International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-11 Issue-9, August 2022

Enhancing AES with Key Dependent S-Box and Transpose MDS Matrix

S Fazila, B Reddaiah, S Sai Ramya, B J Job Karuna Sagar, C Swetha

Abstract*: Privacy is an important feature in transmission of data. Due to continuous flow of data over network, there may be a chance of attacks on sensitive data, either passive or active. To provide security, Cryptography plays a vital role by scrambling data into unreadable form. Several techniques have been developed to provide security for digital data transmission. AES is one of the efficient encryption engaged for the past decade. There is every need to improve its security mechanism periodically. In this paper we implement Transpose mix column and S-BOX Rotation to enhance efficiency. This proposed model provides more Avalanche Effect than traditional AES. Moreover, Diffusion and Confusion are crucial in Cryptography. The more the diffusion rate the more secure the data is and is shown in this proposed model. However, S-Box rotation provides more confusion. AES is most efficiently used in Wi-Fi, particularly in WPA2-PSK(AES), so enhancing security mechanism is needed.

Keywords: AES, Transpose Mix Column, S-Box Rotation, Symmetric Encryption.

I. INTRODUCTION

In recent times, communication is getting digital, such as making online transactions, online shopping, applications such as WhatsApp Messenger and Biometric Database Recognition System. The digital data is vulnerable for attacks. With this vulnerability Cyber-attacks are most common these days. So, organizations have to protect data from different types of attacks. Cryptography is the science introduced for the purpose of providing security and also provides data confidentiality. Cryptography is mainly based on three features such as Encryption, Decryption and Hashing. Scrambling of data is done using encryption process. The privacy of information is grounded on encryption, decryption and the strength of the secret key used [11]. It is the procedure of transforming original data into an obscure form. The reverse of encryption is done to retrieve original form of data from scrambled data using decryption. Cryptography is classified into two types. They are Symmetric-Key cryptography where common key is used for enciphering and deciphering and in Asymmetric cryptography a public key intended for enciphering and private key intended for deciphering [12].

A. Modern Block Ciphers

The most familiar symmetric encryption algorithms are Data Encryption Standards (DES) [13] and Advanced Encryption Standard [14]. Data Encryption Standard (DES) was developed in 1971 by IBM. It has been accepted by the National Institute of Standards and Technology (NIST)[13]. DES is fast in hardware but comparatively slow in software. The biggest difficulty of the DES is the Key size used that is of 56-bit. It has become easier to break the encrypted code in DES. As the technology is steadily improving Nowadays AES is preferred over DES. Advanced Encryption Standard (AES) also known by its original name Rijndael [5]. It is used for encrypting of electronic data. This in 2001 was recognized by U.S, National Institute of Standards and Technology. AES is a symmetric key algorithm which accepts three different key lengths. The size of key varies from 128,192 and 256 bits [14]. Substitution, Permutation and Network are the basic principles of AES. It is efficient in both software and hardware. In this paper, S-Box Rotation and Transpose Mix Column are implemented to enhance the efficiency of AES which in turn provides more avalanche effect compare to existing AES.

II. LITERATURE SURVEY

Krishnamurthy G N, V Ramaswamy [3] in 2006 proposed "Making AES Stronger: AES with Key Dependent S-Box". This version of AES doesn't adverse the AES Encryption security. Niharika Tyagi, Priyanka [5] in 2014 developed different approaches on Multimedia Communication by using Modified AES.These approaches result in reducing time and complexity. M.Pitchaiah, Philemon Daniel, Praveen [7] proposed and implemented AES algorithm on 128-bit message. Sreyam Dasgupta, Pritish Das [10] in 2019 proposed "Extended AES Algorithm with Custom Encryption for Government-level Classified Messages". The disadvantage is it operates solely on plain data. Shyam Nandan Kumar [15] proposed "A REVIEW PAPER ON CRYPTOGRAPHY AND NETWORK SECURITY", discussed several cryptography techniques and explained a few encryption approaches. It concludes that several cryptographic concepts are developing gradually. Furthermore, the proposed version produces more effectiveness [18]. Jeffrey Sorrentino [16] discussed difficulties pointed by various sectors on the digital communication attacks and determined different encryption standards.

Manuscript received on 30 July 2022 | Revised Manuscript received on 06 August 2022 | Manuscript Accepted on 15 August 2022 | Manuscript published on 30 August 2022.

***** Correspondence Author
S Fazila*, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: fazila042000@gmail.com
B Reddaiah, Department of Computer Science and Technology, Yogi Vemana University, India. Email: b.reddaiah@yogivemanauniversity.ac.in
S Sai Ramya, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: sairamya9703@gmail.com
B J Karuna Sagar, Department of Computer Science and Technology, Yogi Vemana University, kadapa, India. Email: jksagar@yahoo.com
C Swetha, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: reddyswetha95@gmail.com

Ajay Kr. Phogat, Archana Das [17] "Embedding Randomness into Symmetric Key Encryption using Genetic Algorithm". They suggested genetic algorithms for cryptanalysis and showed the advantage of such algorithms to decrypt the data. Athmane Seghier1, Jianxin Li1, Da Zhi Sun [9]in 2019 implemented an advanced version of AES, "Advanced Encryption Standard Based on Key Dependent S-Box Cube". This proposed version produces the possible S-Boxes and likely solutions around the encryption, that obstruct different cryptanalytical attacks. Besides, this improvement does not influence the standard of the adopted S-Boxes. Harpeet Singh, Paramvir Singh [8]in 2016 designed and implemented "Enhancing AES using Novel Block Key Generation Algorithm and Key dependent S-Box". Dynamic S-Boxes eradicates cryptanalytical attacks. It is beneficial in security critical systems.

III. PRELIMINARIES

Advanced Encryption Standard is a symmetric block cipher. It is developed to displace DES. Because of its high standards in providing privacy to data, it is used in different applications. AES uses different key sizes as shown in the table 1.

Table- I: AES Parameters

	Words	Bytes	Bits
Key Size	4	16	128
Plain Text Block Size	4	16	128
No. of Rounds	10		
Round Key Size	4	16	128
Expanded Key Size	44	-	176

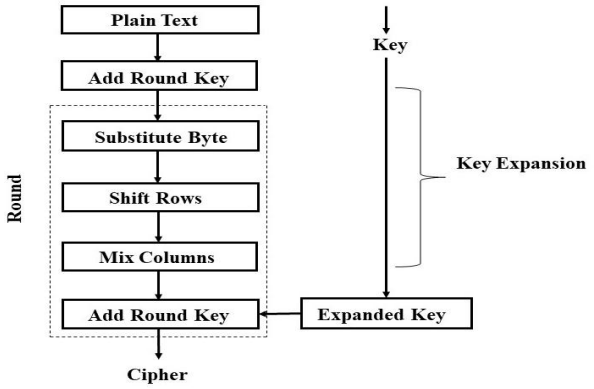

Fig.1. Advanced Encryption Standard

In AES Feistel Structure is used. Here each full round comprises of four distinct functions namely Substitution Bytes, Shift rows, mix columns and add round key. There are mainly two sections in AES. They are Key Generation and Rounds as shown in figure 1.

A. Sub Byte

Advanced Encryption Standard (AES) [1],[4] makes use of matrix with byte values. It is termed as an S-box.

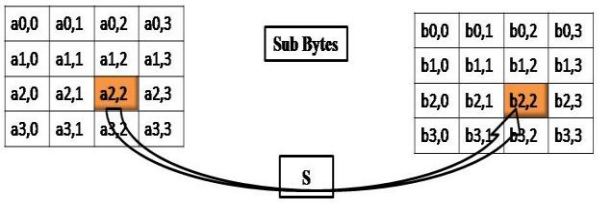

Fig.2. Sub-byte transformation

Every distinct byte of state [1],[2] is aligned into a different byte as shown in the figure 2. The left most 4 bits of the byte [2] are given as a row value. The right most 4 bits are given as column value [2]. The defined row and column value compose as entries into the S-box to choose different 8-bit value.

B. Shift Rows

Shift Rows [6] are used to perform circular left shift for the array state. The first row persists same. The next row of state [6] is rotated towards left by one byte. The third state row is rotated towards left by two bytes. Finally, the last state row is rotated towards left by three bytes as shown in figure 3.

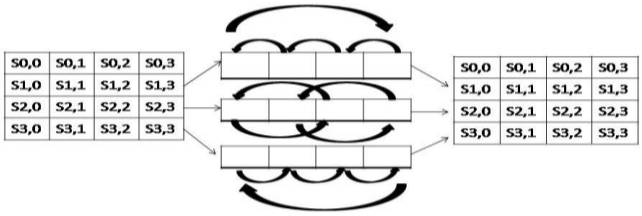

Fig.3. Shift Rows transformation

C. Mix Columns

Mix Columns are the strength of Advanced Encryption Standard (AES). Mix Columns operation is performed on column manner [4]. In Mix Columns, a predefined constant matrix and the current state are operated by applying matrix multiplication.

$$(02.S0,0) \oplus (01.S1,0) \oplus (01.S2,0) \oplus (03.S3,0)$$

D. Add Round Key

Add Round Key is a function in which bit-wise XOR operation is performed. The current state of the array and a part of the expanded key are XOR-ed. The result that is obtained is the output for that particular round. Also, it acts as an input for the next round.

IV. PROPOSED MODEL

A. Encryption Block Diagram

This proposed system is a modified AES with functions defined as S-box left rotation, Sub bytes, Shift Rows, application of transpose on MDS matrix and Add Round Key. It is shown in figure 4.

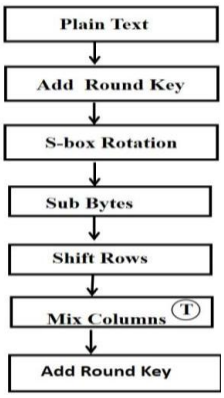

Fig.4. Modified Advanced Encryption Standard (MAES)

Retrieval Number: 100.1/ijitee.G92450811922
DOI: 10.35940/ijitee.G9245.0811922
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

B. Pseudo code for Encryption

Step 1: Cipher (input, key, output)
Step 2: Begin
Step 3: Add Round Key (input, key)
Step 4: r=XOR (derived key)
Step 5: S-box Rotation(r)
Step 6: For Round =1 to Nr-1
Step 7: Sub Bytes(input)
Step 8: Shift Rows(input)
Step 9: Transpose Mix Columns(input)
Step 10: Add Round Key(input, key)
Step 11: End For
Step 12: Sub Bytes(input)
Step 13: Shift Rows(input)
Step 14: Add Round Key(input, key)
Step 15: output=input
Step 16: End

C. Modified States for Encryption

1) S- Box Rotation

S-box are used to provide confusion. The procedure for performing S-box Rotation is as follows. The round key is derived from the actual key of AES. The obtained derived key is adapted to rotate the s-box. Hence, S-box is rotated by applying XOR on all the bytes of the derived Key as shown in figure 5.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	19	73	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E
1	0B	DB	E0	32	3A	0A	49	6	24	5C	C2	D3	AC	62	91	95
2	E4	79	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A
3	AE	8	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD
4	8B	8A	70	3E	B5	66	48	3	F6	0E	61	35	57	B9	86	C1
5	1D	9E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55
6	28	DF	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54
7	BB	16	63	7C	77	7B	F2	6B	6F	C5	30	1	67	2B	FE	D7
8	AB	76	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4
9	72	C0	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8
A	31	15	4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27
B	B2	75	9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3
C	2F	84	53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C
D	58	CF	D0	EF	AA	FB	43	4D	33	85	45	F9	2	7F	50	3C
E	9F	A8	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF
F	F3	D2	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D

Fig.5. Modified S-box

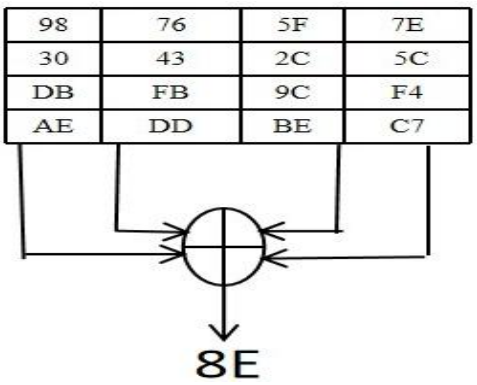

Fig.6. S-box rotation

For instance, expanded key is given as 98765F7E30432C5CDBFB9CF4AEDDBEC7. Applying XOR on all bytes we obtain 8E as the result. Hence, 8E is used to perform S-box Rotation. The obtained s-box after rotation is shown in figure 6.

2) Mix Columns

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix}^{T} = \begin{pmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{pmatrix}$$

Fig. 7. Transpose Matrix

Mix Columns is the main part of AES. It involves affine transformation on the message state. In this paper, Mix Columns is modified by applying transpose on the constant matrix. It is defined as shown in figure 7

Modified MDS Matrix is intended to provide diffusion with an increased level to that of Original AES Mix column as shown in figure 8.

$$\begin{pmatrix} 02 & 01 & 01 & 03 \\ 03 & 02 & 01 & 01 \\ 01 & 03 & 02 & 01 \\ 01 & 01 & 03 & 02 \end{pmatrix} \bullet \begin{pmatrix} S0,0 & S0,1 & S0,2 & S0,3 \\ S1,0 & S1,1 & S1,2 & S1,3 \\ S2,0 & S2,1 & S2,2 & S2,3 \\ S3,0 & S3,1 & S3,2 & S3,3 \end{pmatrix} = \begin{pmatrix} S'0,0 & S'0,1 & S'0,2 & S'0,3 \\ S'1,0 & S'1,1 & S'1,2 & S'1,3 \\ S'2,0 & S'2,1 & S'2,2 & S'2,3 \\ S'3,0 & S'3,1 & S'3,2 & S'3,3 \end{pmatrix}$$

Fig.8. Transpose Mix Columns

D. Decryption Block Diagram.

The decryption process with S-box rotation, Sub bytes, Shift Rows, application of inverse transpose on MDS matrix and Add Round Key is shown in figure 9.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

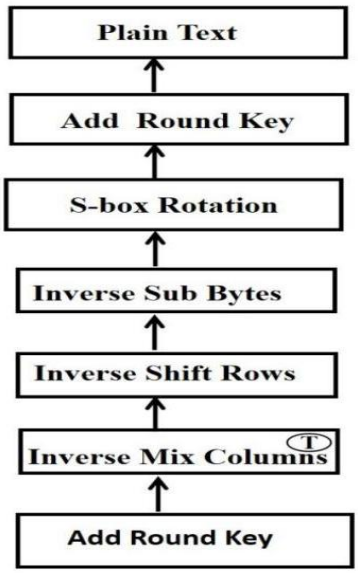

Fig 9. Modified Advanced Decryption Standard (MAES)

E. Pseudo code for Decryption

Step 1: Cipher (input, key, output)
Step 2: Begin
Step 3: Add Round Key (input, key)
Step 4: r=XOR (derived key)
Step 5: Inverse S-box Rotation(r)
Step 6: For Round =1 to Nr-1
Step 7: Inverse Sub Bytes(input)
Step 8: Inverse Shift Rows(input)
Step 9: Inverse Transpose Mix Columns(input)
Step 10: Add Round Key(input, key)
Step 11: End For
Step 12: Inverse Sub Bytes(input)
Step 13: Inverse Shift Rows(input)
Step 14: Add Round Key(input, key)
Step 15: output=input
Step 16: End

F. Modified States for Decryption

1) Inverse Mix Column

In decryption, inverse mix columns are performed by applying transpose on the constant matrix defined by existing AES. The transformation applied on inverse mix columns is defined as shown in figure 10.

$$\begin{pmatrix} 0E & 09 & 0D & 0B \\ 0B & 0E & 09 & 0D \\ 0D & 0B & 0E & 09 \\ 09 & 0D & 0B & 0E \end{pmatrix} \bullet \begin{pmatrix} S'0,0 & S'0,1 & S'0,2 & S'0,3 \\ S'1,0 & S'1,1 & S'1,2 & S'1,3 \\ S'2,0 & S'2,1 & S'2,2 & S'2,3 \\ S'3,0 & S'3,1 & S'3,2 & S'3,3 \end{pmatrix} = \begin{pmatrix} S0,0 & S0,1 & S0,2 & S0,3 \\ S1,0 & S1,1 & S1,2 & S1,3 \\ S2,0 & S2,1 & S2,2 & S2,3 \\ S3,0 & S3,1 & S3,2 & S3,3 \end{pmatrix}$$

Fig.10. Inverse Mix Columns

The equation for inverse mix columns is defined as

$$(0E.S'0,0) \oplus (09.S'1,0) \oplus (0D.S'2,0) \oplus (0B.S'3,0)$$

2) Inverse Sub Byte

Inverse Sub Byte is same as actual AES Inverse Sub Byte. However, decryption of a byte say x_{ij} is done using, x_{ij} = (Inverse (y_{ij}) - S-box Rotation value) mod 256.

For instance, to find the inverse of 71 it is performed as follows

(Inv(71)- 0E) mod 256 = (2C - 0E) mod 256=1E.

V. RESULT

This paper is successfully completed by implementing encryption and decryption algorithm of AES. This implementation provides more avalanche effect. It is shown in figure The steps included in this modified AES are S-Box Rotation, Sub byes, Shift Rows Transformation, Transpose MDS Matrix and Add Round Key. The encryption process for the above- mentioned steps is shown in table 1 with an example. The Decryption Process for this modified AES is Inverse MDS Matrix, Inverse Sub Byte, Inverse Shift Rows Transformation, Inverse MDS Matrix and Add Round Key. The calculated values for encryption is shown in table II.

Table-II: Encryption Process

Key	Plain Text	Add Round Key	Sub Byte	Shift Rows	Transpose Mix Column	Add Round Key	Cipher Text
49	57	1E	71	71	07	B6	B6
6D	68	05	7D	C9	77	88	88
70	61	11	C0	C0	07	C1	C1
72	74	06	FA	AD	A2	90	90
6F	61	0E	9C	9C	70	AE	AE
76	72	04	C9	72	95	1C	1C
65	65	00	AB	34	98	3B	3B
64	79	1D	F1	FA	5D	0B	0B
53	6F	3C	D6	D6	38	B5	B5
65	75	10	72	47	DE	32	32
63	72	11	C0	C0	75	B5	B5
75	70	05	7D	F1	33	10	10
72	6C	1E	71	71	B3	4C	4C
69	61	08	47	7D	BF	3A	3A
74	6E	1A	34	AB	C6	72	72
79	73	0A	AD	7D	10	4A	4A

A. Diffusion

The purpose of diffusion is to obscure the connection between the cipher text and the plain text. That means, if a single bit of the plain text, then there must have a great impact and the diffusion rate is shown in figure 11 where the new proposed method is more effective than traditional AES.

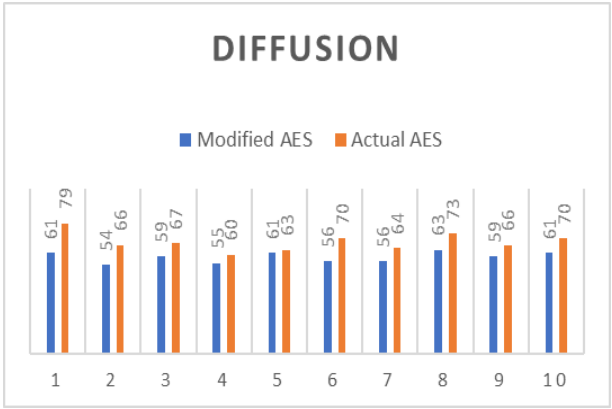

Fig. 11. Diffusion

Retrieval Number: 100.1/ijitee.G92450811922
DOI: 10.35940/ijitee.G9245.0811922
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

B. Diffusion

Avalanche Effect is one of the distinguished metrics in cryptography. Avalanche Effect states that a small change in the plain text must have a great impact in several bits of cipher text. Avalanche Effect is defined as

$$\text{Avalanche Effect (A.E)} = \frac{\text{No. of bits changed}}{\text{Total No. of bits}} \times 100$$

Figure 12 shows the difference between proposed method and the actual AES. It is proved that the modified AES is stronger that actual AES.

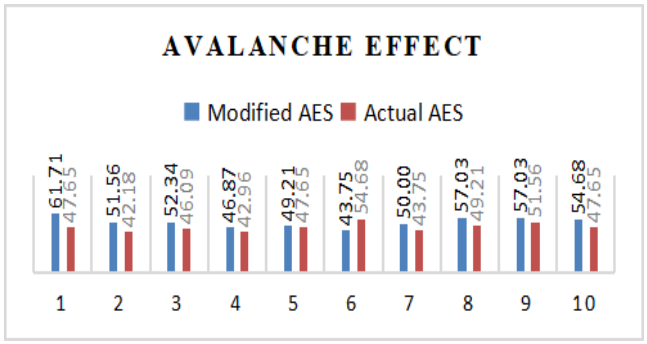

Fig. 12. Avalanche Effect

C. Confusion

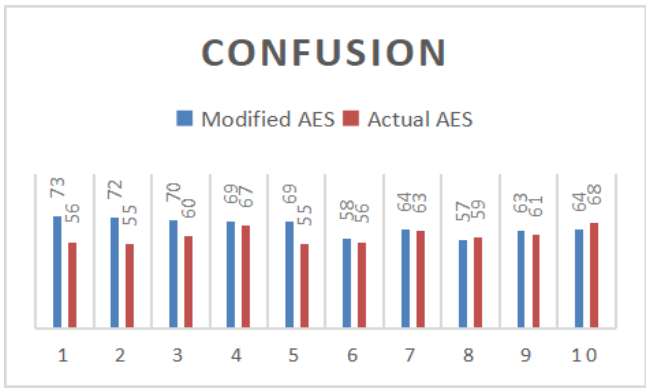

Fig.13. Confusion

Confusion property obscures the connection between the key and the cipher text. It builds it complex to find the key from the cipher text. That means, a single bit change in key should have a great change in cipher text. The confusion rate and Avalanche effect is far better than actual AES in modified AES and is shown in figure 13 and 14

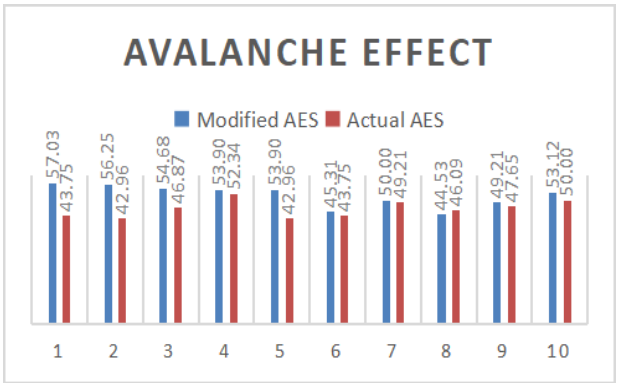

Fig.14. Avalanche Effect

The calculated values for decryption is shown in table III.

Table-III: Decryption Process.

Key	Cipher Text	Add Round Key	Inverse MDS Matrix	Inverse Shift Rows	Inverse Sub Bytes	Add Round Key	Plain Text
49	B6	07	71	71	1E	57	57
6D	88	77	C9	7D	05	68	68
70	C1	07	C0	C0	11	61	61
72	90	A2	AD	FA	06	74	74
6F	AE	70	9C	9C	0E	61	61
76	1C	95	72	C9	04	72	72
65	3B	98	34	AB	00	65	65
64	0B	5D	FA	F1	1D	79	79
53	B5	38	D6	D6	3C	6F	6F
65	32	DE	47	72	10	75	75
63	B5	75	C0	C0	11	72	72
75	10	33	F1	7D	05	70	70
72	4C	B3	71	71	1E	6C	6C
69	3A	BF	7D	47	08	61	61
74	72	C6	AB	34	1A	6E	6E
79	4A	10	7D	AD	0A	73	73

VI. DISCUSSION

The comparison in figure 11 and 12 shows the diffusion rate and Avalanche Effect for both actual and modified AES. The proposed AES has effective diffusion rate compared with actual AES as shown in blue lines in the graph. From Figure 5.2, it is shown that how the bits are flipped for each round of AES. In Figure 13, the confusion rate is calculated and represented graphically for both actual and modified AES. Furthermore, it is clearly seen that the modified AES has more confusion rate. Hence, Avalanche Effect for confusion is shown in figure 14, It shows how the number of bits are flipped for each round of actual AES and Modified AES.

VII. CONCLUSION

In this paper, an enhanced AES is implemented. It is focused on S-Box Rotation and Transpose MDS Matrix. This S-Box Rotation procedure initially performed by applying Exclusive-XOR on all bytes derived key. Hence, the result obtained after XOR is used to rotate S-box which in turn construct a new S-Box. This enhancement provides more confusion for AES. From the calculated results, it is ended that the implemented model gives an effective result compared with actual AES. Furthermore, Mix Columns is the prominent function of AES. It is intended to provide diffusion over bits. In proposed method, mix column function is modified by applying transpose operation on MDS Matrix of AES. This enhancement provides more diffusion rate compared with actual AES. Moreover, Avalanche effect, which is an effective test in cryptography is calculated for both actual AES and modified AES. The results that are derived concludes Modified AES has more avalanche effect.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

1. Ako Muhamad Abdullah, " Advanced Encryption Standard(AES) Algorithm to Encrypt and Decrypt Data" , 16 June 2017
2. National Institute of Standards and Technology. Advanced Encryption Standard. Federal Information Processing Standard (FIPS),Publication 197, U.S. Department of Commerce, Washington D.C., November 2001.
3. Krishnamurthy G N, V Ramaswamy , "Making AES Stronger: AES with Key Dependent S-Box" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, September 2008.
4. Daemen, Joan; Rijmen, Vincent (March 9, 2003). "AES Proposal: Rijndael" (PDF). National Institute of Standards and Technology. p. 1. Archived (PDF) from the original on 5 March 2013. Retrieved 21 February 2013.
5. Niharika Tyaga 1,Priyanka, "A Survey on Ensemble of Modifications on AES Algorithm" Journal of Basic and Applied Engeneering Research Print ISSN: 2350-0077;Online ISSN:2350-0255;Volume 1,Number 7;October, 2014 pp.19-2
6. SistlaVasundhara Devi and Harika Devi Kotha,, "AES encryption and decryption standards" International conference on computer vision and machine learning . IOP Conf. Series: Journal of Physics: Conf. Series 1228(2019) 012006 [CrossRef]
7. M.Pitchaiah, Philemon Daniel, Praveen,"Implementation of Advanced Encryption Standard Algorithm"International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 ISSN 2229-5518
8. Harpreet Singh, Paramvir Singh, "Enhancing AES using Novel Block Key Generation Algorithm and Key Dependent S- boxes" International Journal of Cyber- Security and Digital Forensics 5(1):30-45 [CrossRef]
9. Athmane Seghier1, Jianxin Li1, Da Zhi Sun, "Advanced encryption standard based on key dependent S-Box cube" IET Information Security Research Article ISSN 1751-8709.
10. Sreyam Dasgupta, pritish Das "Extended AESTAlgorithm withTCustomT Encryption for Government- level Classification Messages", International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue -8,June, 2019.
11. Behrouz A. Forouzan, Cryptography and Network Security, Special Indian Edition, TATA McGraw Hill
12. www.webopedia.com/TERM/S/symmetric_key_cryptography.html
13. G. Singh, Supriya, "A study of encryption algorithms (RSA, DES, 3DES and AES) for Information Security," International Journal of Computer Applications, vol. 67, no. 19, pp. 33-38, April 2013 [CrossRef]
14. W. Burr, "Selecting the Advanced Encryption Standard," IEEE, vol. 1, no. 2, pp. 43-52, 2003. [CrossRef]
15. Kumar, Shyam Nandan ,"Review on Network Security and Cryptography", International Transaction of Electrical and Computer Engineers System, 2015, Vol. 3
16. Sorrentino, Jeffrey, "Information Security: An Introduction to Cryptography"
17. Phogat, Ajay Kr., Das,Archana,"A Symmetric Cryptography Based on Extended Generic Algorithm". International Journal of Current Trends in Engineering and Research, Volume 22, Issue 4, April 2016
18. Shyam Nandan Kumar, "Technique for Security of Multimedia using Neural Network," Paper idIJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

AUTHORS PROFILE

S Fazila is pursuing M.Sc Computer Science from department of Computer Science and Technology in Yogi Vemana University, Kadapa. Areas of interest are cyber Security and Web Development. Secured Rank-1 in PGCET-2020. I am a Self-learner and passionate to explore new things. I am interested to do research in the field of cyber security.

B Reddaiah is working as Assistant Professor in department of computer science and technology, Yogi Vemana University, Kadapa, driven to inspire students to pursue academic and personal excellence. Areas of research and interest is in Network Security and Software Engineering. I published 35 papers in various international journals and published 15 papers in different international conferences.

S Sai Ramya is pursuing M.Sc Computer Science from department of Computer Science and Technology in Yogi Vemana University. Areas of interest are Software Engineering and Cyber security. I am interested to do research in the filed of cyber security and Software Engineering. I am a Hard worker and punctual towards my work. I gave many seminars and received certifications.

Dr. B.J.Job karuna sagar has 18 years of experience in teaching and research. Areas of interest are Network Security, Hybrid routing protocols. I published papers in various journals. My core research area is Adhoc Sensor Networks. I published 15 papers in various international journals and published 5 papers in different international conferences.

C Swetha has 15 years of experience in teaching and research. Area of interest is Software Engineering. My core research area is Cloud Computing. she published 10 papers in various international journals and published 5 papers in different international conferences.