QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

An Analytical Study for Some Drawbacks and Weakness Points of the AES Cipher (Rijndael Algorithm)

Omar A. Dawood
Computer Science, College of Computer, University of Anbar - Iraq
The_lionofclub@yahoo.com
Othman I. Hammadi
Computer Science, College of Computer, University of Anbar - Iraq
othmanibraheem@yahoo.com.

ARTICLE INFO

Article History:

Received: 19 March 2017

Accepted: 1 April 2017

Published: 10 April 2017

DOI:

10.25212/lfu.qzj.2.2.13

Keywords: *Rijndael cipher, MARS, Serpent, Twofish, RC6, DES, AES, Block Cipher, Symmetric Cipher.*

ABSTRACT

The present paper includes a research study about the weak points and the major weakness aspects of the Rijndael cipher from the point of view design. Although several published papers for most researchers around the world included either the developing models or improving techniques by depending on Rijndael cipher. In this study, opposite matter about some scientific criticism for certain essential points in the AES construction will be discussed. When the AES was selected 16 years ago, the digital technologies were quite different from now and the magnitude of the challenges was less, so with the recent advanced technology and the emergence of new applications like Big data's applications in addition to the applications have run with 64-bit and a lot of other applications, it has become a necessity for designing a new contemporary algorithm for the current demands. Especially young Rijndael that has faded and its sun had set as it has been believed by many researchers. Since the experts and designers of information security in previous time determined its retired date for ten years. In this study, a list of drawbacks and vulnerabilities for the Rijndael internal structure in addition to new recommendations for the future work will be diagnosed. No one denies that the selection of Rijndael was a good choice for civil applications on software and hardware implementations and on many of various platforms, but the excessive speed for the IT progress leads to take in to account recalculation of the security level for the current and perspective future requirements.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

1. INTRODUCTION

In 1997, the National Institute of Standard and Technology (NIST) unit of the US commerce department announced an open competition, and invited the cryptography and the data security specialists from around the world to participate in the conference to select a replacement for the old standard cipher algorithm (DES) and Triple-DES, because, during the last years DES has become obsolete for its too short key and block sizes, notwithstanding the current advances in computing technology [1]. The new encryption standard should support block lengths of 128-bits and key lengths of 128-bit, 192-bit and 256-bits. This demand determined by the NIST. In this conference applied twenty-one candidate's algorithms, the specification of these algorithms varies widely in structure and form and their coverage of implementation some of these candidate using formal mathematical style and other depending on combinations text diagrams and pseudo code. The first round of conferences held in California in 1998 and fifteen algorithms have been submitted. The initial evolution criteria determined by three elementary categories security, cost and algorithm and implementation characteristics. The large majority of the candidates' algorithms satisfy the criteria determined by the NIST [2]. In March 1999 the second AES conference was held in Rome, Italy submitted the final evolution criteria that include general security, ease of implementation on both software and hardware, implementation attacks and flexibility in encryption and decryption, ciphering key and other factors. Later fifteen algorithms were reduced to five algorithms [3].

2. THE SELECTION OF DES REPLACEMENT

There were several algorithms that were not accepted because either they did not satisfy the security requirements presented by NIST or because the weakness such as LOKI97, DAL, HPC and another some candidates algorithms had not been eliminated because of the security problems but for other reasons such as cost, slow and bad performance for example Cast-256, Crypton, DFC, E2 and SAFER+. Only five algorithms were accepted in this conference that were considered as the optimal algorithms and have a good specification with margin of security these algorithms include (MARS, RC6, Rijndael, Serpent, and Towfish) [4]. The origin of each candidate algorithm with submitters and countries can be shown in the following Table 1.

TABLE 1: The First of the AES Candidates Algorithms

Countries	Submitters	Algorithms
Canada	Entrust Technologies, Inc.	CAST-256
South Korea	Future Systems, Inc.	CRYPTON
Canada, Norway	Richard Outer bridge, Lars Knudsen	DEAL
France	CNRS - Centre National pour la Recherche Scientifique – Ecole Normale Supérieure	DFC

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

Japan	NTT – Nippon Telegraph and Telephone Corporation	E2
Costa Rica	Tec-Apro Internacional S.A.	FROG
U.S.A	Richard Schroeppel	HPC
Australia	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry	LOKI97
Germany	Deutsche Telekom AG	MAGENTA
U.S.A.	IBM	MARS
U.S.A.	RSA Laboratories	RC6
Belgium	Joan Daemen, Vincent Rijmen	Rijndael
U.S.A.	Cylink Corporation	SAFER+
U.K., Israel, Norway	Ross Anderson, Eli Biham, Lars Knudsen	Serpent
U.S.A.	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson	Twofish

The selection process was in accordance with a hundred points that were distributed according to seven criteria and these criteria gave the algorithms variations in access to capture points in these seven criteria [5]. As it shown in Table 2.

TABLE 2: The Main Criteria for the Selection of AES Cipher

The main Criteria determined by NIST	Distribution Points
Algorithm Design & Presentation	(10 points)
Security	(30 points)
Ease of implementation	(10 points)
Usage Flexibility	(10 points)
Performance/ Computational Efficiency	(10 points)
Performance/Adaptability on Smart cards	(10 points)
Demonstrated/Expected strength against Cryptanalysis	(10 points)
Future Resilience	(10 points)

3. SPEED OVERVIEW ON THE FIVE FINALISTS CANDIDATES

There is no doubt about the AES candidate algorithms have been designed by the world's best academic cryptographers. The majority of these candidates are highly regarded for their security and there seems little doubt that when the finalists are selected. In the second and

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

the first round of conferences all of them were be very high quality and performance. But the last five AES finalists (MARS, RC6, Rijndael, Serpent, and Twoftsh) were believed to be secure, and none was clearly superior in all aspects. So the choice of Rijndael was based on its balance of flexibility, ease of implementation and speed in both hardware and software [6]. The stats for the number of votes obtained by each algorithm during the voting process in the conference. Rijndael obtained on 86 votes, Serpent 59 votes, Towfish 31 votes, RC6 23 votes and MARS 13 votes. In October 2000 NIST announced that the Rijndael algorithm selected as a winner because it took most of the votes. All the five finalist algorithms were not built from scratch since all of these algorithms were based on the predecessors algorithms. Originally these finalists block ciphers similar in their structure and internal work to their predecessors. Each of these ciphers inherited properties from them and enriched with new ideas to be more resistance structure for facing all the known attacks. Each of these competitions ciphers deduced good ideas and strong points from their predecessors and addressed the weakness points. Like MARS, Twofish and RC6 that are dependent on DES cipher [7]

3.1. ADVANCE ENCRYPTION STANDARD (MARS CIPHER)

One of the five finalist block cipher chosen as AES, IBM s' algorithm uses innovative techniques including multiplication data-dependent rotation. One of the components of the cipher is 9*32-bits of S-box. MARS is a 128 bit-block cipher and a variable key size ranging from 128-bit to 444-bit. As most symmetric-key block ciphers MARS is based on a ‘‘Feistel” network structure and a “round function”. This function provides the basis for the encryption mechanism and combines several linear and non-linear operations [8]. MARS operates on 32-bits microprocessor and run slowly. MARS designed to be more secure than triple–DES and to be used in computers today but it has been observed that it is more complicated overall the AES candidates. The main strength of MARS is its robustness. This was the main design goal but MARS contains more “fail stop” mechanisms than any of the other finalists. Due to the heterogeneous structure and the large variety of “strong operations” in MARS. Because the fail-stop mechanisms in MARS makes its hardware implementation more involved than the other finalists [9].

3.2. ADVANCE ENCRYPTION STANDARD (SERPENT CIPHER)

Serpent cipher Created by R.Anderson and E.Biham, two of the leading experts in cryptanalysis, which can be viewed as an indication to its strength. It is one of the AES candidates and it has been implemented on 8-bit, 16-bit, and 32-bit platform like other AES submissions. Serpent is a (SPN) that uses 32-rounds. The algorithm has two different modes of implementation: standard and bitslice mode. The standard mode operates on individual bits or groups of four bits, while the bitslice mode improves software efficiency by operating on entire 32-bit words [10]. Serpent has a block size of 128-bits and support a key size 128-bits, 192-bits, and 256-bits. The main operations on a block are implemented by four word (32-bits). The S-box of Serpent appears to have a high security margin. Serpent uses the set of different S-boxes with four bits inputs and four bits outputs. In each round there is used one of S-box working in parallel 32 times. After the first eight rounds, all S-boxes are used and this unit of eight rounds is repeated four times. The main selling point of Serpent is its very conservative number of rounds. Serpent does not have “fail-stop” mechanisms as in MARS [11].

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

3.3. ADVANCE ENCRYPTION STANDARD (TWOFISH CIPHER)

Symmetric key block cipher proposed by Counterpane. The Twofish block cipher employs a 16-round feistel network with additional whitening of the input and output. The 128-bit plaintext block is split into four 32-bit words. In the input whitening step each 32-bit word is XORed with a different 32-bit input whitening key. Towfish work with 128-block size and accept a variable length key up to 256-bit sufficient on a various platforms, with objective function work on 32-bits word with four key dependent 8*8 S-box followed by 4*4 maximum distance separable matrix over GF(2^8) a pseudo hadamard transform and key addition [12]. Twofish cipher was designed for flexibility, and indeed it offers a wide variety of implementation tradeoffs. It is also a very fast cipher. However, the same design for flexibility also resulted in a cipher which is very hard to analyze. The designers used many "tricks" to obtain flexibility which security implications are not clear. Towfish has the efficiency and speed on both software and hardware implementable on a wide variety of platform and applications and suitable for stream cipher, hash function, and MAC [13].

3.4. ADVANCE ENCRYPTION STANDARD (RC6 CIPHER)

RC6 is very simple algorithm and the easiest of the AES candidates to implement developed by Ron Rivest in collaboration with associates from RSA laboratories. It is based on carefully crafted ciphers such as RC2, RC4, and RC5 exactly it is strengthened version of RC5 which was proposed in 1995. The RC6 cipher works with 20-rounds feistel structure with objective function work on 32-bit modular multiplication, addition, and XOR with addition key [14]. The main advantage of RC6 is its simplicity and speed which may serve as an indication of the suitability of the current design as well. The main argument against RC6 is "single point of failure" for the design method. There are also lingering concerns regarding the number of rounds used in RC6. The main difference between the RC6 and its predecessor RC5 is the RC6 algorithm depends mainly on the usage of four working registers each with size of 32-bits, this means it handles 128-bits input/output blocks in contrast to the RC5 cipher which works in two registers of 64-bits [15].

3.5. ADVANCE ENCRYPTION STANDARD (RIJNDAEL CIPHER)

The Rijndael cipher is the winner algorithm in the NIST competition designed by Joan Daemen and Vincent Rijmen from Belgium and recently selected as the official (AES). It is well suited for work across all platforms and involve clean mathematical structure and seem as a unique among the candidates ciphers. It is an iterated block cipher that has a very simple structure and easily implemented in both hardware and software. Rijndael operates with block size 128-bits and with variable key length of 128-bits, 192-bits and 256-bits. It is a fast and flexible cipher. Rijndael is somewhat similar to SQUARE cipher and the lessons from SQUARE are incorporated in its design [16].

4. ANALYSIS AND JUSTIFICATIONS FOR THE DRAWBACKS OF THE RIJNDAEL CIPHER

After deep study and an intensive analysis of the internal structure and the algebraic foundation of the AES cipher, there is evidence that the AES algorithm has many suspicious aspects and it has suffered from several vulnerabilities from the design term that brings the attention and can be listed as follows:

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

1- Most of the developing methods of the previous studies for most researchers and specialists deal with the AES improvement and exactly focus on increasing the number of rounds or increasing the block size in order to increase the security level and this clue does not consider the best solution for the development experiments.
2- Most of the AES algorithms (MARS, Serpent, RC6, Twofish, and Rijndael) designed to work with platforms of 32-bits and could not work with 64-bit and this is considered a negative factor in some operating system of 64-bit from the designing perspective as it was mentioned in the personal blog of Bruce Schneier.
3- The three keys of changeable length (128-bit, 192-bit, and 256-bit) of the AES cipher have not real length except the first one with a length of (128-bit) and the two others are unreal as it claimed in the most references. Since the XORing operation between the key and state matrix is not fit to the same size or in another word it only increased the probability of the search space for the key generation to the rest rounds.
4- The R-Con table with fixed values calculated according to specific formula can be considered as an awkward point in the designing map for the key F-function especially for the key generation that should depend on a complicated one-way technique or intractable methods.
5- The decryption process with AES structure is slower than the encryption process especially in the embedded devices and this feature refers to the unbalancing structure in encryption and decryption process for some devices.
6- The encryption process for thousands of bits will give an obvious difference time between the encryption and decryption process due to the accumulator for repetition of thousand rounds, so the difference will be a clearly evident.
7- The AES cipher work with 128-bit of plaintext or 16-byte and all internal operations rely on the byte-oriented implementation that means the maximum value can be implemented in Hexa-decimal is (FF).

$$FF\ (byte) * FF\ (byte) \bmod M = (FF)\ Byte$$

So the multiplying byte by byte also will give byte as a final result.
8- The selection only one algorithm (Rijndael) and discarding the other four best algorithms (MARS, RC6, Twofish, and Serpent) according to the essay that was mentioned in NIST report (do not put all eggs in the one basket) is an unsatisfactory reason. Since there is a possibility to combine all the candidates algorithms in one package of software and give more options and flexibility for selecting an appropriate algorithm according to the application nature.
9- Several modern attacks have proven their effectiveness from a theoretical perspective like the algebraic attacks, implementation attack and side channel attacks.
10- The AES cipher's life time is dedicated for ten years to face the advance of technology progress at that time. So many researchers think that finding an alternative model becomes a vital issue according to the requirements of the last decade. So the current state may need more options from all aspects
11- AES cipher with secure of 128-bit may not be appropriate for the big data applications and others modern big applications like secure cloud storage. Therefore; these applications with huge data may need a larger algorithm with a larger order of mathematical and structure foundations with tradeoff speed.
12- The Rijndael cipher got the higher voting in the NIST competition but this does not means it is the best from all factors since some algorithms exceed the Rijndael from certain aspects but the accumulated scores were from the Rijndael share.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

13- The X-time function designed to work with (02) recursive multiplications clue for a number of times according to the coefficient values instead of the tradition mathematical multiplication operations that have taken modular on the irreducible polynomial equation of degree eight.
14- The last round without mixcolumn has no effective role in the security factor as it was mentioned by the authors of the Rijndael. So it can be added or discarded.
15- The fixed S-Box with two tables of 256-values in hexa-notation may form a good objective for the cryptanalysts' attacks, since each value has a mapping to the corresponding value with inverse picture.

5. RECOMMENDATIONS

After this contrastive study, there are several important recommendations for future work that can be summarized here:

1. Design a dynamic algorithm with the changeable stage for all linear and non-linear layers.
2. Develop a new model with a higher mathematical order of finite field or Galois Field (GF) and with higher irreducible polynomial to increase the security level and the complexity.
3. Improve the AES cipher to work with the system of 64-bits and eliminate any numerical constants that can be exploited by the attackers.
4. Made the improved algorithm more balanced in encryption and decryption process with embedded devices and restricted hardware devices.
5. Develop new techniques for the key generation that generated key with real length specifically for the long keys that comprises 192-bit, 256-bit and upper than that increase the guessing probabilities effectively.

6. CONCLUSIONS

The current research presented a simple literature review and an analytical study for the AES selection and the main standard criteria for the design principles. The basic target of this study is to highlight weaknesses and vulnerabilities in addition to explain the gaps of the design elements that possible to be exploited in the AES structure. This paper discussed the Rijndael features on the one hand construction's fails stop and what are the best alternatives by given a set of fundamental factors diagnostic for the negative aspects from the point of view author and the scientific researchers' articles around the world. The introduced research also includes some future recommendations for the designers and academic specialists in addition to the essence solutions for developing a modern algorithm.

7. REFERENCES

[1] A. M. Sagheer, S. S. Al-Rawi, and O. A. Dawood, "Proposing of Developed Advanced in Encryption Standard AES", IEEE Computer Society DOI 10.1109/DESE, Page No. 197, 2011, The Fourth International Conference in Developments in E System Engineering DESE, Dubai, 2011.
[2] J. Daemen and V. Rijmen, "The design of Rijndael: AES the advanced encryption standard", Springer-Verlag, 2002.

QALAAI ZANIST JOURNAL
A Scientific Quarterly Refereed Journal Issued by Lebanese French University – Erbil – Kurdistan – Iraq
Vol. (2), No. (2), April 2017
Speical Issue : The 1st International Conference on Information Technology (ICoIT'17)
ISSN 2518-6566 (Online) - ISSN 2518-6558 (Print)

[3] Dr B. Gladman, "Implementation Experience with AES Candidate Algorithms", Second AES Conference, 28th February 1999.
[4] B. Gladman and Worcester, "The Need for Multiple AES Winners", United Kingdom, 7th April 1999.
[5] J. Dray, "Report on the NIST Java™ AES Candidate Algorithm Analysis",http://csrc.nist.gov/encryption/aes/round1/r1-java.pdf, November 8, 1999.
[6] O. A. Dawood, A. S. Rahma and A. J. Abdul Hossen, "The Euphrates Cipher", IJCSI International Journal of Computer Science Issues, Volume 12, Issue 2, March 2015, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.
[7] Federal Information Processing Standards Publication 197 "Announcing the ADVANCED ENCRYPTION STANDARD (AES)", November 26, 2001.
[8] IBM MARS Team, "MARS and the AES Selection Criteria", May 15, 2000.
[9] "A Request for Comments on Candidate Algorithms for the Advanced Encryption Standard (AES)", Federal Register, Volume 63, Number 177, September 14, 1998.
[10] T. Pornin, "Automatic software optimization of block ciphers using bitslicing techniques", Paris, France, 1999.
[11] E. Biham, RJ. Anderson, and LR Knudsen, \Serpent: A New Block Cipher Proposal", in Fast Software Encryption | FSE 98, Springer LNCS, vol 1372, pp 222.
[12] B. Schneier and his colleagues, "The Twofish Encryption Algorithm: A 128-Bit Block Cipher", John Wiley & Sons, 1999. www.counterpane.com/twofish-paper.html.
[13] A. J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA-Based Performance Evaluation of the AES Block Cipher Candidate Algorithm Finalists", IEEE Transactions On Very Large Scale Integration (VLSI) Systems, VOL. 9, NO. 4, AUGUST 2001
[14] R. L. Rivest1, M.J.B. Robshaw and Yiqun Lisa Yin, "The Security of the RC6™ Block Cipher", RSA Laboratories Version 1.0, August 20, 1998.
[15] M. Y. Rhee, "Internet Security Cryptographic Principles, Algorithms and Protocols", John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, England, 2003.
[16] O. A. Dawood, A. S. Rahma and A. J. Abdul Hossen, "The New Block Cipher Design (Tigris Cipher)", I.J.Computer Network and Information Security (IJCNIS).