21}	S_{29}	S_{37}	S_{45}	S_{53}	S_{61}
S_6	S_{14}	S_{22}	S_{30}	S_{38}	S_{46}	S_{54}	S_{62}
S_7	S_{15}	S_{23}	S_{31}	S_{39}	S_{47}	S_{55}	S_{63}

(a) State Array

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

(b) Key Array

Table (1) key of RIJNDAEL-M

It should be noted that only a single plaintext block is encrypted into cipher text at a time with Rijndael-M. This process is iterated until all of the plaintext blocks are encrypted. Although the XOR process in this algorithm may seem incompatible, it actually offers an efficient technique for the expansion key which reduces the burden of introducing a large volume of key bits.

4.1 Sub Byte Operation

The SubByte operation used in Rijndael-M is very similar to the one used in (AES) which basically utilizes the same S-box adopted in the (Rijndael), since it provides a good confusion factor, high linearity, in addition to high resistance against known attacks. It is worth mentioning that to this moment, no real attacks have been registered.

4.2 Shiftrows Transformation Matrix

In this ShiftRows operation, some modifications are introduced where each state row is operated on individually by cyclically shifting each byte in the row. It should be noted that the operation depends on the row index r and the state size Nb where shift (r,Nb) = r mod Nb which basically moves the bytes to lower positions in each row. On the other hand, the lowest bytes are wrapped around into the top of the row. One must keep in mind that the shift values are selected based on the diffusion criteria under consideration. To enhance cipher strength, the bytes in each column of the state are diffused to as many columns as possible, where each column of the state will contain different bytes from as many columns as possible after this transformation is performed.

4.3 Mixcolumns Operation

The mixcolumns operation acts on the state column by column where each column of the state is treated as an eight-term polynomial s(x) with coefficients in GF(28) and a multiplied modulo x8 + 1 with a static polynomial a(x). The criteria for selecting the coefficients of mixcolumns is described below:

s’(x) = a(x) ⊕ s(x)

Where

a (x) ={01} x7 + {01} x6 + {02} x5 + {02} x4 +{01} x3 + {01} x2 + {03} x + {02}…(4.9)

The main difference from the original algorithm is the criteria used in selecting the coefficients for the mixcolumns transformation of the extended model of the Rijndael-M block cipher. The size of the matrix is 8 x 8 is also different compared to that of the Rijndael block cipher which requires the use of 8th degree equation. Moreover, the space available for the selection of mixcolumns transformation is much more improved than that of the original (AES). Other important criteria for selecting the coefficients for mixcolumns are listed below:

1. Relevance to diffusion power
2. Linearity in GF (2).
3. Inevitability.
4. All coefficients and their Inverse must be selected in preference of 1, 2, 3, 4, 5… while their summation should be minimized.

It should be noted that no solutions can be found to satisfy the above mentioned criteria in the original Rijndael cipher. The last criterion is not satisfied in AES although its designers have come up with the best solution. On the other hand, the mixcolumns transformation in Rijndael-M has been chosen from the space of 8-byte to 8-byte linear transformations instead of 4-byte to 4-byte which gives rise to an enlarged space by which many choices become available to find an optimal solution. Generally, solutions are found in a dot Net environment using visual C# program, Using 2.2 GHz CPU CORE I5 running Microsoft Windows 7 Ultimate, the solutions for satisfying the above mentioned criteria typically takes several weeks. It is worth mentioning that other suitable solutions can be found in different implementations, which makes the Rijndael-M more flexible, secure and appropriate. It also takes approximately the same time to implement the inverse cipher in as the original cipher. It is also worth noting that the inverse cipher is about 30% slower than the original Rijndael block cipher.

As an optimal solution for the given coefficients, two 8th order equations are proposed in polynomial format with their inverses in the Rijndael-M. The first equation is deployed in the Rijndael-M, The resulting polynomial is shown below:

$a = a x + a x + a x + a x + a x + a x + a x + a x$ …(1)

$7\ b = b x + b x + b x + b x + b x + b x + b x + b x$ …(2)

c(x) = a(x) · b(x)

is extended algebraically, and similar powers are collected to give :

c(x) = c14x14 + c13x13 + c12x12 + c11x11 + c10x10 + c9x9 + c8x8 + c7x7 x6 + c5x5 + c4x4 + c3x3 + c2x2 + c1x + c0 …(3) Where,

c0 = a0 · b0

c1 = a1 · b0 ⊕ a0 · b1

c2 = a2 · b0 ⊕ a1 · b1 ⊕ a0 · b2

c3 = a3 · b0 ⊕ a2 · b1 ⊕ a1 · b2 ⊕ a0 · b3

c4 = a4 · b0 ⊕ a3 · b1 ⊕ a2 · b2 ⊕ a1 · b3 ⊕ a0 · b4

c5 = a5 · b0 ⊕ a4 · b1 ⊕ a3 · b2 ⊕ a2 · b3 ⊕ a1 · b4 ⊕ a0 · b5

$$\begin{bmatrix} \mathrm{d}_0 \\ \mathrm{d}_1 \\ \mathrm{d}_2 \\ \mathrm{d}_3 \\ \mathrm{d}_4 \\ \mathrm{d}_5 \\ \mathrm{d}_6 \\ \mathrm{d}_7 \end{bmatrix} = \begin{bmatrix} a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 & a_3 \\ a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 & a_4 \\ a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 & a_5 \\ a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 & a_6 \\ a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 & a_7 \\ a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_0 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix}$$

$$\begin{bmatrix} \mathrm{d}_0 \\ \mathrm{d}_1 \\ \mathrm{d}_2 \\ \mathrm{d}_3 \\ \mathrm{d}_4 \\ \mathrm{d}_5 \\ \mathrm{d}_6 \\ \mathrm{d}_7 \end{bmatrix} = \begin{bmatrix} 2 & 1 & 1 & 2 & 2 & 1 & 1 & 3 \\ 3 & 2 & 1 & 1 & 2 & 2 & 1 & 1 \\ 1 & 3 & 2 & 1 & 1 & 2 & 2 & 1 \\ 1 & 1 & 3 & 2 & 1 & 1 & 2 & 2 \\ 2 & 1 & 1 & 3 & 2 & 1 & 1 & 2 \\ 2 & 2 & 1 & 1 & 3 & 2 & 1 & 1 \\ 1 & 2 & 2 & 1 & 1 & 3 & 2 & 1 \\ 1 & 1 & 2 & 2 & 1 & 1 & 3 & 2 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 1 \\ 2 \\ 2 \\ 1 \\ 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$c6 = a6 \cdot b0 \oplus a5 \cdot b1 \oplus a4 \cdot b2 \oplus a3 \cdot b3 \oplus a4 \cdot b2 \oplus a5 \cdot b1 \oplus a6 \cdot b0$
$c7 = a7 \cdot b0 \oplus a6 \cdot b1 \oplus a5 \cdot b2 \oplus a4 \cdot b3 \oplus a3 \cdot b4 \oplus a2 \cdot b5 \oplus a1 \cdot b6 \oplus a0 \cdot b7$
$c8 = a7 \cdot b1 \oplus a6 \cdot b2 \oplus a5 \cdot b3 \oplus a4 \cdot b4 \oplus a3 \cdot b5 \oplus a2 \cdot b6 \oplus a1 \cdot b7$
$c9 = a7 \cdot b2 \oplus a6 \cdot b3 \oplus a5 \cdot b4 \oplus a4 \cdot b5 \oplus a3 \cdot b6 \oplus a2 \cdot b7$
$c10 = a7 \cdot b3 \oplus a6 \cdot b4 \oplus a5 \cdot b5 \oplus a4 \cdot b6 \oplus a3 \cdot b7$
$c11 = a7 \cdot b4 \oplus a6 \cdot b5 \oplus a5 \cdot b6 \oplus a4 \cdot b7$
$c12 = a7 \cdot b5 \oplus a6 \cdot b6 \oplus a5 \cdot b7$
$c13 = a7 \cdot b6 \oplus a6 \cdot b7$
$c14 = a7 \cdot b7$

$d(x) = c(x) \bmod (x^{8}+1)$ that is, $d(x)$ must satisfy the equation below:
$c(x) = [(x^8+ 1) * q(x)]\ d(x)$ such that the degree of $d(x)$ is 7 or less.

An efficient and practical technique for performing multiplication along this polynomial ring is based on the $X^{i} \bmod (x^8 +1) = x^{i \bmod 8}$.

$d(x) = c(x)$ mod $(x^8 +1)$ $= [c14x^{14} + c13x^{13} + c12x^{12} + c11x^{11} + c10x^{10} + c9x^9 + c8x^8 + c7x^7 + c6x^6 + c5x^5 + c4x^4 + c3x^3 + c2x^2 + c1x + c0]$ **mod** $(x^8 +1) = c7x^7+ (c6 \oplus c14)\ x^6 + (c5 \oplus c13)\ x^5 + (c4 \oplus c12)\ x^4 + (c3 \oplus c11)\ x^3 + (c2 \oplus c10)\ x^2 + (c1 \oplus c9)\ x^1 + (c0 \oplus c8)$

Expanding the ci coefficient provides the d(x) coefficient:

$d0 = a0 \cdot b0 \oplus a7 \cdot b1 \oplus a6 \cdot b2 \oplus a5 \cdot b3 \oplus a4 \cdot b4 \oplus a3 \cdot b5 \oplus a2 \cdot b6 \oplus a1 \cdot b7$
$d1 = a1 \cdot b0 \oplus a0 \cdot b1 \oplus a7 \cdot b2 \oplus a6 \cdot b3 \oplus a5 \cdot b4 \oplus a4 \cdot b5 \oplus a3 \cdot b6 \oplus a2 \cdot b7$
$d2 = a2 \cdot b0 \oplus a1 \cdot b1 \oplus a0 \cdot b2 \oplus a7 \cdot b3 \oplus a6 \cdot b4 \oplus a5 \cdot b5 \oplus a4 \cdot b6 \oplus a3 \cdot b7$
$d3 = a3 \cdot b0 \oplus a2 \cdot b1 \oplus a1 \cdot b2 \oplus a0 \cdot b3 \oplus a7 \cdot b4 \oplus a6 \cdot b5 \oplus a5 \cdot b6 \oplus a4 \cdot b7$
$d4 = a4 \cdot b0 \oplus a3 \cdot b1 \oplus a2 \cdot b2 \oplus a1 \cdot b4 \oplus a0 \cdot b4 \oplus a7 \cdot b5 \oplus a6 \cdot b6 \oplus a5 \cdot b7$
$d5 = a5 \cdot b0 \oplus a4 \cdot b1 \oplus a3 \cdot b2 \oplus a2 \cdot b3 \oplus a1 \cdot b4 \oplus a0 \cdot b5 \oplus a7 \cdot b6 \oplus a6 \cdot b7$
$d6 = a6 \cdot b0 \oplus a5 \cdot b1 \oplus a4 \cdot b2 \oplus a3 \cdot b3 \oplus a4 \cdot b2 \oplus a5 \cdot b1 \oplus a6 \cdot b0 \oplus a7 \cdot b7$
$d7 = a7 \cdot b0 \oplus a6 \cdot b1 \oplus a5 \cdot b2 \oplus a4 \cdot b3 \oplus a3 \cdot b4 \oplus a2 \cdot b5 \oplus a1 \cdot b6 \oplus a0 \cdot b7$

4.4 Key Schedule

The key schedule of Rijndael-M algorithm is based on two techniques:

1) Key Expansion technique which is based on two steps. The first step is initiated after taking the input key with a length of 128-bit which operates by (g) function for the input key array, whereas the second step, which is very similar to the RC6 cipher's key expansion, is started afterwards. The first round uses two constant words that consists of the base natural algorithm and golden ratio, and then implements the same steps that compensates RC6 key's expansion to reach the key length of 512-bits. This process is described in the diagram below:

2) Secure Hash Algorithm (SHA-512): The second technique the key schedule algorithm performs is responsible for the remaining rounds of the key expansions. Once the first technique runs and expands the key in the first round by converting from 128-bits to the 512-bits, the output of first round will act as the input to the second round through hash function (SHA-512). Finally, the output of the second round will be the input to the third. This process is iterated until the last round is implemented as shown in the figure below:

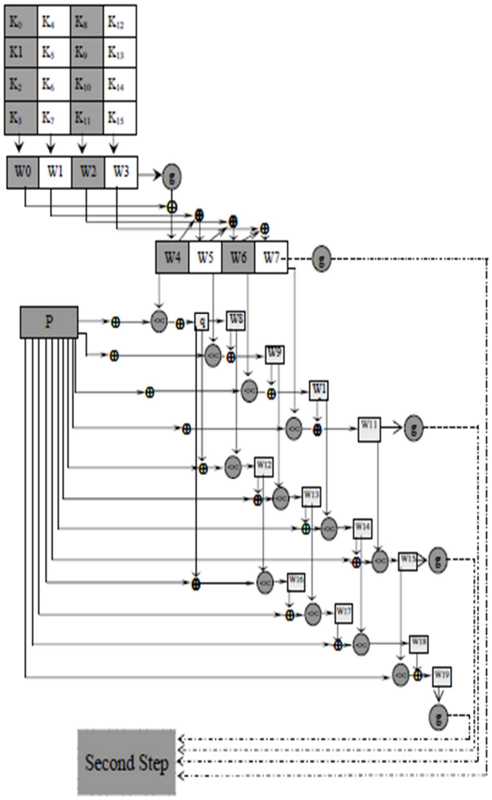


Figure (2) Key Process

4.5 Hash Function

Hash function is one of the most important cryptographic basics and it is applied in a wide spectrum of applications such as: digital signatures and commitment schemes. A hash function is a transformation that is implemented by mapping a variable-length input to a fixed-size output, which often called: message digest. It is worth noting that some improvement in the differential cryptanalysis framework for finding collisions is introduced in hash functions. The main principle of such function is based on compression linearization which is essential in finding low weight differential characteristics. When attacks are taken into account, they can be operated on utilizing the first technique in the key expansion by combining the key with two constant words represented by base natural algorithm, golden ratio, and nearly the same steps involved in RC6 key expansion.

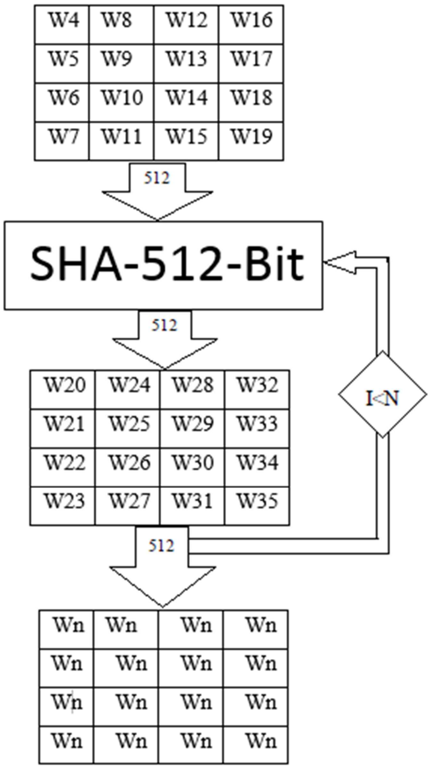


Figure (3) Hash Function

4.6 Inverse Cipher

The inverse cipher is virtually the same as in the original algorithm except for some minor modifications. One of the major changes made in this model is the implementation of inverse mixcolumns transformation. In this transformation, each column of the state is treated as an 8th order polynomial s(x) over GF(28), and then multiplied by modulo x8 +1 with the a static polynomial b(x): $S(x) = b(x) \oplus s(x)$ Where $b(x) = \{03\}\ x7 + \{02\}\ x6 + \{01\}\ x5 + \{01\}\ x4 + \{02\}\ x3 + \{02\}\ x2 + \{01\}\ x + \{01\}$...(4.13)

Each coefficient in this polynomial is upper bounded by 03, and its inverse matrix is non-zero.

5. CONCLUSION

An enormous number of organizations using the technology are suffering from several security problems in cipher system[14]. Consequently, Organizations need to develop the multi-key cipher algorithm in order to manage the encryption based on the level of security[14]. Thus, this study adds an important contribution of Rijndael-M algorithm through four phases. Firstly, it is an extremely secure cipher. Secondly the key size is 25% the size of the state array (block size) which promotes simplicity in the generating and exchanging processes of the key. Thirdly, it represents a hybrid cipher since it utilizes some characteristics from RC6, and the original Rijndael by using the hash function in the key expansion. Finally, the block size of Rijndael-M encryption is four times larger than the size of the original Rijndael. Hence, the process of expanding the key leads to more flexibility and security in Rijndael algorithm. Besides, it will increase the range of its usage among the organizations.

REFERENCES

[1]http://searchsecurity.techtarget.com/definition/Rijndael

[2] Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael". National Institute of Standards and Technology. p. 1. Retrieved 21 February 2013

[3]"Announcing the ADVANCED ENCRYPTION STANDARD (AES)". *Federal Information Processing Standards Publication 197*. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.

[4] John Schwartz (October 3, 2000). "U.S. Selects a New Encryption Technique". *New York Times*.

[5] Westlund, Harold B. (2002). "NIST reports measurable success of Advanced Encryption

Standard". *Journal of Research of the National Institute of Standards and Technology*.

[6] Bruce Schneier; John Kelsey; Doug Whiting; David Wagner; Chris Hall; Niels Ferguson; Tadayoshi Kohno et al. (May 2000). "The Twofish Team's Final Comments on AES Selection"

[7] Duong Anh Duc, Tran Minh Triet and Luong Han Co, "The Extended Rijndael-like Block Ciphers", Faculty of Information Technology University of Natural Sciences, VNU-HCMC Vietnam, Proceedings of the International Conference on Information Technology: Coding and Computing, 2002.

[8] Cliford Bergman, "A Description of Baby Rijndael", February, 2003. [9] Naim Aljouni, Asim El-Shiekh and Abdullah Abd ali Rashed, "A New Approach in Key Generation and Expansion in Rijndael Algorithm", The International Arab Journal of Information Technology, January 2004.

[10] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, November 16, 2005.

[11] Lingguo Cui, "A NEW S-BOX STRUCTURE NAMED AFFINE- POWERAFFINE", International Journal of Innovative Computing, Information and Control, Volume 3, Number 3, June 2007.

[12] Md. Nazrul Islam and his colleagues, "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

[13] John Schwartz (October 3, 2000). "U.S. Selects a New Encryption Technique". New York Times.

[14] Mohanaad T Shakir , Asmidar Bte Abu Bakar, and Yunus Bin Yusoff," Diagnosis Security Problems for Hybrid Cloud Computing in Medium Organizations", NIST 2016 National Conference on Information Systems Trends(Theme:Cloud Computing, 11th Feb 2016),Oman