DOI: https://doi.org/10.53555/nncse.v2i1.508 **Publication URL: http://nnpub.org/index.php/CSE/article/view/508**

AN APPROACH TO RIJNDAEL ALGORITHM

Ms. J. V. Shiral*[1], Ms. R. C. Deshmukh[2], Mr.J. S. Zade[3], Mrs. A. Potnurwar[4]
*[1]*Asst. Prof., CSE Dept, DBACER, Nagpur, Maharashtra*
[2]Asst. Prof., CSE Dept, DBACER, Nagpur, Maharashtra
[3]CSE Dept, GHRCE, Nagpur, Maharashtra
[4]Prof., IT Dept, PIET, Nagpur, Maharashtra

Corresponding Author: -

Abstract: -

Rijndael or Advanced Encryption Standard (AES) is the most secure symmetric encryption technique and is available in many different encryption packages. The AES based on the Rijndael Algorithm is an efficient cryptographic technique that includes generation of ciphers for encryption and inverse ciphers for decryption. High security and speed of encryption and decryption is ensured by various operations. It has been standardized by the National Institute of Standards and Technology of the United States (NIST) and comprises three block ciphers, AES-128, AES-192 and AES-256 and it is adopted from Rijndael algorithm. This paper presents a encryption and decryption process of the rijindael algorithm. The paper also explains the comparative study of various rijindael algorithms with other algorithms based on the various parameters.

Index terms: - *Rijndael algorithm, DES, AES, Blowfish, Encryption, Decryption. Rijndael, encryption-decryption.*

I. INTRODUCTION

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Encryption is the process of converting normal text to unreadable form i.e ciphertext. Decryption is the process of converting encrypted text to normal text i.e ciphertext in the readable form [8].

Symmetric encryption is a form of cryptography using a single encryption key which recognizes an electronic message. It processes data conversion which uses a mathematical algorithm alongwith a secret key which in turn results in the inability to make sense out of a message. Here, symmetric encrpytion is also called as two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key. Fig 1. Shows the symmetric key encryption and decryption process [8].

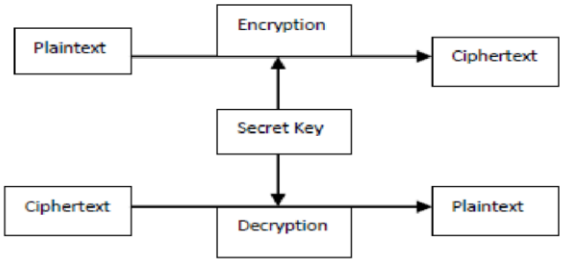

Figure 1: Symmetric Key Cryptography Process

II. REASONS FOR USE OF SYMMETRIC APPROACH FOR ENCRYPTION AND DECRYPTION

- Encryption process is very simple.
- Two communicating parties can use the same encryption algorithm, to develop and exchange secret algorithms is not necessary.
- Security is dependent on the length of the key, large key size provides more security.
- High data rates throughput which provides high performance rate.
- Symmetric key ciphers is useful to construct various cryptographic mechanisms.
- Symmetric key ciphers is used in combination with other algorithms to produce stronger ciphers

III. RIJNDAEL ALGORITHM

The Rijndael (AES) algorithm uses a symmetric key block cipher both in encryption and decryption. A prime feature of Rijndael is its ability to operate on varying sizes of keys and data blocks. It provides additional flexibility in that both the block size and the key size. At the start of encryption, input is copied to the array. The encryption algorithm encrypts one block of data at a time to produce the encrypted data block with the use of a secret key. The decryption is the reverse process of the encryption and each operation is the inverse of the corresponding one as in encryption. The data block length is fixed to 128 bits, while the key length can vary from 128, 192, or 256 bits. Each data block is rearranged in a matrix form. AES algorithm is an iterative algorithm and each iteration is called a round. Fig 2. gives the clear idea [3].

Type	Block Size Nbwords	Key Length Nkwords	Number of Rounds Nr
AES -128 bits key	4	4	10
AES -192 bits key	4	6	12
AES -256 bits key	4	8	14

Fig 2: Comparison between various AES

Each round uses four transformations and inverses but final round excludes Mix Column transformations. To encipher a block of data in Rijndael, an Add Round Key step is performed by XORing a subkey with the block or by itself, then the regular transformation rounds, and finally a final round with the Mix Column step is removed. The cipher itself is defined by the following steps:

- an initial Round Key addition;
- N^r-1 Rounds;
- a final round.

Following Figure 3 shows the flow of AES Encryption and Decryption algorithm [5]

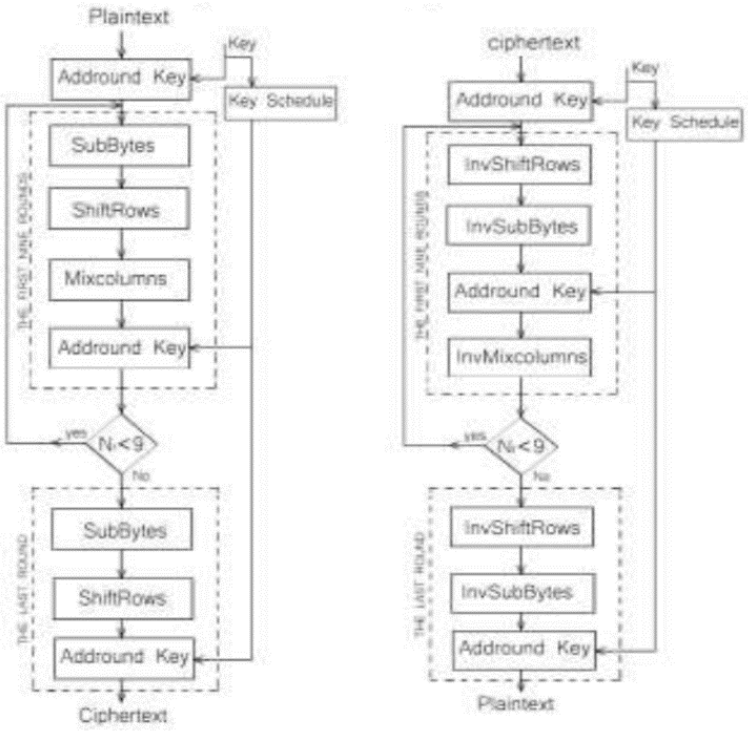

Fig 3: AES Encryption and Decryption process

IV. Rijndael Algorithm operation

The AES is a cryptographic algorithm that is used to encrypt (encipher), and decrypt, (decipher), information. Key Expansion generates a Key Schedule that is used in Cipher and Inverse Cipher procedures. Cipher and Inverse Cipher are composed of specific number of rounds. The number of rounds to be performed during the execution of the algorithm is dependent on the key length. The four transformations used in each round are [1]:

(i) SubBytes : Every element of State array is first inverted and processed through an affine transformation. SubBytes transformation is performed on each byte of the State array. In most of the practical applications SubBytes is calculated in advance and stored in a look-up table called Sbox of 2 8 = 256 elements.

(ii) ShiftRows : The rows in State array are rotated. The byte in first row is not shifted whereas second, third and fourth row is shifted left by one byte cyclically.

(iii) MixColumns: MixColumns is a linear transformation and is done on the State array by column by column. Each transformed byte is a linear combination of the state matrix.

(iv) AddRoundKey: Every 128-bit round key is divided in to 16 bytes as of data block. AddRoundKey is a linear transformation. A round key is added to the State array by bitwise Exclusive-OR (XOR) operation. Key is used as initial set of bytes in each row and the rest of the bytes are generated from the key iteratively.

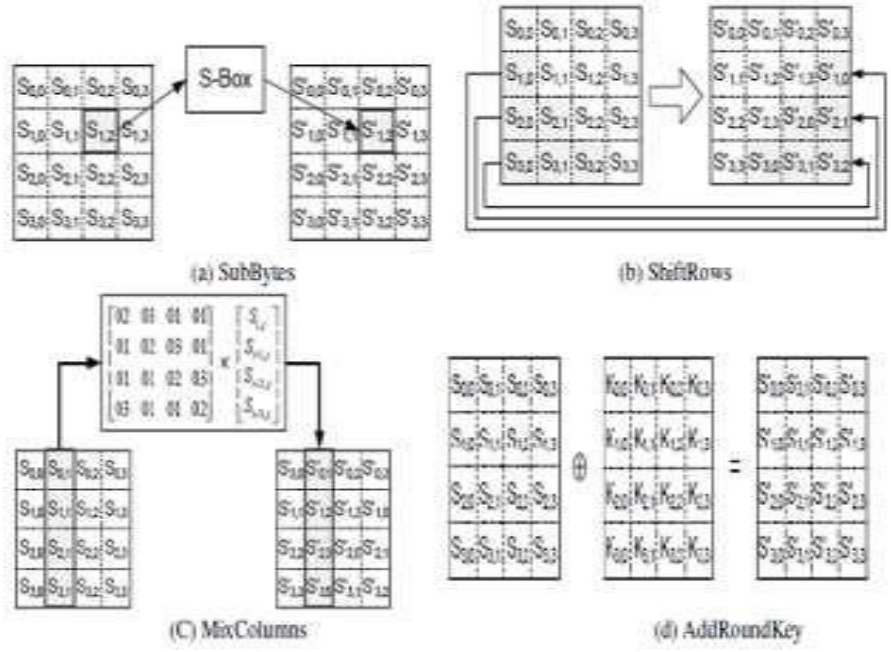

Fig 4: AES Operation

V.COMPARATIVE STUDY BETWEEN RIJNDAEL, DES AND BLOWFISH

1	DES	Rijndael(AES)	Blowfish
2	Data Encryption Standard(DES), was the first encryption standard	Advanced Encryption Standard(AES), also known as the Rijndael algorithm, is a symmetric block cipher	It is a symmetric block cipher
3	published by NIST.It was designed by IBM based on their Lucifer cipher.	AES was introduced to replace the DES.	It is unpatented and freeware, and is available free for all uses
4	DES became a standard in 1974	-	Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms.
5	DES uses a 56 bit key, and maps 64 bit input block into a 64 bit output block.	can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256	It takes a key of variable-length, from 32 bits to 448 bits, making it ideal for securing data.
6	The key takes one bit in each of the 8 octets is used for odd parity on each octet.		
7	There are many attacks and methods recorded till now those exploit the weaknesses of DES, which made it an insecure block cipher.	Brute force attack is the only effective attack known against this algorithm.	it suffers from weak keys problem, till date no attack is known to be successful against it (Bruce, 1996) (Nadeem, 2005).

CONCLUSION

Rijindael algorithm is a powerful cryptographic technique that is gaining more popularity because of its strength. Thus analysis of improvements in this field becomes very important. Today cryptanalysis attacks is growing frequently and powerful hence it becomes increasingly important to develop a private key cryptosystem to resistant such kind of attacks. When the number of rounds is increased, it considerably improves the complexity of the algorithm making it strong against the cryptographic attacks. The length of the key is increased to increase the number of rounds involved as number of rounds depend on the length of the key used. Thus, the increase in the key size provides the rijindael algorithm strong resistance against the new existing attacks and has an high speed of data encryption and decryption.

REFERENCES

[1].Renjith V Ravi, Dr.R. Mahalakshmi, “Simulation and Error Analysis of Rijndael Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 5, May 2014.

[2].Jayanta Gope, Prakash Kumar Shah,“Advanced and Secured Rijndael Hardware Realization Using Single Electron Transistor Technology”, International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 Volume-3, Issue-5, May 2014.

[3].Manjesh.K.N, R K Karunavathi, “Secured High throughput implementation of AES Algorithm”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[4].[4] M.Gnanambika, S.Adilakshmi,Dr.Fazal Noorbasha,“AES-128 Bit Algorithm Using Fully Pipelined Architecture for Secret Communication”, International Journal of Engineering Research and Applications (IJERA), pp.166-169, Vol. 3, Issue 2, March -April 2013.

[5].Shylashree.N, Nagarjun Bhat and V. Shridhar,” Fpga Implementations Of Advanced Encryption Standard: A Survey, International Journal of Advances in Engineering & Technology, May 2012.

[6].Nitin K. Jharbade and Rajesh Shrivastava, “Network based Security model using Symmetric Key Cryptography (AES 256– Rijndael Algorithm) with Public Key Exchange Protocol (Diffie-Hellman Key Exchange Protocol)”, IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.8, August 2012

[7].Vishwa gupta,Gajendra Singh ,Ravindra Gupta, “Advance cryptography algorithm for improving data security”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012

[8].Jawahar Thakur, Nagesh Kumar, “DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis”, International Journal of Emerging Technology and Advanced Engineering, Volume 1, Issue 2, December 2011.

[9].P.Karthigaikumar, Soumiya Rasheed, “Simulation of Image Encryption using AES Algorithm”, IJCA Special Issue on “Computational Science - New Dimensions & Perspectives” NCCSE, 2011

[10]. Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath, “A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm”, IEEE International Conference on Communication Systems and Network Technologies, 2011.

[11]. A.Nath, S.Ghosh, M.A.Mallik, “Symmetric key cryptography using random key generator”, Proceedings of International conference on SAM, 12-15 Vol-2,P-239-244, July,2010.

[12]. A.Nath, S.Das, A.Chakrabarti, "Data Hiding and Retrieval", Proceedings of IEEE International conference on Computer Intelligence and Computer Network, Nov, 2010. [13] Jayanta Gope, et.al., "Cellular Automata Based Data Security Scheme in Computer Network using Single Electron Device", International Conference [ACCTA-2010], 3-5 August 2010.

[13]. [14] Chen-Hsing Wang, Chieh-Lin Chuang, and Cheng-Wen Wu, "An Efficient Multimode Multiplier Supporting AES and Fundamental Operations of Public-Key Cryptosystems", IEEE Transactions on Very Large Scale Integration Systems (VLSI), Vol.18, No.4, pp.553-563, 2010.

[14]. [15] Shtewi,A.M., "An Efficient Modified Advanced Encryption Standard (MAES) adapted for image cryptosystems", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, pp 226-232, February 2010.

[15]. Yan Wang and Ming Hu,"Timing evaluation of the known cryptographic algorithms", IEEE International Conference on Computational Intelligence and Security, 2009.

[16]. 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, 4th-6th June 2009.

[17]. D.Dia, M.Zeghid, M.Atri, B.Bouallegue, M.Machhout and R.Tourki, "DWT-AES Processor for a Reconfigurable Secure Image Coding", International Journal of Computer Science and Engineering,vol.1,no.2, June 2009.

[18]. A. E. Rohiem, F. M. Ahmed and A. M. Mustafa, "FPGA Implementa-tion of Reconfigurable Parameters AES Algorithm", 13th International Conference on Aerospace Sciences and Aviation Technology, ASAT- 13, May 26 – 28, 2009.

[19]. Md. Nazrul Islam, Md. Monir Hossain Mia, Muhammad F. I. Chowdhury, M.A. Matin "Effect of Security Increment to Symmetric Data Encryption through AES Methodology", Ninth ACIS IEEE International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008.

[20]. N. Mentens, L. Batina, B. Preneel, and I. Verbauwhede, "A Systematic Evaluation of Compact Hardware Implementations for the Rijndael SBox", In Alfred Menezes, editor, CTRSA, volume 3376 of LNCS, pages323-333. springer, 2005.