Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 7, No. 1, March 2019, pp. 29~36
ISSN: 2089-3272, DOI: 10.11591/ijeei.v7i1.652

Modified AES cipher round and key schedule

Edjie M. De Los Reyes[1], Dr. Ariel M. Sison[2], Dr. Ruji P. Medina[3]
[1,3]Technological Institute of the Philippines, Philippines
[2]Emilio Aguinaldo College, Philippines

Article Info

Article historys:

Received Aug 24, 2018
Revised Dec 20, 2018
Accepted Jan 16, 2019

Keywords:

Avalanche effect
Confusion
Cryptographic algorithm
Diffusion
Frequency test

ABSTRACT

In this paper, Advanced Encryption Standard was modified to address the low diffusion rate at the early rounds by adding additional primitive operations such as exclusive OR and modulo arithmetic in the cipher round. Furthermore, byte substitution and round constant addition were appended to the key schedule algorithm. The modified AES was tested against the standard AES by means of avalanche effect and frequency test to measure the diffusion and confusion characteristics respectively. The results of the avalanche effect evaluation show that there was an average increase in diffusion of 61.98% in round 1, 14.79% in round 2 and 13.87% in round 3. Consequently, the results of the frequency test demonstrated an improvement in the randomness of the ciphertext since the average difference between the number of ones to zeros is reduced from 11.6 to 6.4 along with better-computed p-values. The results clearly show that the modified AES has improved diffusion and confusion properties and the ciphertext can still be successfully decrypted and recover back the original plaintext.

Corresponding Author:

Edjie M. De Los Reyes,
Technological Institute of the Philippines,
Quezon City, Philippines.
Email: emdelosreyes@tsu.edu.ph

1. INTRODUCTION

Development of information technology has immensely influenced the change in communication from conventional to digital means [1]-[3], this improvement in communication lead to confidentiality issues especially during the transit of information from source to its intended recipient [4], [5].

Information hiding and cryptography are the most common approach in providing information security [6], [7]. Steganography is a method of information hiding where it uses digital media as a cover to conceal information. However, once the pattern is known the information can be easily recovered [8], [9].

Cryptography is used to secure any form of communication system [10]-[12] by scrambling the information so that only the intended recipient can access it. Cryptography uses two general schemes: hashing and encryption. The cryptographic encryption scheme is classified into asymmetric and symmetric. The Advanced Encryption Standard (AES) is a symmetric block encryption defined by the Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST) of the United States of America (USA) and is currently the standard for encryption.

The AES algorithm, founded on the design of Belgian cryptographers Joan Daemen and Vincent Rijmen became the standard for encryption starting 2002 [13]. The algorithm has a data block length of 128 bits with variable key sizes of 128-bit (called AES-128), 192-bit (AES-192), and 256-bit (AES-256). The number of rounds to complete the process of encryption depends on the key size: 10 rounds for AES-128; 12 rounds for AES-192; and 14 rounds for AES-256 [14]. AES has different advantages such as security, flexibility, and ease of implementation.

Although AES is secured there is still room for improvement, especially in its diffusion property [15], [16] as it was observed that diffusion rate is quite slow in the early rounds [17], [18]. This paper introduced two modifications to the standard AES to improve the diffusion property and as well as its confusion property. First modification is in the AES key schedule, additional permutation operations are used in the cipher key before it is expanded and second is in the AES cipher round where additional key permutation operations were introduced between states to achieve faster diffusion rates and better randomness of encrypted data.

2. RESEARCH METHOD

The two modifications to the standard AES are in (1) the key schedule algorithm and (2) the cipher round algorithm.

The key scheduling algorithm of AES is modified by introducing an additional byte substitution process and round constant addition through XOR prior to the generation of the subkeys: to prevent the cipher key bits from being used directly [19]. These modifications in the key scheduling algorithm are shown in Figure 1.

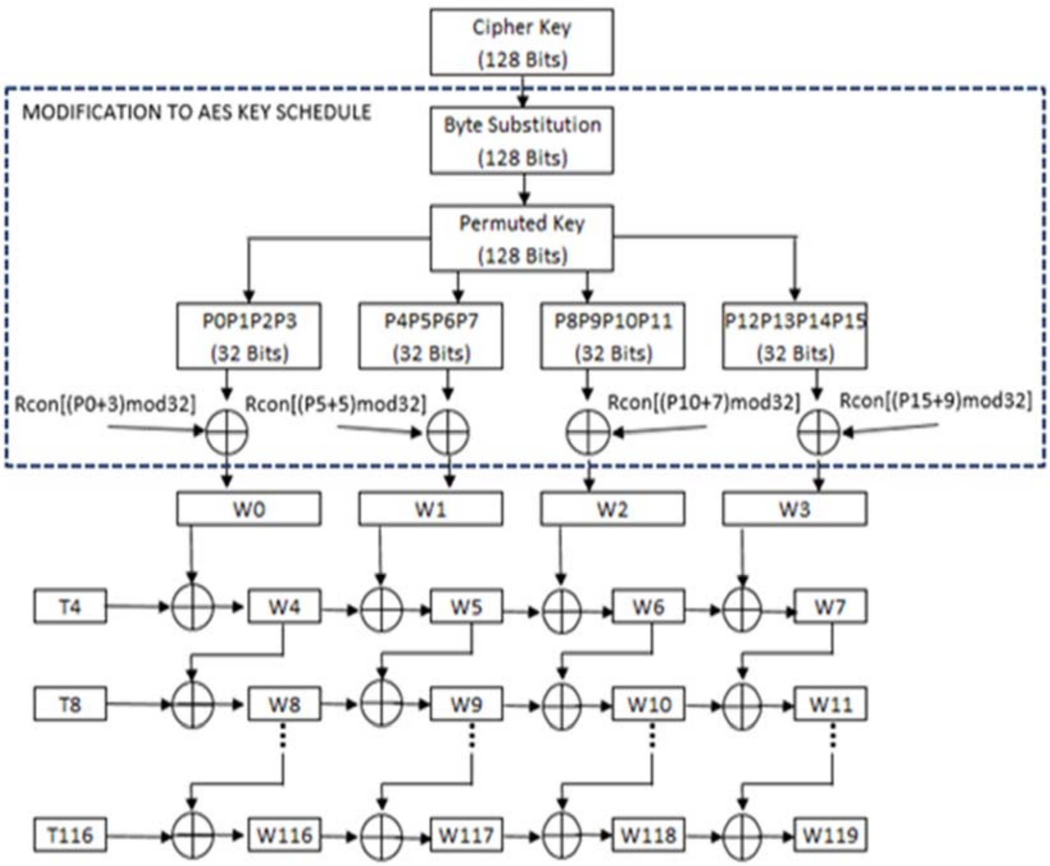

Figure 1. Modified AES Key Schedule

The standard S-box of the AES is used in the additional byte substitution process to provide additional obscurity to the cipher key since part of the design of the S-box is nonlinearity [20]. Furthermore, the output of the substitution herein referred to as permuted key (P), is then divided into four words where each word consists of 32 bits in length and each word is XORed with a value taken from the round constant of AES.

The round constant to be used will depend on the value of a specific byte of a word. The round constant is utilized to remove any symmetries in the cipher key [20]. Lastly, the succeeding stages in the key schedule algorithm are the same as the standard AES except for the number of iterations needed to generate all the required subkeys. The key schedule for both the encryption and decryption processes of the modified AES are the same.

Subsequently, the modifications to the cipher round algorithm of the AES in the encryption cycle are shown in Figure 2.

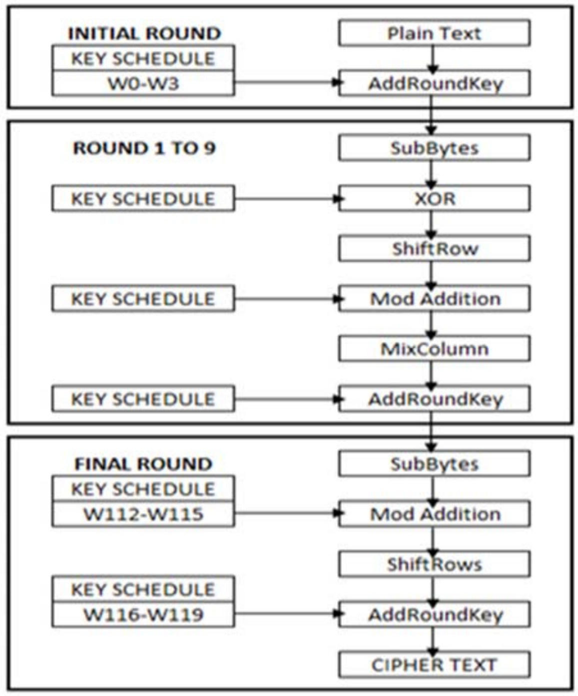

Figure 2. Modified AES Cipher Round - Encryption

The modifications to the AES cipher round are inclusions of XOR key permutation after the SubBytes operation and Modulo Addition key permutation after the ShiftRow operation from rounds one to nine. In the final round of the encryption, round ten, modulo addition is added after the SubBytes operation. The XOR operation is the same as the original add round key function, while modulo addition in the encryption process is a byte operation using the (1):

$$S'x = (Sx + Bwx)\ mod\ 256 \qquad (1)$$

Where $S'x$ is the new byte of the resulting state after modulo addition, Sx is a byte of the current state to undergo modulo addition, and Bwx is the respective byte of the subkey that is to be added with the current state matrix.

To elucidate the modified AES encryption process, let "a3bb37a0fcfbff36ec56b737529723d2" be the plaintext in hexadecimal format and the cipher key as "6d6e636b795f72656f7365797765745f". The given strings are first translated into 4 by 4 state matrix, the state matrix is formed by taking 2 hexadecimal characters at a time from the given string and arranged from top to bottom then left to right as shown in Figure 3.

In the initial round of the modified AES, the plaintext is XORed (AddRoundKey) with the first subkey in the key schedule which is W0-W3. The result of the AddRoundKey is then passed to the SubBytes process for byte substitution using the standard AES S-box.

The SubBytes process is the start of a new round. The succeeding processes: the byte substitution, the added add round key using XOR operation, the shift row operation, the added add round key operation using modulo addition, the mix column and the add round key using an XOR operation will iterate until round 9.

The last AddRoundKey operation of round 9 is then passed through the SubBytes. In this process, a byte substitution takes place where each byte of the AddRoundKey state matrix is replaced with an equivalent value based on the AES S-box, producing the SubBytes state matrix of the final round. The SubBytes state matrix is then modulo added with the subkey W112-W115 of the key schedule followed by a ShiftRow operation. The ciphertext is finally derived from the AddRoundKey operation of the ShiftRow state matrix and the final subkey W116-W119.

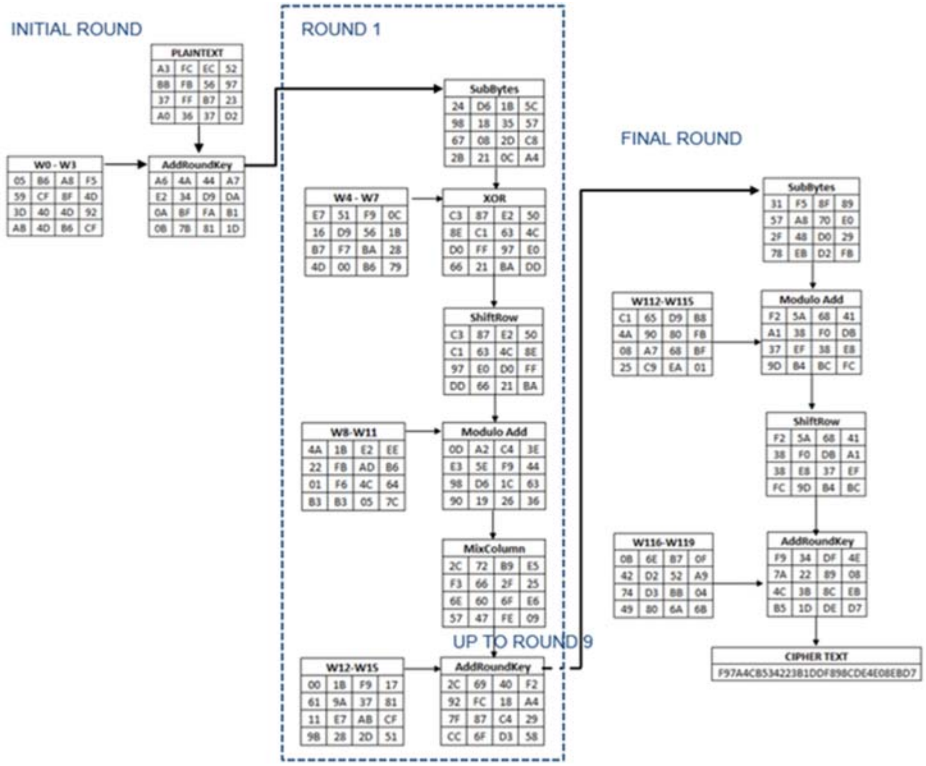

Figure 3. Illustrated Simulation of the Modified AES - Encryption Cycle

The decryption process will be the opposite of the encryption round where the different functions will be using their inverses: ShiftRow to Inverse ShiftRow, SubBytes to Inverse SubBytes, and MixColumns to Inverse MixColumns. While the modulo addition is changed to modulo subtraction and the formula used for modulo subtraction is shown in (2). The modified AES cipher round algorithm for decryption is shown in Figure 4.

$$Sx = (S'x - Bwx) mod\ 256 \quad (2)$$

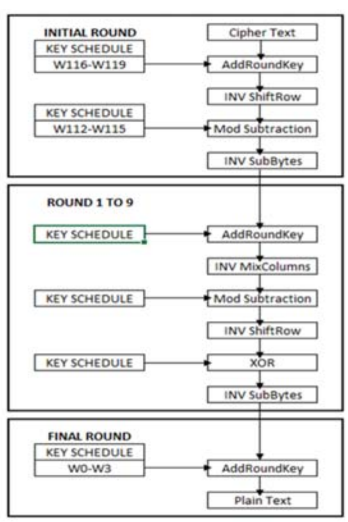

Figure 4. Modified AES Cipher Round - Decryption

An illustrative simulation of the decryption process is shown in Figure 5. The ciphertext input is XORed with the subkey W116-W119 of the modified AES key schedule, the key scheduling during decryption is also the inverse of the encryption key schedule, i.e. the first key schedule in the encryption cycle is the last key schedule in the decryption cycle.

The AddRoundKey state matrix is then applied with an inverse shift row operation and then modulo subtracted with the subkey W112-W115. The last operation in the initial round is an inverse byte substitution to the modulo subtraction state matrix.

The state matrix of the inverse SubBytes of the initial round is then XORed with the subkey W108-W111. The result of this step is the state matrix of the AddRoundKey and is then processed using the inverse mix column. These stages are repeated 9 times.

Subsequently, the state matrix of the inverse SubBytes of the ninth round is then XORed with W0-W3 subkey to recover back the original plaintext.

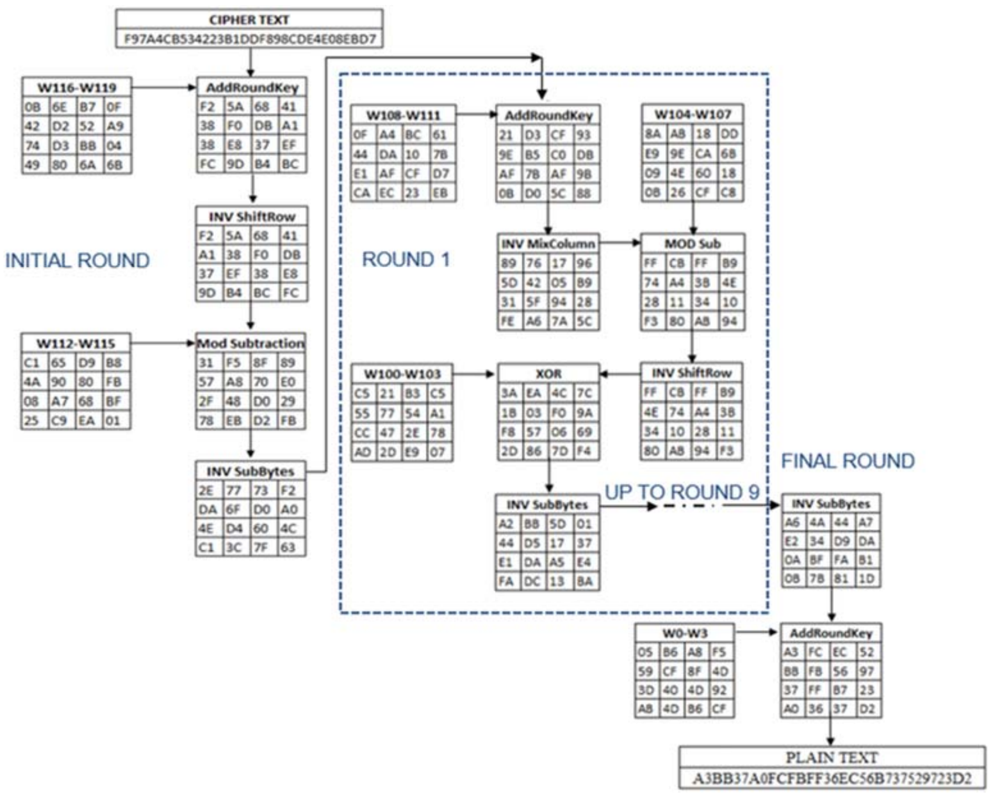

Figure 4. Illustrated Simulation of Modified AES Decryption Cycle

3. RESULTS AND ANALYSIS

The modifications to AES are tested using 10 different samples of plaintexts in hexadecimal format and to determine the performance of the modified AES in terms of its diffusion characteristics: the avalanche effect is employed. Hence, the status of one bit of the plaintext is changed (from bit 0 to bit 1 and vice versa) the highlighted hexadecimal character signifies this change in the bit status. The plaintexts are shown in Table 1.

The cipher key: 45654C65644D6F796A44736569655273 is used to encrypt the plaintexts enumerated in Table 1. The encrypted results of the standard AES for the 10 input samples of the original plaintexts and the plaintexts with one flipped bit are shown in Table 2. While the encrypted results for the modified AES are shown in Table 3.

The avalanche effect is computed by getting the summation of the number of bits that have changed between the encrypted plaintext and the ciphertext of the input with one bit flipped.

To demonstrate the effect of the modified AES cipher round and key schedule, the avalanche effect for the first 5 rounds of both the standard AES and the modified AES are taken and shown in Table 4.

Table 1. Input plaintexts

Samples	Plaintexts	Plaintexts with One Bit Flipped
1	8CE0522352A3622E39D82E4E0C69459B	8CE0522352A3622E**1**9D82E4E0C69459B
2	B7FFDB3473357E17A08D8DDE34D614B9	B7**D**FDB3473357E17A08D8DDE34D614B9
3	AEF6A545B7B00CA10225CBE70EE25907	AEF6A545B7B00CA1**4**225CBE70EE25907
4	2A60EF8D9F0F6909612E7CE1734F33D6	2A60EF8D9F0F69**2**9612E7CE1734F33D6
5	B9A920481E1DC1705EB238D7C256665A	B9A920481E**3**DC1705EB238D7C256665A
6	AFDEAE30C1D4A939E89011467C11C955	AFDEAE30C1D4A939**6**89011467C11C955
7	0AE231D3CC3865DAB650465BE5A61D62	0AE231D3CC3865DAB650465BE5A61D6**3**
8	6AAB3E2CE1EB488AEDE3E5C271E7B59D	6AAB3E2CE1EB**6**88AEDE3E5C271E7B59D
9	5C484433CA71082A6544D0D923A5BC36	5C**C**84433CA71082A6544D0D923A5BC36
10	F68545373518FE8658C8DF729DFCE965	F685453**5**3518FE8658C8DF729DFCE965

Table 2. Standard AES ciphertext results

Samples	Encrypted Plaintexts	Encrypted Plaintexts with One Bit Flipped
1	50796041DDC6C7748CD16621D03730BC	95006CC37096C0D44D44ADBC3E717A5D
2	1E44EFE4637CCAB5295BE522B38033FE	B5C1B3E66D05550C093167863ED4CA30
3	93737532CA9A374202A85A265879B2AD	272A23CF82DA81096785FFE9EDD646F3
4	E46E0D7E8740FBB9D6D765F7ECE61CED	EA62609CD436C42B97C15CA99B6509E9
5	27C24083CF405EA7D32FF5F5AF56DA2A	D35EA9DDF514FA899E02D4F422051050
6	F7864F3BC4785C3F306B6C7735A8D632	8ABE1E0CAF227A539A0CCE4625D3B827
7	6D904E0F746CE9950BB4B7257706BC6F	60DAAADCDB8F9A5F1EBD1718BCAF4521
8	6FBDBDBE2AAAF889FE7D9812C7765D82	5084EAEDE99F2869DD8678976FABAB47
9	0D39B23D5045A22AFB72DFE63427B7D7	B90CBAC30B12037857DBA82023C30CCD
10	78224BBB5F4061F92D463175F3BF4AFD	B06A2C1A27AFAB8F718B8463EB39F963

Table 3. Modified AES ciphertext results

Samples	Encrypted Plaintexts	Encrypted Plaintexts with One Bit Flipped
1	B3A29FB59A819F5BD6B9A041FBA7BE93	F847568BA83F2E8B74E9B9E3C26E476C
2	2F32B3FF51F1808E85A3E0441EEDD43D	42BD8A1A90B0FA91096C3B8861820C1B
3	65BB3DB5163CA56B388FA44518156F45	616C805C353F49F5FDBA163DD92BD668
4	E68585DC6BBA52013EE676BE0AF2F10E	946C0199AE2EB5241747DF154A05D50C
5	2762D80CEBE87736C8AD29AE5C15D3AD	59C287045E148A23C958AC78432985FA
6	BF20B2AAEAF5162BCB6A3736EEC56F75	D3D9CCE19AAE704650C04DB4FB922880
7	BA1E83967AF7699223F6DC125BF4C44D	19D905B7B6FA9E2147AFA662767CFEBB
8	18AA0019AF8B669EECE63AE57155CFE4	D65DCD48AEEC1E240A653CC5747B67FA
9	09D8A5397E0D65C2FD8FE81517803275	89DC4B724D54307543E1B55C6DCEF6C6
10	3E64BA827097E648CA387E16421A49B5	7C75DD0FC8F7408BD1F3C7713F706F5B

Table 4. Avalanche effect for the first five rounds

Samples	Round 1		Round 2		Round 3		Round 4		Round 5	
	S.AES	M.AES	S.AES	M.AES	S.AES	M.AES	S.AES	M.AES	S.AES	M.AES
1	13	21	60	66	65	69	72	78	76	67
2	13	19	51	78	64	74	72	72	59	63
3	16	19	62	69	69	84	55	72	76	67
4	5	16	75	77	55	67	71	69	62	65
5	5	22	60	62	59	62	64	73	64	70
6	13	20	59	73	69	72	61	68	63	67
7	10	20	65	74	62	66	69	74	67	62
8	10	20	63	70	57	73	66	63	66	70
9	18	19	75	76	53	64	53	65	58	69
10	18	20	59	77	60	67	66	62	63	72

Based on these results, there is a significant increase in the avalanche effect of the modified AES cipher round and key schedule compared to the standard AES. In round 1, the average avalanche effect of the standard AES is 12.1 bits while the modified AES is 19.6 bits giving 61.98% improvement over the standard AES. Moreover, the modified AES has an improvement of 14.79% and 13.87% in round 2 and round 3 respectively. Consequently, an increase in the average results of the avalanche effect of the modified AES rivaled with the standard AES is evidently shown in Figure 6, the increase in avalanche effect also indicates an increase in security compared to the standard AES [21], [22]. The overall improvement of the modified AES in the avalanche effect over the standard AES is about 7%.

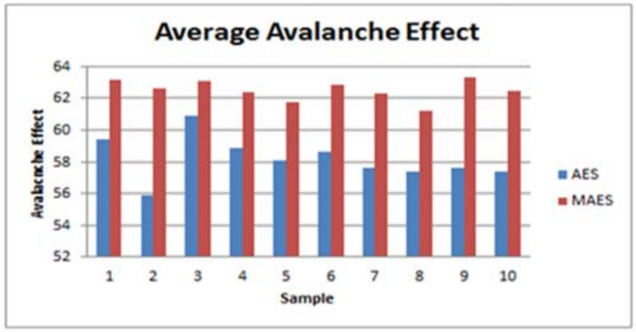

Figure 6. Comparison between Standard AES and Modified AES

To measure the confusion property of the modified AES, frequency test is utilized. The frequency test determines the randomness of a string by assessing the number of ones and zeros: when they are approximately the same in number then it indicates randomness [23]. The *P-value* in (3) will be used in determining whether a cryptographic result is either random or not.

$$P - value = erfc\left(\frac{Sobs}{\sqrt{2}}\right) \quad (3)$$

The *P-value* is the probability of finding the observed results, under the null hypothesis of randomness [23], hence if the result of the *P-value* is <0.01 the null hypothesis is accepted meaning the cryptographic result is non-random. However, if the *P-value* is >0.01 then the cryptographic result is random.

The results of the frequency test of both the standard AES and the modified AES using the same input samples and key are shown in Table 5. The Ones and Zeros columns in the table represent the total number of ones and zeros respectively in the ciphertext string while the Sobs-column is the observed value.

Table 5. Frequency test results

Samples	Ones		Zeros		Sobs		*p-value*	
	S.AES	M.AES	S.AES	M.AES	S.AES	M.AES	S.AES	M.AES
1	58	72	70	56	1.061	1.414	0.289	0.157
2	67	65	61	63	0.530	0.177	0.596	0.860
3	60	64	68	64	0.707	0.000	0.480	1.000
4	76	66	52	62	2.121	0.354	0.034	0.724
5	68	66	60	62	0.707	0.354	0.480	0.724
6	69	73	59	55	0.884	1.591	0.377	0.112
7	67	68	61	60	0.530	0.707	0.596	0.480
8	74	65	54	63	1.768	0.177	0.077	0.860
9	69	62	59	66	0.884	0.354	0.377	0.724
10	70	59	58	69	1.061	0.884	0.289	0.377

Based on these frequency test results, all the encrypted texts for both standard AES and modified AES are random and henceforth non-linear since the computed *p-values* are higher than 0.01. However, it is noteworthy to point out that the distribution of ones and zeros have improved in the modified AES over the standard AES. The average difference between the distribution of 1's and 0's for the 10 samples are: 6.44 bits in the modified AES; 11.6 bits in the standard AES. Conversely, there are 7 instances where the modified AES is better than the standard AES in terms of computed *p-values.*

4. CONCLUSION

In cryptography, diffusion and confusion property indicates the strength of a cryptographic algorithm [24]. Based on the results, the modified AES cipher round and key schedule algorithm have shown an increased in the diffusion characteristics both in the early rounds and in the full rounds of encryption. This improvement is attributed to the introduction of additional key permutations in the cipher round using simple primitive operations such as exclusive OR and modulo arithmetic. Likewise, the confusion characteristics of the modified AES are enhanced based on the results of the frequency test. Moreover, the modified AES can be successfully decrypted and recover back the original plaintext. However, though improvements were noted in the confusion property, there is still room for improvements.

For future works, the following may be considered, to introduce additional linear operations to improve further the confusion property and apply the modified AES cipher round and key schedule algorithm in securing confidential files. Additonal study may be conducted to determine the effect of the added operations in terms of performance with respect to execution throughput of the modified AES.

REFERENCES

[1] E. Setyaningsih and R. Wardoyo,"Review of Image Compression and Encryption Techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 2, pp. 83–94, 2017.
[2] M. Mostafa, "Joint Image Compression and Encryption Based on Compressed Sensing and Entropy Coding Joint Image Compression and Encryption Based on Compressed Sensing and Entropy Coding," 2017.
[3] A. Vaish, S. Gautam, and M. Kumar, "A wavelet based approach for simultaneous compression and encryption of fused images," *J. King Saud Univ. - Comput. Inf. Sci.*, 2016.
[4] P. Kumar, A. K.M, and P. B.R, "Enhanced Cloud Data Security Using AES Algorithm," *2017 Int. Conf. Intell. Comput. Control Enhanc.*, 2017.
[5] A. Ray, A. Potnis, P. Dwivedy, S. Soofi, U. Bhade, and A. A. E. S. Algorithm, "XOR Operation, And Watermarking for Image Encryption," pp. 27–29, 2017.
[6] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least signi fi cant bit and integer wavelet transform," vol. 29, no. 3, pp. 639–649, 2018.
[7] N. Islam, Z. Shahid, and W. Puech, "Denoising and error correction in noisy AES-encrypted images using statistical measures," *Signal Process. Image Commun.*, vol. 41, pp. 15–27, 2016.
[8] D.-H. Kim and H.-Y. Lee, "Deep Learning-Based Steganalysis Against Spatial Domain Steganography," *2017 Eur. Conf. Electr. Eng. Comput. Sci.*, pp. 1–4, 2017.
[9] C. Qin, W. Zhou, W. Zhang, and N. Yu, "Ensemble Steganography," *2018 IEEE Third Int. Conf. Data Sci. Cybersp.*, pp. 582–587, 2018.
[10] A. Devi, A. Sharma, and A. Rangra, "A Review on DES , AES and Blowfish for Image Encryption & Decryption," *IJCSIT (International J. Comput. Sci. Inf. Technol.*, vol. 6, no. 3, pp. 3034–3036, 2015.
[11] A. Karthikeyan, V. Srividhya, P. Gupta, and N. Rai, "A hybrid approach for simultaneous compression and encryption of an image in wireless media sensor networks," *Adv. Intell. Syst. Comput.*, vol. 452, pp. 475–484, 2016.
[12] M. Socha, Petr; Brejnik, Jan; Bartik, "Attacking AES Implementations Using Correlation Power Analysis on ZYBO Zynq-7000 SoC Board," *7th Mediterr. Conf. Conf. Embed. Comput.*, no. June, pp. 11–14, 2018.
[13] J. Cho, S. Soekamtoputra, K. Choi, and J. Moon, "Power dissipation and area comparison of 512-bit and 1024-bit key AES," *Comput. Math. with Appl.*, vol. 65, no. 9, pp. 1378–1383, 2013.
[14] N. At, J. L. Beuchat, E. Okamoto, I. San, and T. Yamazaki, "A low-area unified hardware architecture for the AES and the cryptographic hash function Grøstl," *J. Parallel Distrib. Comput.*, vol. 106, pp. 106–120, 2017.
[15] N. Thi and T. Nga, "On the improving Diffusion layer and Performance of AES algorithm," pp. 288–292, 2017.
[16] S. Guo *et al.*, "Exploiting the Incomplete Diffusion Feature: A Specialized Analytical Side-Channel Attack Against the AES and Its Application to Microcontroller Implementations," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 6, pp. 999–1014, 2014.
[17] J. Huang, H. Yan, and X. Lai, "Transposition of AES key schedule," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 10143 LNCS, pp. 84–102, 2017.
[18] A. Bogdanov, D. Khovratovich, and C. Rechberger, "Biclique cryptanalysis of the full AES," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 7073 LNCS, pp. 344–371, 2011.
[19] H. M. Hussien, Z. Muda, and Sharifah Md Yasin, "Enhance The Robustness Of Secure Rijndael Key Expansion Function Based On Increment Confusion," *6th Int. Conf. Comput. Informatics*, no. 169, pp. 722–728, 2017.
[20] J. Daemen and V. Rijmen, "The Design of Rijndael," 2002.
[21] T. F. G. Quilala, A. M. Sison, and R. P. Medina, "Modified blowfish algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 3, pp. 1027–1034, 2018.
[22] H. V. Gamido, A. M. Sison, and R. P. Medina, "Modified AES for text and image encryption," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 11, no. 3, pp. 942–948, 2018.
[23] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications,", 2010.
[24] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, pp. 617–624, 2016.