A detailed Study on various Modified Advanced Encryption Standard Algorithms

R.Caroline Kalaiselvi [1], Dr. S. Mary Vennila[2]

[1]Associate Professor and Research Scholar, Presidency College, Chennai.
[2]Associate Professor & Head, PG and Research Dept. of Computer Science, Presidency College, Chennai.
Email:carrie.jonna@gmail.com[1], vennilarhymend@yahoo.co.in[2]

Abstract
In the recent times, with the tremendous growth of digital communication over electronic network, the content security becomes a chief concern. Web itself permits several security threats and people will simply corrupt the data over the network. Cryptography plays a very important role by providing security for digital transmission of information over the insecure network. The protocols scramble the knowledge into indecipherable text which might be solely scan or decrypted by those possesses the associated key. The Advanced Encryption Standard (AES) is a standard rule that provides higher security with higher cryptography speed and turnout however still modifications are happening to enhance its performance. In this paper we tend to survey and analyze many modifications on AES cryptography techniques on totally different parameters and compare their performance with typical AES.

Keywords: *Cryptography, Decryption, Encryption, Block cipher, S-Box, Encoder.*

I. INTRODUCTION
The ascent of digital knowledge transmission has significantly raised the importance of data security in our fashionable digital life. In digital communication the development of recent transmission technologies have ascended the want of specific strategy for security mechanisms. Network security has become more and more important as digitalization and transmission of huge knowledge over web are reworking from time to time. Cryptography and different cryptography techniques give security and protection to the information transmitted over non secure networks used for digital transmission of information.

The Advanced Encryption Standard (AES) called as Rijndael is a well-known symmetric block cipher rule adopted by the United States of America government as a national cryptography rule an it provides movableness, hardiness and high level security against several science attacks. To possess higher performance, certain efforts have already been created in designing and reconstructing the AES rule.

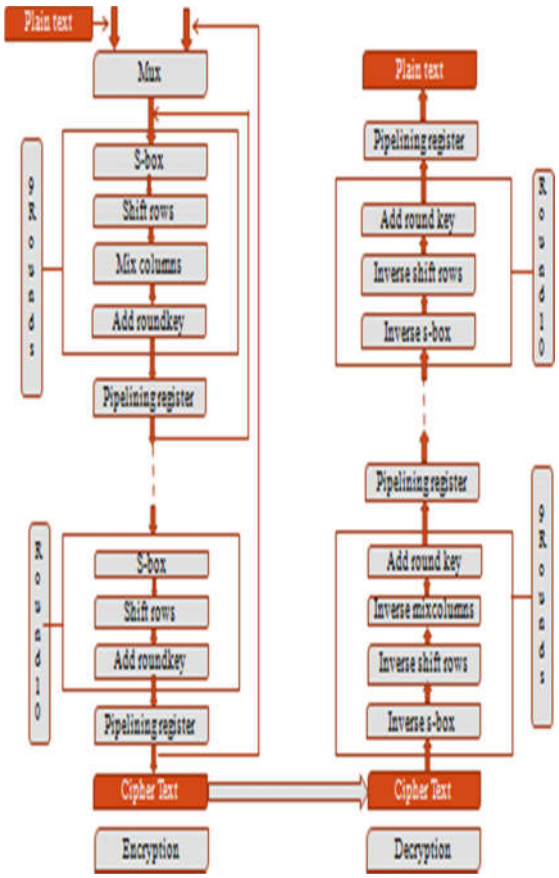
During this paper we tend to discuss certain totally different modifications on AES algorithm and scrutiny their result on the idea of various parameters. To reinforce the potency of AES researchers generally changed the prevailing structure of the AES algorithm and generally merging the AES block cipher with alternative models from numerous fields. Here during this paper, we tend to associate many characteristics of all those chan

Advanced Encryption Standard Algorithm
The developed Encryption regular relies on the Rijndael cipher developed by using Joan Daemen and Vincent Rijmen. It is a ordinary block cipher that approaches potential blocks of 128 bits utilizing key dimension of 128, 192, and 256 bits. Each information block of 128 bit is split into sixteen Bytes. These bytes are mapped to a 4 x 4 array and one and all operations of AES are carried out on this state. The AES algorithm continues 4 stages for you to make a circular round which is carried out 10 instances for a 128-bit key, 12 instances for a 192-bit key, and 14 instances for a 256-bit key.

- "SubBytes" implements easy substitution of each byte. It makes use of one desk of 16x16 bytes containing a permutation of all 256 eight-bit values.
- "ShiftRows" circular shifts (permutes) the bytes inside the block
- "MixColumns" transformation teams 4-bytes along forming 4-term polynomials and multiplies the polynomials with a standard polynomial mod (x^4+1).
- "AddRoundKey" adds the round key with the block of data.

In AES rule, cryptography procedure starts with Add round Key stage followed by (Nr-1) rounds having four stages each and therefore the cryptography method ends with the last round that contains 3 stages.This full cryptography and secrets writing

procedure is shown by Figure-1. This diagrammatic illustration is cited here for references as a result of most of the modifications wiped out the AES rule is reflected in these step directly or indirectly. Figure 1: diagram of Main Steps of AES



The decryption procedure is precisely the inverse of encryption procedure consisting conjointly four stages specifically InverseSubBytes, Inverse ShiftRows,InverseMixColumns, and AddRoundKey.

Typical AES 128 bit provides higher security, higher cryptography speed, and higher turnout compared to alternative regular cryptography technique. However still modifications are happening to scale back hardware resources, increase security against applied mathematics attacks, higher cryptography speed, less overhead on the information, transferring giant scale transmission knowledge as per totally different wants in numerous things.

II. Analysis Report

We tend to understand that typical AES provides smart encryption-decryption speed, and turnout. It has high security than alternative existing encryption-decryption rule. Then the researchers are attempting to switch this rule to enhance its security, encryption- decryption time and to increase turnout as per demand. A number of modifications to enhance AES are mentioned below:

Shtewiet. al. bestowed an idea on modification to the Advanced encryption Standard (MAES) to replicate a high level security and higher image cryptography. The modification is done by adjusting the Shift Row part [2].

Ritu &Vikas projected a changed AES having two hundred bit block furthermore as key size using 5x5 Matrix in contrast to the conventional 128 bit AES with 4x4 Matrix. The projected work is then compared with the 128, 192, 256 bit AES.The combine column transformation is modified during this method. The result shows cryptography speed and turnout at encryption speed is raised and decryption speed, turnout at decryption end is shrivelled than typical AES Algorithm [4].

Dandekaret. al. projected a changed regular AES algorithm. They used 512 bit length so as to produce a high level of security and high turnout needed application. Strength of the AES rule is increased by increasing the key length to 512 bit and so as to

produce a stronger encryption technique for secure communication the quantity of rounds is raised [5].

Vandana C. Koradia is implemented with optimizing the existing standards of cryptography for the pictures and text knowledge cryptography. The modification is completed by totalling the Initial Permutation step, takes from Data Encryption Standard (DES), so as to enlarge the cryptography performance. This modification indubitably will increase the potency of encryption and makes the rule speedier than the prevailing one [6].

Manish Kumar Aery has implemented a combination of encryption feature of AES and the compression feature of Base64 encoder to develop an economical cryptography system which will encode the information and therefore saving time and increasing the turnout. Initial Base64 encoder encodes or converts the text into string worth or whole knowledge into string so encrypted by AES algorithm; finally cipher text is generated. Once cryptography is done the file size is reduced and is then sent to encryption that additionally reduces the time for processing [7].

Zeghidet.al. projected a brand new cryptography schemes by adding a key stream generator, like (A5/1, W7), to the AES rule so as to extend the high image security and increase cryptography performance, in the main for pictures characterised by reduced entropy. Key stream generator into AES for image cryptography helps to beat the matter of rough-textured zones and increase cryptography performance [8].

Yogeswari& Eswaran projected a novel method to reinforce security aspects by associating science techniques together with Steganography. This paper offers confidence and trust by build use of improved twin key AES rule together with Steganography [9].

Abdulazeez& Tahir projected 2 architectures, one for AES cryptography 128-bit method, and therefore the alternative for AES Decryption128- bit method. Each architectures are supported associate with iterative structure and modifications like merging transformation, find tables for decryption, generating keys, and improvement of every clock cycle to include maximum variety of operations to enhance the turnout and reducing hardware resources [10].

III. Comparative Analysis

To enhance the performance of AES rule, varied efforts are wiped out redesigning and reconstructing of AES that we've got mentioned within the previous section. A comparative analysis of performance of totally different modified AES rules compared to traditional AES algorithm is done on the idea of six different parameters, that is disobdurate below and shown in Table-1.

Performance of all changed AES in terms of cryptography and secret writing speed are higher than the traditional AES, except AES- 512 rule and AES-200 rule. In AES- 512 rule, because of increase in variety of rounds, the encryption and decryption procedures become additional complicated thereby degrading the speed. Therefore there's a exchange between speed and security. Once more in AES- 200 solely decryption time per bit slightly shrivelled however cryptography time per bit up to twenty and decryption time per bit raised up to twenty five than typical AES. On the opposite hand, modification done by Vandana C. Koradia uses Initial Permutation table replacement combine Column step of AES extremely will increase cryptography and decryption speed, that is useful for transmission of data encryption. The turnout is also outlined as variety of bits which will be encrypted or decrypted throughout one unit of your time [4].

From the Table-1, it's discovered that out of those eight totally different modifications on AES, additional or less all the changed AES algorithms are performing arts well in respect of turnout, however AES-512 rule and AES with merging transformation.

Table 1.Comparison of Various Modified AES Algorithms

Parameters	Key Length (Bits)	Added Technology	Encryption Speed	Decryption Speed	Through put	Security
AES with adjustment of Shift Row[2]	128	NO	Increased	Increased	Increased	High
AES-200 [4]	200	NO	Increased	Decreased	Increased	High

AES-512 [5]	512	NO	Decr ease d	Decre ased	Doub le In-creas ed	Extre me High
AES with Perm utatio n Table [6]	128	NO	High ly In-creas ed	Highl y Incre ased	Incre ased	Good
AES with Base 64 Enco der [7]	128	YES	Incre ased	Incre ased	Incre ased	Extre me High
AES with A5/1 & W7 Enco der [8]	128	YES	Incre ased	Incre ased	Good	High
AES with Stagn ograp hy[9]	128	YES	Goo d	Good	Good	Extre me High
AES using FPG A [10]	128	NO	Incre ased	Incre ased	Highl y In-creas ed	Good

show glorious performance by giving better double throughput. Again some modifications didn't show any vital rise of throughput once merging further technology with the traditional AES. There are several strategies employed by researchers within the style and modification of AES block cipher so as to reinforce Table 1: Performance Analysis and Comparison of assorted changed AES Algorithms the safety of the rule and a few together with merging the AES block cipher with alternative models from numerous fields[11].AES algorithms give sturdy security however there are still some problems associated with Brute Force attack and applied mathematics attacks.

From Table-1, it's discovered that the safety strength of changed AES algorithms has improved, however implementation of Permutation Table in AES reduces security strength of AES rule. In our study, we tend to analysed that AES- 512 rule give extreme high security by increasing key bit length and numbers of rounds. Merging of technology like Stagnography and Encoder like Base64 with AES ready to produce higher security than the traditional AES. Mainly the changed rule (MAES) o ffers higher cryptography results in terms of security against applied mathematics attacks in comparison to original AES.

IV. Conclusion

During this paper we tend to surveyed and analyzed many modifications on AES cryptography techniques on totally different parameters and compared their performance with typical AES. Performance of those changed AES algorithms vary on totally different parameters. Generally, with the rise demand of sturdy security wherever high level security is required, we tend to need to compromise with cryptography speed in those modifications. Once more for cryptography of huge knowledge like multimedia data transmission, higher cryptography speed is required, that security is somewhere to be compromised to realize higher cryptography speed.These modifications are helpful in numerous conditions consistent with matters demanded. So modifications on AES ought to target planning such strategies and techniques that would be used on existing applications in an economical manner and supply us an extremely secured, extremely quick cryptography system which might give high security against all attack together with applied mathematics attack and Brute Force attack.

ACKNOWLEDGMENT

The authors also are grateful to authors / editors / publishers of all those articles, journals and books from wherever the literature for this text has been reviewed and mentioned.

REFERENCES

[1] Patel, F. R., Dr. Cheeran, A. N. (2015). Performance Evaluation of Steganography and AES encryptionbasedon different formats of the Image. International Journal of Advanced Research in Computer and Communication Engineering, 4(5), 659-664, 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 on 27/04/2017.

[2] Shtewi, A.A., Hasan, B. E. M., Hegazy, A. El F. A. (2010). An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems. International Journal of Computer Science and Network Security (IJCSNS), 10(2), 226- 232. http://paper.ijcsns.org/07_book/201002/20100234.pdf on 08/08/2017 at 01:25 AM

[3] Gurkaynak, F. K. (2006). GALS System Design:Side Channel Attack Secure Cryptographic Accelerators. Retrieved from https:/ iis-people.ee.ethz.ch/~kgf/ acacia/fig /aes.png on 15/06/2017 at 10:25 PM

[4] Pahal, R., Kumar, V. (2013). Efficient Implementation of AES.International Journal of Advanced Research in Computer Sci ence and Software.pdf on 27/04/2017 at 11:45 PM.

[5] Dandekar, A. K., Pradhan. S., Ghormade.S. (2016).Design of AES-512 Algorithm for Communication Network. International Research Journal of Engineering, 3(7), 290-295, ISSN: 2277 128X. http://ijarcsse.com/Before_August_2017/docs/papers/ Volume_3/ 7_July2013/V3I7-0246Engineering and Technology (IRJET),3 (5), 438-443, e-ISSN: 2395 -0056. https://www.irjet.net/archives/ V3/i5/IRJET-V3I592.pdf on 27/04/2017 at 12:13 AM.

[6] Koradia, V. C. (2012-2013). Modification in Advanced Encryption Standard. Journal of Information, Knowledge, and research in Computer Engineering, 2(2), 356-358, ISSN: 0975 – 6760. http://www.ejournal.aessangli.in/ASEEJournals/CE73.pdf on 26/05/2017 at 12:33 AM.

[7] Aery, M. K. (2016). String Compression Technique with Modified AES Encryption. International Journal of Advanced Com puting and Electronics Technology (IJACET), 3(1), 13-25, ISSN (Print): 2394-3408, (Online): 2394-3416. http://troindia.in/jour nal/ijacet/vol3iss1/13-25.pdf on 09/06/2017 at 08:37 PM.

[8] Zeghid, M., Machhout, M., Khriji, L., Baganne, A. and Tourki, R. (2007). A Modified AES Based Algorithm for Image Encryption. International Journal of Computer, Electrical, Automation, Control and Information Engineering, 1(3), 745-750, www.waset.org/Publication/7580 on 25/05/2017 at 1.03 AM.

[9] Yogeswari, G., Eswaran, P. (2016). Enhancing Data Security for Cloud Environment based on AES Algorithm and Steganog raphy Technique. International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), 3(20), 233- 236. http://ijartet.com/v3s20alagappa on 27/04/2017 at 12:52 AM.

[10] Abdulazeez, A. M., Tahir, A. S. (2013). Design and Implementation of Advanced Encryption Standard Security Algorithm using FPGA.International Journal of Scientific & Engineering Research, 4(9), 1988-1993, ISSN 2229-5518. https://www. ijser.org/paper/Design-and-Implementation-of-Advanced-Encryption-Standard-Security-Algorithm-using-FPGA.html on 08/08/2017 at 01:55 AM.

[11] Juremi, J., Mahmod, R., Zukarnain, Z. A., Yasin, S. Md. (2017). Modified AES S-Box Based on Determinant Matrix Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering, 7(1), 110-116, ISSN: 2277 128X. http://ijarcsse.com/Before_August_2017/docs/papers/ Volume_7/1_January2017/V7I1-01112.pdf on 08/08/2017 at 01:46 AM.