Journal of Theoretical and Applied Information Technology
10th February 2015. Vol.72 No.1

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

ENHANCING ADVANCED ENCRYPTION STANDARD (AES) S-BOX GENERATION USING AFFINE TRANSFORMATION

[1]NUR HAFIZA ZAKARIA, [2]RAMLAN MAHMOD, [3]NUR IZURA UDZIR, [4]ZURIATI AHMAD ZUKARNAIN

[1]Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia
[2]Prof., Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia
[3,4]Assoc. Prof., Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Malaysia
E-mail: [1]mz.hafiza@gmail.com, [2]ramlan@upm.edu.my, [3]izura@upm.edu.my, [4]zuriati@upm.edu.my

ABSTRACT

The development of technology has resulted in a number of new suggestions done on block ciphers. Although there have been so much evolvement of the block cipher, the industry still needs another block cipher as long as the cipher is secured and met all the security requirements. One of the critical parts is, secured communication which assists to protect the confidentiality and integrity of the data. Secured communication can be attained by encrypting the data. In this research, we proposed to enhance Advanced Encryption Standard (AES) S-Box generation using affine transformation approach which shall meet the security requirements. AES is one of the best cryptographic algorithms that can be used to protect electronic information. Researchers have found a weakness in the AES algorithm. They managed to come up with a clever new attack that can recover the secret key four times easier than anticipated by experts. In this research, we are trying to remove the weaknesses of AES by changing the S-Box and adding one new function which are inspired from crossover and mutation process. This improvement will satisfy the security of AES.

Keywords: *AES, Affine Transfomation, S-box, Randomness, Cryptanalysis, Confusion, Diffusion*

1. INTRODUCTION

In January 1997, the US National Institute of Standards and Technology (NIST) announced the start of a proposal to develop a new encryption standard: the Advanced Encryption Standard (AES) [1]. The new encryption standard was to become a Federal Information Processing Standard (FIPS), replacing the old Data Encryption Standard (DES) and triple-DES. Unlike the selection process for the DES, the Secure Hash Algorithm (SHA-1) and the Digital Signature Algorithm (DSA), NIST had declared that the AES selection process would be open. Anyone could submit a candidate cipher. Each submission, provided it met the requirements, would be considered on its merits. NIST would not perform any security or efficiency evaluation itself, but instead invited the cryptology community to mount attacks and try to cryptanalyze the different candidates and anyone who was interested to evaluate implementation cost. All results could be sent to NIST as public comments for publication on the NIST AES website or be submitted for presentation at AES conferences. Finally, on 2 October 2000, NIST officially announced that Rijndael without modifications would become the AES [1]. The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is based on Rijndael cipher which is developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen. AES is a block cipher with block size of 128 bits or 16 bytes. Keys for the cipher come in one of three lengths: 128, 192 or 256 bits, which is 16, 24, or 32 bytes. The main mathematical difficulty with the algorithm is

Journal of Theoretical and Applied Information Technology
10th February 2015. Vol.72 No.1

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

that it uses arithmetic over the field $GF(2^8)$. Aim for this research is to propose new design of S-box based on affine transformation and add new function of AES block cipher algorithm based on crossover and mutation approach. This element can be associated with the confusion and diffusion properties in cryptography.

The S-box constructed in AES algorithm uses the affine transformation

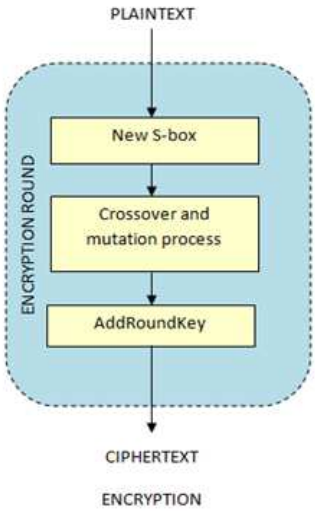
$$y = Ax \oplus C \bmod m(x) \quad (1)$$

where A is an 8x8 matrix with entries in GF(2) and C is a column matrix in GF(2), m(x) is an irreducible polynomial in $GF(2^8)$. The entries used in A matrix are:

$[f8_h:7c_h:3e_h:1f_h:8f_h:c7_h:e1_h:f1_h]$ and $C=[63]^T$ (2)

To be useful as S-box generator, matrix A should be non-singular. We can generate approximately 2^{63} such non-singular matrices with each irreducible polynomials [2]. In this paper, we construct different S-boxes using affine transformation and add new component which are inspired from crossover and mutation process.

2. PROPOSED DESIGN FOR NEW AES ALGORITHM



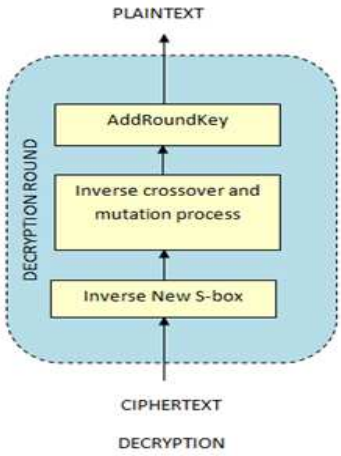


Figure 1 : Proposed Design for New AES Algorithm

This new proposed design uses affine transformation for S-Box operation. The steps involved in generating an S-Box for AES algorithm using an affine transformation are as follows[2] :

i. S-box is a 16x16 matrix. Initialize the first row with [00];[01];[02]:::[0f], second row with [10];[11];[12]:::[1f] and so on with last row as [f0];[f1];[f2]:::[ff].

ii. Map each byte into its multiplicative inverse with any one of the irreducible polynomials m(x), with [00] mapped to itself.

iii. Using affine transformation in equation (1), construct S-box with polynomials given in equation (2).

It is possible to construct different S-boxes using different A, C and irreducible polynomials m(x). It is found that with cyclic shift only the following independent polynomials will give non-singular matrices. They are 01_h,07_h,$0b_h$,$0d_h$,13_h,15_h,19_h,$1f_h$,25_h,$2f_h$,37_h,$3d_h$,57_h ,$7f_h$. By using any one of these polynomials, S-box can be constructed. However in this paper, only one S-box was chosen to be tested for statistical test. The generated S-box is as below:

Journal of Theoretical and Applied Information Technology
10th February 2015. Vol.72 No.1

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

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	61	78	8e	f4	c7	95	c0	b2	fd	31	e2	02	a0	a8	ec
1	8b	0a	36	f5	50	35	a3	dd	d3	1d	98	fa	9c	e3	be	06
2	17	bf	d7	80	c9	f9	32	f0	e0	77	52	49	03	eb	26	e6
3	3b	e9	46	bb	84	11	af	e7	86	09	23	bd	8d	14	d1	51
4	59	9e	0d	ad	39	01	88	b1	2c	ab	34	45	cb	29	b0	71
5	b8	db	69	f6	fb	2b	6c	1c	53	1f	27	82	c1	ba	a1	4d
6	4f	df	3c	c4	f1	2e	0f	e5	8a	ed	40	dc	05	44	21	15
7	91	0c	4c	68	43	08	16	1b	0e	83	c2	6f	20	96	60	66
8	64	9f	9d	62	4e	85	1e	cf	54	5e	48	d0	8c	67	10	2a
9	de	b7	07	b9	d2	76	6a	87	37	4b	5c	72	90	da	70	56
a	94	9b	3f	e4	7c	12	a9	f3	2f	f2	47	f7	fe	ac	c6	a7
b	7b	a2	5d	bc	41	89	93	81	28	7e	8f	19	18	1a	6e	cd
c	75	33	3d	24	d6	ca	aa	7d	30	2d	c5	6b	55	9a	3a	ae
d	97	6d	3e	a5	e8	d4	a6	b6	4a	74	ea	c8	58	92	42	b5
e	00	79	ce	b4	ee	7f	fc	38	73	ff	cc	a4	d9	c3	5f	04
f	d5	25	13	0b	b3	ef	65	7a	d8	5a	99	22	f8	57	e1	5b

Figure 2 : S-Box for the polynomial 01_h

3. RESULTS AND DISCUSSIONS

All data of the 128 bits plaintext and 128 bits key were generated and evaluated offline. These values were based on data generated using the Blum-Blum-Shub (BBS) pseudo-random bit generator. The BBS was chosen in this experiment testing because it has been shown to be cryptographically secure pseudo-random bit generator [3] [4]. This popular approach for generating secure pseudo-random number was also used to select finalist candidates for the AES block cipher in [5][6][7]. Randomness test is one of the security analyses which measures confusion and diffusion properties of the new symmetric block cipher. The experiment was made using NIST Test Suite application.

Table 1 below display the results of the Frequency Test for AES and S-Box 01_h. For S-box with polynomial 01_h, it was reported that 49 out of 50 sequences recorded a p-value greater than 0.01, which means that the S-box with polynomial 01_h passes the Frequency Test with a proportions of 0.98.

Table 1: Frequency Test for AES and S-Box 01_h

No.	Ciphertext	AES	S-Box 01_h
1	Ciphertext 1	1.000000	0.479500
2	Ciphertext 2	0.595883	0.021556
3	Ciphertext 3	0.595883	0.723674
4	Ciphertext 4	1.000000	0.021556
5	Ciphertext 5	0.723674	1.000000
6	Ciphertext 6	0.859684	1.000000
7	Ciphertext 7	0.595883	0.288844
8	Ciphertext 8	0.215925	0.215925
9	Ciphertext 9	0.215925	0.859684
10	Ciphertext 10	0.859684	0.479500
11	Ciphertext 11	0.215925	0.288844
12	Ciphertext 12	0.723674	0.376759
13	Ciphertext 13	0.595883	0.479500
14	Ciphertext 14	0.859684	0.479500
15	Ciphertext 15	0.595883	0.376759
16	Ciphertext 16	0.595883	0.021556
17	Ciphertext 17	0.376759	0.479500
18	Ciphertext 18	0.021556	0.157299
19	Ciphertext 19	0.376759	0.376759
20	Ciphertext 20	1.000000	0.595883
21	Ciphertext 21	0.859684	0.595883
22	Ciphertext 22	0.723674	0.595883
23	Ciphertext 23	0.859684	0.288844
24	Ciphertext 24	0.157299	0.479500
25	Ciphertext 25	0.859684	0.595883
26	Ciphertext 26	0.288844	1.000000
27	Ciphertext 27	0.859684	0.376759
28	Ciphertext 28	0.376759	0.051830
29	Ciphertext 29	0.288844	0.376759
30	Ciphertext 30	0.157299	0.479500
31	Ciphertext 31	0.723674	0.479500

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

32	Ciphertext 32	0.215925	0.859684
33	Ciphertext 33	0.859684	0.595883
34	Ciphertext 34	0.859684	1.000000
35	Ciphertext 35	0.595883	0.008010
36	Ciphertext 36	0.479500	0.859684
37	Ciphertext 37	1.000000	0.288844
38	Ciphertext 38	0.376759	0.376759
39	Ciphertext 39	0.021556	0.479500
40	Ciphertext 40	0.595883	0.376759
41	Ciphertext 41	0.288844	0.595883
42	Ciphertext 42	0.859684	0.288844
43	Ciphertext 43	0.595883	0.157299
44	Ciphertext 44	0.595883	0.595883
45	Ciphertext 45	0.595883	0.595883
46	Ciphertext 46	0.479500	0.288844
47	Ciphertext 47	0.595883	0.859684
48	Ciphertext 48	0.859684	1.000000
49	Ciphertext 49	0.051830	0.288844
50	Ciphertext 50	0.376759	0.376759

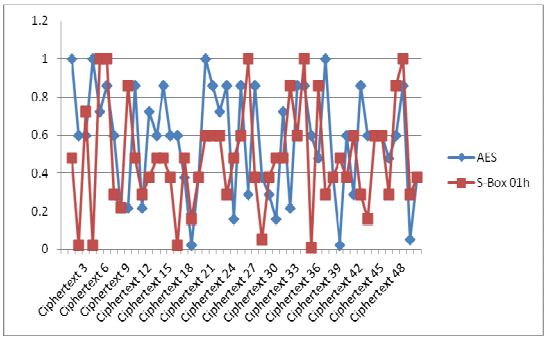


Figure 3 : Frequency Test for AES and New Design (Sbox 01_h)

4. FUTURE ENHANCEMENT

AES has been designed to have very strong resistance against linear and differential cryptanalysis. After the new proposed algorithm successfully passes the NIST statistical tests, we will perform algebraic attack in attempt to break the cipher and test the security of this new design.

5. CONCLUSION

In this paper, a new design of S-box for enhancing the security of AES algorithm is proposed. Referring to the analyzed results of randomness test, new S-box fulfils the confusion and diffusion properties. The results indicate that the new S-box is capable to increase the performance of generating random output. Therefore, it can be able to create larger confusion and diffusion properties.

REFERENCES:

[1] Daemen, J. And Rijmen, V. (2002). *The Design of Rijndael, AES – The Advanced Encryption Standard.* Springer-Verlag.

[2] Chandrasekharappa, T.G.S., Prema, K.V. and Kumara, S (2011). S-boxes generated using Affine Transformation giving Maximum Avalanche Effect. *International Journal on Computer Science and Engineering (IJCSE)* on 3(9):3185-3193.

[3] Stallings, W. (2001). *Cryptography and network security: principles and practice.* Prentice Hall.

[4] Menezes, A. J., Oorschot, P. C. V., and Vanstone, S. A. (1997). *Handbook of Applied Cryptography.* CRC Press.

[5] Soto, J. (2000). Randomness testing of the AES candidate algorithms. Technical report, National Institute of Standards and Technology.

[6] Soto, J. And Bassham, L. (2000). Randomness testing of the advanced encryption standard finalist candidates. Technical report, National Institute of Standards and Technology.

[7] Murphy, S. (2000). The power of NIST's statistical testing of AES candidates.

[8] Partheeban, P. And Nityanandam, N. (2013). Generation of Dynamic S-Box Using Irreduceable Polynomial and the Secret Key Used. *International Journal of Research in Engineering and Science (IJRES on,* 1(5):24-27.

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

[9] de Castro, L. N. and Timmis, J. (2002). *Artificial Immune Systems: A New Computational Intelligence Approach.* Springer.

[10] Marhusin, M., Cornforth, D., and Larkin, H. (2008). Malicious code detection architecture inspired by human immune system. In *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, 2008. SNPD '08. Ninth ACIS International Conference on,* pages 312-317.

[11] Harmer, P., Williams, P., Gunsch, G., and Lamont, G. (2002). An artificial immune system architecture for computer security applications. *Evolutionary Computation, IEEE Transactions on,* 6(3):252-280.