IMPROVEMENT OF ADVANCED ENCRYPTION STANDARD ALGORITHM USING ROW TRANSFORMATION AND 200 BIT DATA BLOCK

Kirti Prakash Choudhury[1], Sangeeta Kakoty[2], Lakshmi Prasad Saikia[3]
[1]*Research Scholar, Computer Science & Engineering, Assam down town University, Assam, India*
[2]*Dy. Director - Multimedia, Krishna Kanta Handiqui State Open University, Assam, India*
[3]*Professor, Computer Science & Engineering, Assam down town University, Assam, India*
([1]choudhurykirti@gmail.com, [2]kakoty.sangeeta@gmail.com, [3]lp_saikia@yahoo.co.in)

Abstract - In today’s modern world security of data has become one of the most important factor in our technological life. The main objective of this paper is to provide stronger security with higher encryption speed for data communication over the Internet by modifying the Advanced Encryption Standard (AES) algorithm. This paper suggests a new Advanced Encryption Standard encryption technique that provides a stronger encryption technique by enhancing its security and encryption speed. This new algorithm uses 200 bit size data block as well as key in a 5 x 5 matrix format alongwith an additional Row Transformation stage before the shift row stage for each round in the AES algorithm structure. The proposed algorithm can improve security and also enhance the speed of the encryption process.

Keywords - *AES Algorithm; Block cipher; Decryption; Encryption; Modulo Division; Row Transformation; S-Box.*

I. INTRODUCTION

With the rapid growth of information and technology, protection of data during transmission or while in storage becomes an increasing demand for maintaining the confidentiality and integrity of the information represented by the data. Different cryptographic protocols are playing an important role in preserving the confidentiality and integrity of the data transmitted over public communication networks. Advanced Encryption Standard (AES) is one of the strongest Symmetric Cryptographic protocols which are widely used by different govt agencies, financial institutions, and different kind of offices to securely encrypt their important private data. AES is a block cipher with 128 bit block size and supported by three cipher key lengths of 128, 192 and 256 bit that provides high level security in comparison to other symmetric cryptographic protocols. This research is concerned with optimizing security of the existing AES cryptographic protocol without compromising with its encryption speed. The proposed modified AES uses 200 bit block size of data and same size of key in 5 x 5 matrix format alongwith an additional Row Transformation stage before the shift row activity for each round is added. This additional Row Transformation stage and big 200 bit data block size will indubitably make the algorithm more secure and more efficient by improving its speed.

II. ADVANCED ENCRYPTION STANDARD

The Advanced Encryption Standard is based on the Rijndael cipher developed by Joan Daemen and Vincent Rijmen and was adopted by National Institute of Standards and Technology (NIST) of the United States on 26th November, 2001 as new symmetric encryption algorithm. In this standard, cipher has a 128-bit data block size and it uses three different key length sizes of 128 bits, 192 bits, 256 bits respectively. Each data block of 128 bit data is divided into 16 Bytes. These bytes are mapped to a 4 x 4 array called as the state and all operations of AES are performed on this state. [1] The AES comprises several rounds for full encryption of data and the total number of rounds (Nr = 10, 12, 14) depends upon the key length (Nk). For encryption, each round of AES has four stages namely – Substitute bytes, Shift rows, Mix columns, and Add round key. In the encryption procedure, the AddRoundKey stage starts at first and it is followed by (Nr-1) nos. of rounds, each round contains four stages. The last round of encryption contains only three stages. The decryption procedure can be seen as inverse of encryption procedure and it comprises of also four stages namely InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey.

III. RELATED WORK

The Advanced Encryption Standard provides good encryption-decryption speed, throughput alongwith high security. But, lots of researches are going on to improve AES algorithm to enhance its security and encryption-decryption speed.

Ritu and Vikas proposed a symmetric cryptographic technique AES (Advance encryption standard) having 200 bit block as well as key size using 5 x 5 Matrix. Then the proposed work is compared with 128 bit, 192 bits & 256 bits AES techniques on two points. These points are encryption and decryption time and throughput at both encryption and decryption sides. Encryption speed and throughput at encryption side is increased and decryption speed, throughput at decryption side is decreased than standard AES Algorithm.[2]

S. Sankaran, S. Ambhore and P. Vincent proposed a Advance Encryption Standard having 200 bit block as well as key size using 5 x 5 Matrix and a key dependent substitution box which varies according to the 200 bit key provided by the user. The new suggested varying substitution box provides a better and secure way to the encryption of data. Substitution box is being varied using s-box rotation based on the key used for encryption. [3]

S. Shekhar, P. Singh and M. Jaiswa suggested a new modified symmetric Advance Encryption Standard that uses a 128 bit size block encryption scheme and also include a Row Transformation before the shift row activity for each round. This modification indubitably increases the complexity of the system which raises security. [4]

A.K. Dandekar, S. Pradhan and S. Ghormade used a 512 bit length in order to improve security for high security required application. Key length is increased to 512 bit alongwith the number of rounds which provide required higher security. [5]

R. Riyaldhia, Rojalia and A. Kurniawan proposed a method to improve AES algorithm with Shift Row and S-Box modification for Mix Column transformation. This modification shows that improvement that has been made by reducing shift row circular process and S-Box modification for Mix Column transformation but consume bigger memory to store two modified S-Box map and Array Shift Row map. [6]

Vandana C. Koradia modified symmetric Advance Encryption Standard by replacing Mix Column step with the Initial Permutation step taken from DES to increase the encryption speed for large file. [7]

IV. PROPOSED MODEL

The proposed model of Advanced Encryption Standard algorithm works exactly in the same way as the conventional AES with some structural changes in its data block size and numbers stages in each round of iteration. This new algorithm proposed to use 200 bit data block in an array of 5 X 5 matrix format and inclusion of an additional Row Transformation stage before the shift row activity for each round. The cipher key used in this algorithm is also 200 bit size. To make this algorithm more secure, one extra stage for calculation in each round is added. In this modified algorithm, encryption process contains five stages namely – Substitute bytes, Row Transformation, Shift rows, Mix columns, and Add round key. The AddRoundKey stage starts at first and it is followed by nine rounds, each round contains five stages. The last round of encryption contains only four stages. The following block diagram represents the new modified AES algorithm and the various stages of encryption are discussed below.

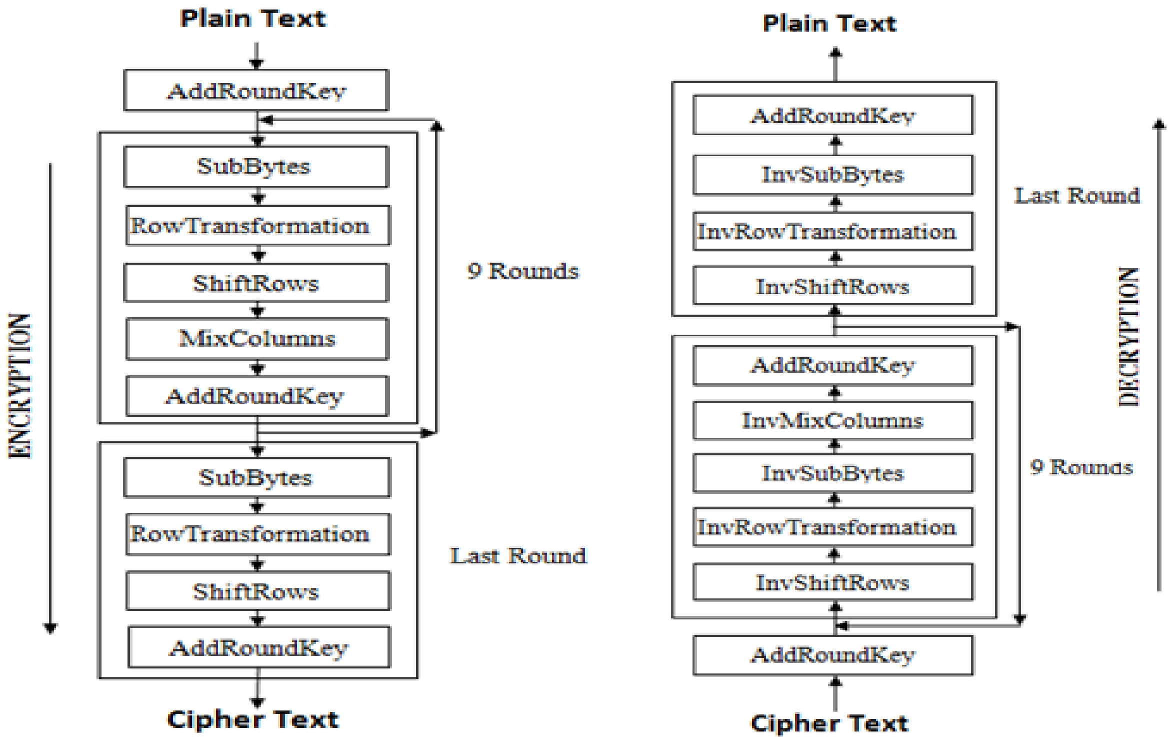
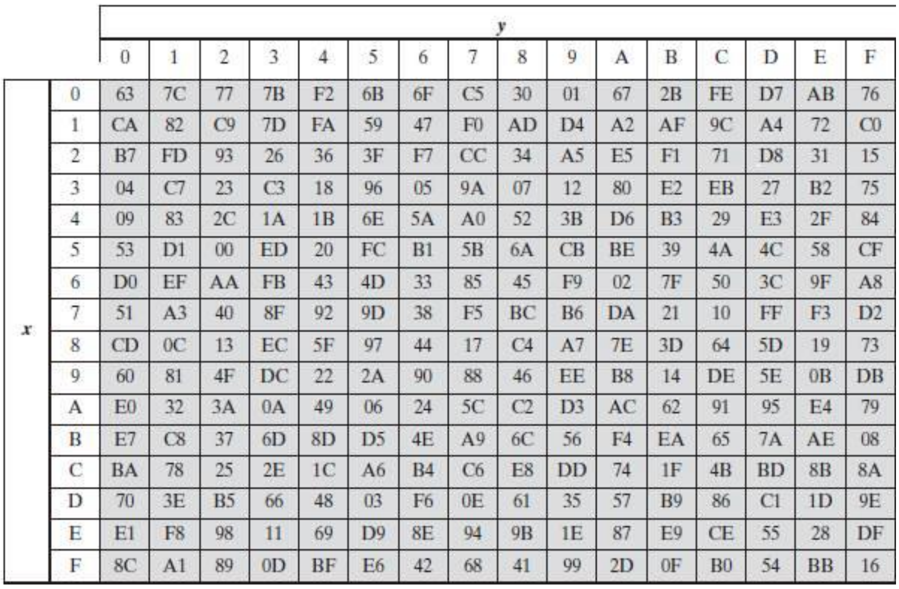


Fig. 1: Block Diagram of Main Steps of Modified AES

A. *SubBytes Transformation*

In this transformation, each byte of input data in the state matrix is replaced with another byte using a 16 x 16 lookup table called Substitution table (S-box). The substitution box is constructed by calculating respective reciprocal of that byte in GF (2^8) at first and then affine transformation is applied. [2] This is the only non linear stage which introduces *confusion* to the data, i.e., it assures that changes in individual state bits propagate quickly across the data path. [8]. The S-box used in this transformation is shown below.



		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Fig. 2: The S-box of AES [3]

B. *Row Transformation*

In this proposed algorithm, another Row Transformation is additionally included before the shift row activity for each round in the encryption process. Inclusion of this stage improves the complexity level of AES, which makes AES more secure. The last number in each row of 5 x 5 matrixes is considered to be decimal number, which modulo division by 10 gives the reminder value. This reminder value is further subtracted from the other numbers of that row.[4] This process continues for each row of the 5 x 5 matrix and provides a new 5 x 5 matrix array. The working of this stage is shown with an example.

Suppose a 200 bit size block of data in a 5 x 5 matrix is –

$$\begin{pmatrix} 17 & 7 & 8 & 22 & 16 \\ 9 & 11 & 45 & 25 & 4 \\ 27 & 5 & 19 & 20 & 35 \\ 43 & 7 & 18 & 8 & 1 \\ 11 & 15 & 27 & 3 & 12 \end{pmatrix}$$

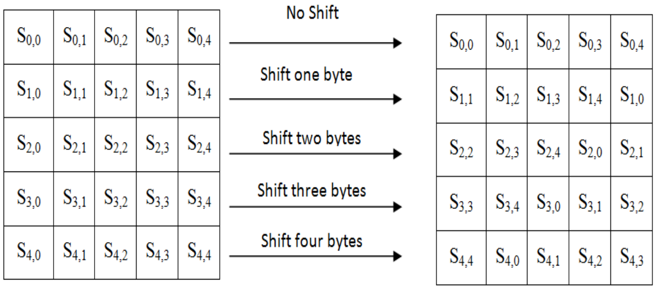
Modulo division by 10 of the last number (i.e. 16) of the first row gives us the last digit or reminder value which is 6 here (i.e. 16 % 10 = 6). Further, the last digit (i.e. 6) is subtracted from the other numbers of the first row. Continuing this process on other rows, we will get a new 5 x 5 matrix that is shown below:

$$\begin{pmatrix} 11 & 1 & 2 & 16 & 16 \\ 5 & 6 & 41 & 21 & 4 \\ 22 & 0 & 14 & 15 & 35 \\ 42 & 6 & 17 & 7 & 1 \\ 9 & 13 & 25 & 1 & 12 \end{pmatrix}$$

In the decryption, the inverse operations will be carried out. The last digit will be added with all corresponding number in the row except the last number.

C. *ShiftRows Transformation*

In this transformation of the proposed new algorithm, five ShiftRow operations occur instead of four ShiftRow operations performed in Rijndael algorithm. The ShiftRows transformation cyclically shifts the second, third, fourth and fifth row of the state matrix by one, two, three and four bytes respectively to the left. But, the bytes in the first row are not shifted in this transformation. This transformation is illustrated in Fig. 3



$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$	$S_{0,4}$	No Shift	$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$	$S_{0,4}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,4}$	Shift one byte	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,4}$	$S_{1,0}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$	$S_{2,4}$	Shift two bytes	$S_{2,2}$	$S_{2,3}$	$S_{2,4}$	$S_{2,0}$	$S_{2,1}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$	$S_{3,4}$	Shift three bytes	$S_{3,3}$	$S_{3,4}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$
$S_{4,0}$	$S_{4,1}$	$S_{4,2}$	$S_{4,3}$	$S_{4,4}$	Shift four bytes	$S_{4,4}$	$S_{4,0}$	$S_{4,1}$	$S_{4,2}$	$S_{4,3}$

Fig. 3: The ShiftRows Transformation.

D. *MixColumns Transformation*

The MixColumn step is a linear transformation which mixes each column of the state matrix. Since every input byte influences four output bytes, the MixColumn operation is the major diffusion element in AES. [8] This transformation mixes the bytes in each column by the multiplication of the state with a fixed 5 x 5 polynomial matrix [2]. Here, a 5 x 5 polynomial matrix is used instead of 4 x 4 matrix and so, the values of cells of the polynomial are also changed. The polynomial used in the multiplication is $2x^4 + 4x^3 + 3x^2 + x + 1$

The polynomial matrix used in mixed column step for encryption is shown below:-

$$\begin{pmatrix} 02 & 04 & 03 & 01 & 01 \\ 01 & 02 & 04 & 03 & 01 \\ 01 & 01 & 02 & 04 & 03 \\ 03 & 01 & 01 & 02 & 04 \\ 04 & 03 & 01 & 01 & 02 \end{pmatrix}$$

And the corresponding inverse polynomial matrix for decryption is shown below:-

$$\begin{pmatrix} E0 & 7D & 09 & 8A & 4C \\ 4C & E0 & 7D & 09 & 8A \\ 8A & 4C & E0 & 7D & 09 \\ 09 & 8A & 4C & E0 & 7D \\ 7D & 09 & 8A & 4C & E0 \end{pmatrix}$$

E. *AddRoundKey Transformation*

In this transformation, bitwise Exclusive-OR (XOR) operation is performed between the state and the Roundkey. This transformation is its own inverse.

Like the conventional AES, the decryption procedure of this modified AES is also exactly the inverse of encryption procedure and it contains of five stages namely InvSubBytes, InvRowTransformation, InvShiftRows, InvMixColumns, and AddRoundKey.

V. CONCLUSION

Advanced Encryption Standard is one of the fastest security algorithms which provide good security. But still researchers are trying to get better security with better encryption and decryption speed through modifications of AES. This proposed model is going to make AES more secure by adding the additional Row Transformation step. But inclusion of this additional stage will not reduce its encryption / decryption speed rather encryption / decryption speed will be increased due to uses of 200 bit big data block size. Also, the combination of 200 data bit block AES with additional Row Transformation will increase the stability and efficiency of AES. By implementing this, we can compare its efficiency with AES-128 which will be our future work.

ACKNOWLEDGMENT

Authors acknowledge the immense help received from the scholars whose articles are cited and included in references of this manuscript. The authors are also grateful to authors / editors / publishers of all those articles, journals and books from where the literature for this article has been reviewed and discussed. The first author also acknowledges the academic support given by Assam down town University (AdtU), Guwahati, Assam, India.

REFERENCES

[1] F.R. Patel, Dr. A.N. Cheeran, "Performance Evaluation of Steganography and AES encryption based on different formats of the Image," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4 , Issue No.5, Page 659-664, 2015, ISSN (Online) 2278-1021 ISSN (Print) 2319-5940, DOI 10.17148/IJARCCE.2015. 45140 664. Retrieved from https://www.ijarcce.com/ upload/2015/may-15/IJARCCE% 20140 .pdf

[2] R. Pahal, V. Kumar, "Efficient Implementation of AES," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3 , Issue No.7, 2013, Page 290-295, ISSN: 2277 128X. http://ijarcsse.com/BeforeAugust2017/docs/papers/ Volume3/7July2013/V3I7-0246.pdf

[3] S. Sankaran, S. Ambhore, P. Vincent, "Modified Advanced Encryption Standard with Additional Row Transformation," International Journal of Pharmacy & Technolog, Vol. 8 , Issue No.3, 2016, Page 16436-40, ISSN: 0975-766X, www.ijptonline.com

[4] S. Shekhar, P. Singh, M. Jaiswal, "An Enhanced AES Algorithm Based on Variable Sbox And 200 Bit Data Block," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4 , Issue No.4, 2016, Page 6470-6477, ISSN (Online) : 2320-9801 ISSN (Print) : 2320-9798, DOI: 10.15680/IJIRCCE.2016. 0404026

[5] A.K. Dandekar, S. Pradhan, S. Ghormade, "Design of AES-512 Algorithm for Communication Network," International Research Journal of Engineering and Technology (IRJET), Volume. 3, Issue No.5, 2016, Page 438-443, e-ISSN: 2395-0056.https://www.irjet.net/archives/V3/i5/IRJET-V3I592.pdf

[6] R. Riyaldhia, Rojalia, A. Kurniawan, "Improvement of advanced encryption standard algorithm with shift row and s.box modification mapping in mix column," 2nd International Conference on Computer Science and Computational Intelligence 2017, ICCSCI, Bali, Indonesia Procedia Computer Science, Page 401–407, www.sciencedirect.com

[7] V.C. Koradia, "Modification in Advanced Encryption Standard," Journal of Information, Knowledge, and research in Computer Engineering, Vol. 2, Issue. 2, 2012-13, pp. 356-358, ISSN: 0975–6760. http://www.ejournal.aessangli.in/ASEEJournals/CE73.pdf

[8] Christof Paar, Jan Pelzl, "Understanding Cryptography," Springer Heidelberg Dordrecht London New York ACM Computing Classification, 1998,ISBN 978-3-642-04100-6 e-ISBN 978-3-642-04101-3, DOI 10.1007/978-3-642-04101-3

Kirti Prakash Choudhury, Research Scholar, Computer Science & Engineering, Assam down town University, Assam, India

Dr. Sangeeta Kakoty, Dy. Director - Multimedia, Krishna Kanta Handiqui State Open University, Assam, India

Dr. Lakshmi Prasad Saikia, Professor, Computer Science & Engineering, Assam down town University, Assam, India