ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
December 2013,
Vol. 6, No. (4):
Pgs. 473-479

Study and Analysis of Efficient AES multi-layer Key

MOHAMMED NAJM ABDULLAH[1], RULA SAMI KHUDHAIR[2] and MOHANED KADAM SABR[3]

[1-3]Computer Engineering, University of Technology, Baghdad, Iraq.
[2]Non-ferrous Materials Engineering Department, Faculty of Materials Engineering, University of Babylon Babylon, Iraq.

(Received: October 16, 2013; Accepted: November 01, 2013)

ABSTRACT

Multi-layer key for AES encryption technique are present in this paper. LFSR and MD5 as a primary key layer was used to increase the security of the key. Three types of tests for ten round for each key layer are tested and analyzed. From the tests the MD5 is present as more suitable for security but it more complexity while LFSR is good for both. The usage of them will be depending on the natural of applications.

Key word: AES Key. Multi-layer AES Key, LFSR, MD5.

INTRODUCTION

Exponential increases in communication on the internet tend to the millions of users generate and interchange large volumes of information in various fields each day, such as financial and legal files, medical reports, and bank services via Internet, telephone conversations, and e-commerce transactions. These and other examples of applications deserve a special treatment from the security point of view, not only in the transport of such information but also in its storage[1]. While, Different security and cryptographic mechanisms has been deployed but no system proven to be a perfect solution. Some solution may be considered secure but less efficient due to complex mechanism of encryption and decryption[2]. While, still the importance of cryptography applied to security in electronic data transactions has acquired the essential relevance during the last few years[1]. In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems[3]. Therefore, cryptography plays an important role in the security of data. It enables to store sensitive information or transmit it across insecure networks so that unauthorized persons cannot read it. Advanced Encryption Standard (AES) is the most common encryption algorithm widely used in applications such as wireless communication. The Advanced Encryption Standard (AES) is well known block-cipher algorithm which is easily portable and reasonable security[4].

AES Algorithm

The AES algorithm is a symmetric-key cipher(Rijndael Algorithm), in which both the sender and the receiver uses a single key for encryption and decryption. The length of the plain text is fixed to be 128 bits, while the key length can be either 128,192, or 256 bits. AES algorithm is an iterative algorithm, every iteration can be called a round, and the total number of rounds is 10, 12, or 14, according to the key length (128, 192, or 256 respectively). The 128 bit algorithm is divided into 16 bytes, these bytes are represented into 4x4 array called the state array, and all the different operations of the AES algorithm such as addroundkey, subbytes, shiftrows, mixcolumns and key expansion are performed on the state[4]. In general, the cipher algorithms have the two general categories: Private Key algorithms and public key algorithms. Private Key algorithms using single key to encrypt plain text and decrypt cipher text in sender and receiver side. Private Key algorithm samples are: DES (DES, 1977), 3DES and Advanced Encryption Standard Public Key algorithms, such as the Rivest-Shamir-Adleman (RSA), using two different key for encrypt plain text and decrypt cipher text in sender and receiver sides[3].

Cryptosystem KEY

Block cipher systems depend on the S-Boxes, which are fixed and no relation with a cipher key. From the analysis of any crypto system it is very clear the effect of the key and it can be considered as only changeable parameter. There are many key mechanism can be used for increasing the strength of AES algorithms.

Ordinary AES Key

In AES there are many Key round each round involves an addition or bitwise EXOR of the plaintext and the key, so the original key must be expanded into a number of Round Keys and this transformation is known as the Key Schedule. A Round Key consists of a Nc word sub-array from the Key Schedule. In general the length of the cipher input, the cipher output and the cipher state is also Nc, and is measured in multiples of 32 bits. Rijndael Algorithm allows Nc to take values 4, 6 or 8 but the AES standard only allows a length of 4. The length of the cipher key, Nk, again measured in multiples

Table 1: Average result for ten rounds of the different kinds (ordinary, LFSR, and MD5) of the key tests

	Frequency (Mono) bit test			Serial (two) bits test			Poker test			Period
	WOCH	W1BCH	W2BCH	WOCH	W1BCH	W2BCH	WOCH	W1BCH	W2BCH	
Ordinary Key	2.0199	2.0938	2.5767	-59.0244	-59.0244	-59.6626	40.4545	40.4545	38.1818	X
LFSR key	2.1676	2.2358	2.1023	-59.7073	-58.3440	-59.0532	36.5455	39.3636	40.3636	X * 25
MD5 key	0.7898	0.6392	0.1318	-59.9128	-60.5351	-59.5119	34.8182	35.3636	32.3636	X *Y

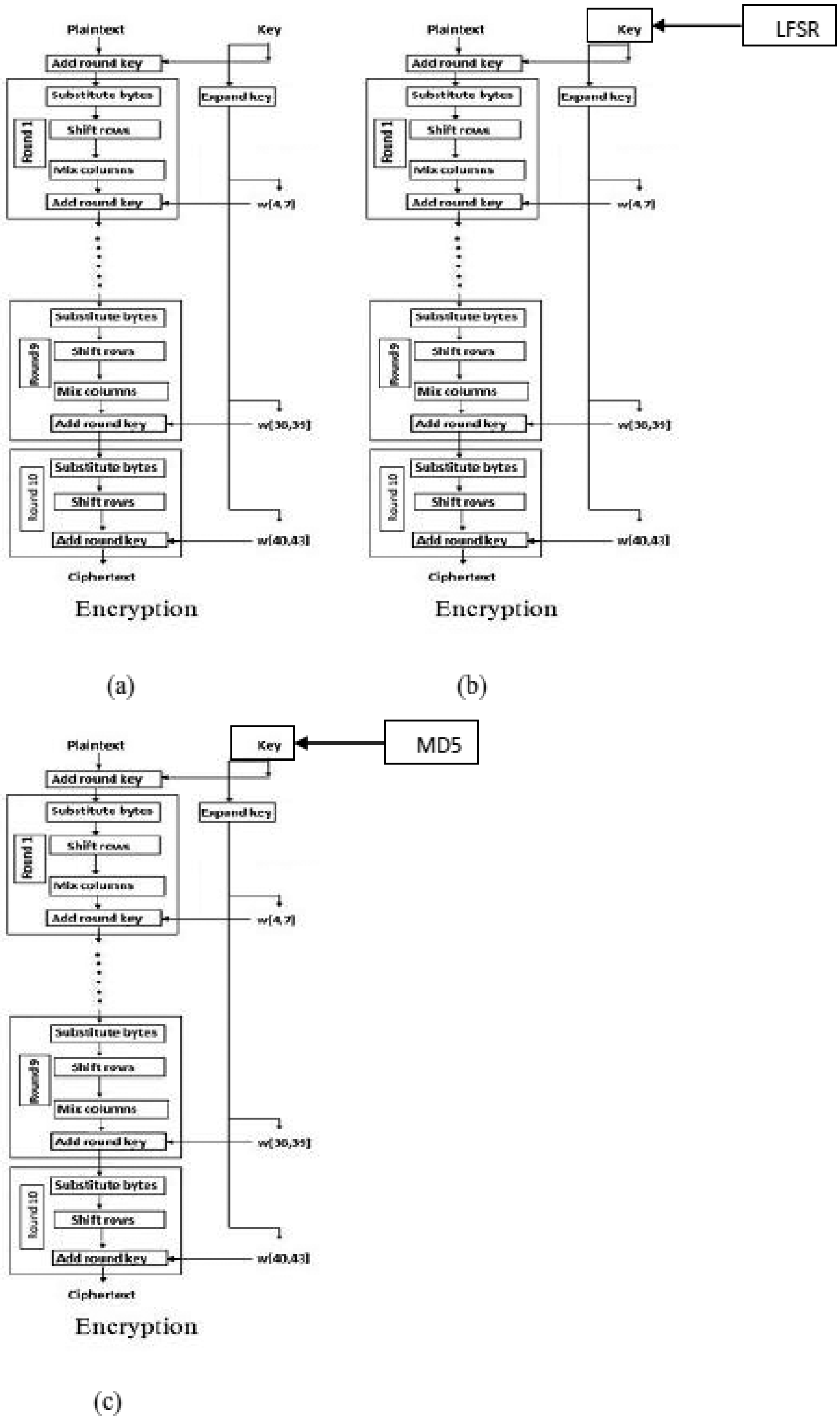

Fig. 1: Encryption process a) ordinary AES b) AES with LFSR additional Key layer c) AES with LFSR additional Key layer

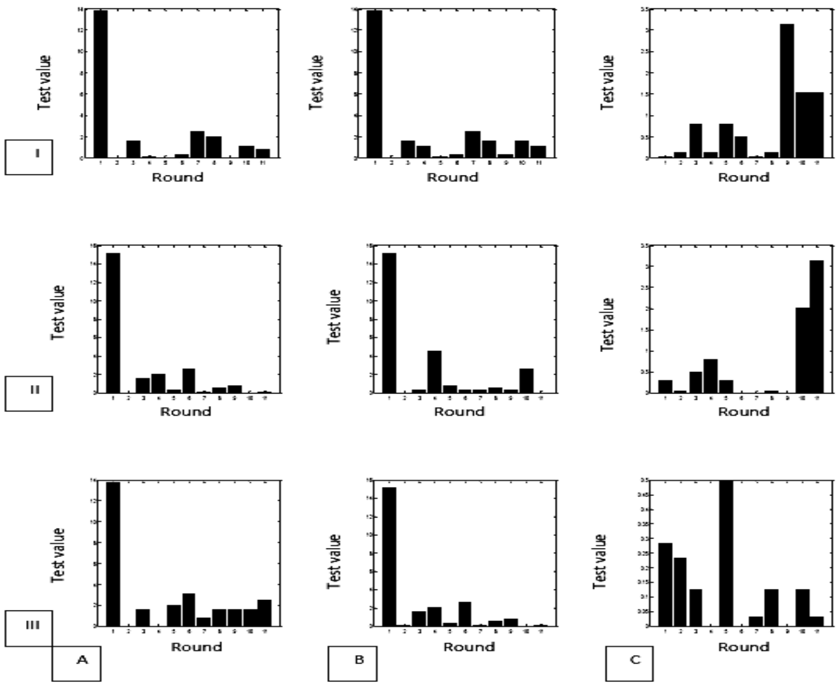

Fig. 2: Frequency (mono)-bit test for different Keys A) ordinary key B) ordinarywith LFSR C) ordinary with MD5 I)key without change II) Keys with change one bit III)keys with change two bits

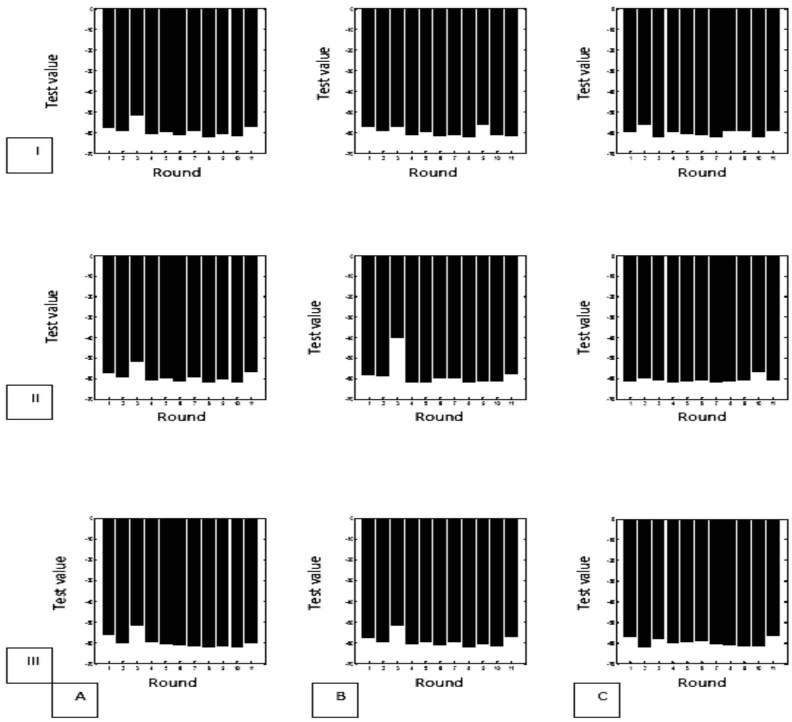

Fig. 3: Serial (two) bits test for different Keys A) ordinary key B) ordinary with LFSR C) ordinary with MD5 I)key without change II) Keys with change one bit III)keys with change two bits

of 32 bits, is also 4, 6 or 8, all of which are al-lowed by both Rijndael and the AES standard[5].

LFSR Key

Stream ciphers (especially LFSR based) are an important class of symmetric ciphers used widely in encryption for hardware-based cryptographic systems. They are simple, efficient without compromising performance. Key generation is the main problem during designing a stream cipher. It generates a key which is as long as the plain message[2]. Then the output of LFSR will be entered to the ordinary AES Key algorithm.

MD5 Key

Message digest (MD) algorithms, also called as Hash algorithms, which generate a unique message digest for an arbitrary message. Also,

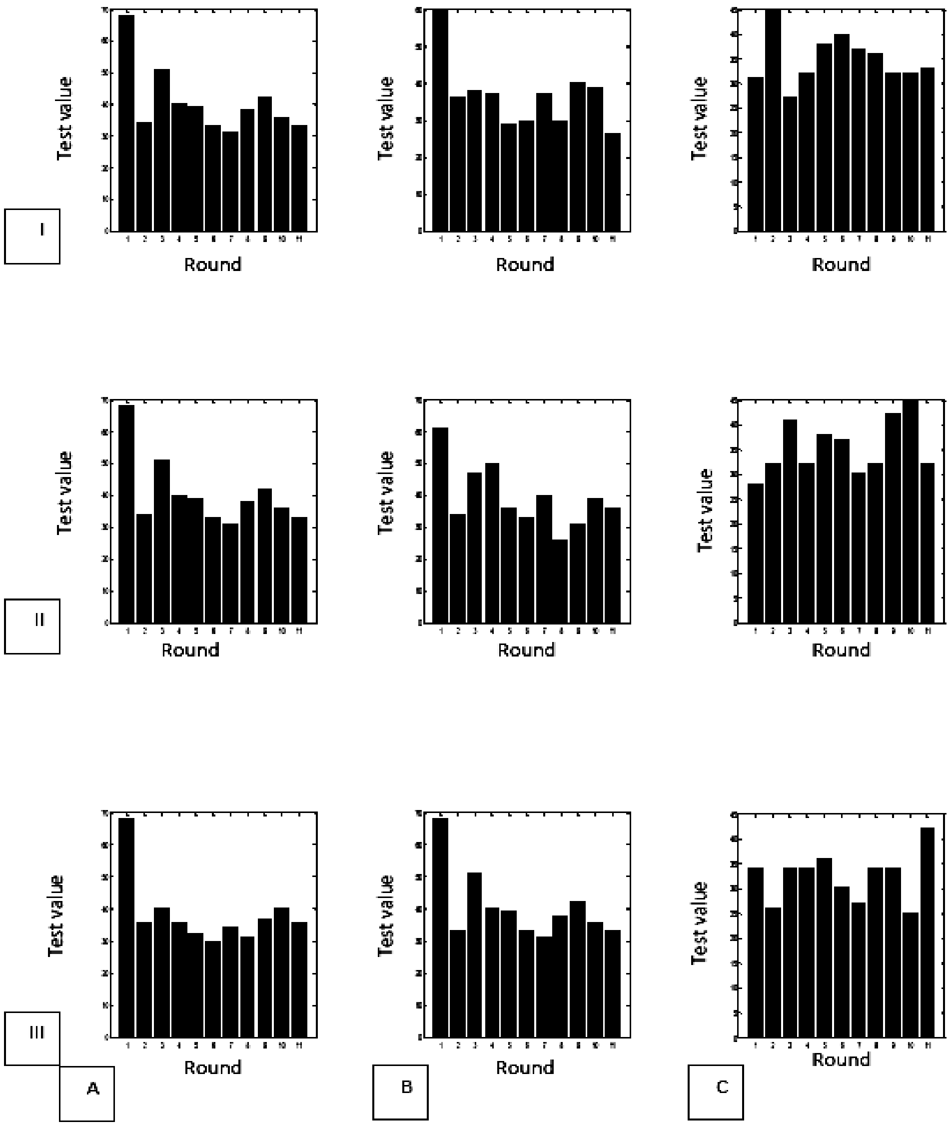

Fig. 4: Pker test for different Keys A) ordinary key B) ordinary with LFSR C)ordinary with MD5 I) key without change II) Keys with change one bit III)keys with change two bits

it's used widely in cryptographic protocols and Internet communication[6]. One of the most famous is the MD5 message digest algorithm developed by Ronald Rivest[7].The message digest to be generated by MD5 algorithm has the irreversible and non-counterfeit features, so MD5 algorithm is superior in anti-tamper capability.

Related Work

Was presented an architecture for the 10 rounds AES Algorithm implemented on an Altera FPGA device. The goal of this design is to produce, in a low cost FPGA, a minimum area core cipher that exploits the symmetry between encryption and decryption operations. A new efficient hardware implementations for the Advanced Encryption Standard (AES) algorithm with two main contributions are presented by[8], the first one is a high speed 128 bits AES encryptor, and the second one is a new 32 bits AES design. Mathematical description of Rijndael cipher and advantages of FPGA hardware implementation and software co-design and AES specifications was presented in[1,3] was described the cipher key generated from image. After this step , cipher key watermarked in image. S-Box generated by this key which it called Key-dependant S-box. These steps make AES algorithm more robust and more reliable[9]. Provides four different architectures for encrypting and decrypting 128 bit information via the AES. The encryption algorithm includes the Key Expansion module which generates Key for all iterations on the fly, Double AES two-key triple AES, AESX and AES-EXE. These architectures are implemented and studied in Altera Cyclone III and STRATIX Family devices.

Key tests

The first step in our work is the statistical testing of the keys. The aim of the statistical tests is to measure the quality of randomness of a generator and to detect certain kinds of weakness it may have. Let the binary sequence $S = s_0, s_1, s_2, \ldots, s_{n-1}$ of length n. The basic tests are[10];

Frequency test (mono-bit test)

The purpose of this test is to determine whether the numbers of 0's and 1's in S are approximately the same. This test is accomplished as follows: Let n_0 denotes the number of 0's and n_1 denotes the number of 1's, the test defined by;

$$X_1 = (n_0 - n_1)^2 / n \qquad ...(1)$$

Serial test (two-bit-test):

The purpose of this test is to determine whether the number of occurrences of 00, 01, 10, and 11 are approximately the same. Let, n_{00}, n_{01}, n_{10}, and n_{11} denote the number of occurrences of "00", "01", "10", and "11" in S, respectively, the test is calculated by;

$$X_2 = \frac{4}{n-1}(n_{00}^2 + n_{01}^2 + n_{10}^2 + n_{11}^2) - (n_0^2 + n_1^2) + 1 \qquad ...2$$

Poker test

The Poker test determines whether the occurrences of each part of length m are approximately the same. This test is accomplished as follows: Let the sequence S is divided into k non-overlapping parts of length m, and let n_i be the number of occurrences of the i^{th} part. This test defined by;

$$X_3 = \frac{2^m}{k}(\sum_{i=1}^{2m} h^2{}_i) - k \qquad ...(3)$$

Proposed Work

The work of this paper is based on the combination of the advantages of different key mechanism with AES. Therefore, the cipher system which exploits the advantages of AES cipher with LFSR and MD5 based stream ciphers and mitigates the weaknesses of these individual ciphers**.**

Our contribution in this paper is a multi-layer Key algorithm, where, as in Figure 1, the key algorithm are made by two stages when use LFSR and MD5 and one stage without it.

Propose system generates large key from short keyword using LFSR or MD5 concept. Plaintext is encrypted with large and pseudorandom letter generated key which help to flatten the letter frequencies of cipher text. AES algorithm was being taken is 128 bit because the output of MD5 is 128 bit.

The first step in the analysis is the test of Keys, then, test was made for each key by three times each one with change one bit and for three kind of test frequency (mono) bit, serial, and poker test. Figure (2) represent frequency (mono) bit test with change one and two bit and without it for ten rounds. From this Figure it's clear the distribution of MD5 is more reliable of the other for this test with and without change the bits. Figure (3) represent serial (two) bits test of these three types of key with and without bits change for ten rounds and this test view the similarity among these kinds of keys. Figure (4) represent the poker test of the keys for ten rounds and from this test, the MD5 is more stability to keep the blocks and gaps for change the bits than the other keys. Table (1) represent the average results for ten rounds of the different kinds (ordinary, LFSR, and MD5) of the key tests.

CONCLUSION

The paper is present a novel idea combining the classical encryption key technique and LFSR, MD5 based stream cipher technique for improved security of cipher key. The proposed work was selected the AES algorithm with 128 bit because MD5 output is 128, and the system can generate key stream with very large period, larger than the ordinary key and, hence provide more encryption security than conventional AES cipher. The Preference of MD5 than the other is clear specially at the frequency and poker test where its values are nearly enclosed. The complexity/security ratio of the design almost is high for ordinary and mid for LFSR and low nearly unity for MD5, therefore, the design also perform reasonably well in restricted resource environments. This work has been found secure for frequency analysis attack since the key period is larger than plain text.

REFERENCES

1. Ashwini M. Deshpande, Mangesh S. Deshpande and Devendra N. Kayatanavar, " FPGA Implementation of AES Encryption and Decryption", International conference on "control, automation, communication and energy conservation -2009, 4th-6 (2009).
2. Abdul Razzaq , Yasir Mahmood, Farooq Ahmed, Ali Hur, "Strong Key Machanism Generated by LFSR based Vigenère Cipher", 13th international arab conf. on information technology(ACIT), 10-13 (2012).
3. Razi Hosseinkhani, and Seyyed Hamid Haj Seyyed Javadi, " Using image as cipher key in AES", *IJCSI International Journal of Computer Science Issues*, **9**(2): (2012).
4. Meghana Hasamnis, Priyanka Jambhulkar, and S. S. Limaye, "Implementation of AES as a custom hardware using nios ii processor", Advanced Computing: An International Journal (ACIJ), Vol.3, No.4 (2012).
5. M. C. Liberatori, and J. C. Bonadero, "AES-128 Cipher. minimum area, low cost fpga implementation", Latin American Applied Research (2007).
6. Dongjing H. and Zhi X., " Multi-parallel Architecture for MD5 Implementations on FPGA with Gigabit-level Throughput", 2010 International Symposium on Intelligence Information Processing and Trusted Computing.
7. Kimmo J., Matti T. and Jorma S., " Hardware Implementation Analysis of the MD5 Hash Algorithm", Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.
8. Issam Mahdi Hammad, "efficient hardware implementations for the advanced encryption standard (AES) Algorithm", Master thesis of Applied Science, Dalhousie University, Halifax, Nova Scotia, October 2010.
9. Sliman Arrag, Abdellatif Hamdoun, Abderrahim Tragha, and Salah eddine Khamlich, " Several AES Variants under VHDL language In FPGA", *IJCSI International Journal of Computer Science Issues*, 9(3) (2012).
10. William Stallings, "Cryptography and network security principles and practice", FIFTH EDITION, 2011.