A New Approach on AES to Increase the Resistivity of the Cipher System

Ranjana Manohar Nayak
Department of Computer Science and Engineering
NMAMIT, Nitte, Karnataka, India

Radhakrishna Dodmane
Department of Computer Science and Engineering
NMAMIT, Nitte, Karnataka, India

ABSTRACT
In today's era, we are facing security- related challenges during information relocation. Amongst the transmitter and receiver, most of the sensitive information is not secured. Encryption and decryption used to secure the information of data's. In the encryption, the original text is converted into indecipherable form. Different techniques can be used to safeguard the information from unlicensed access. The proposed work aims to provide confidentiality through Advanced Encryption Standard (AES). This paper mainly emphases on the security of the existing AES algorithm and aim to heighten the level security of this process through the addition in the existing AES algorithm by including a new operation called Math Trick. The proposed system moderately increased security compared to the existing system.

Keywords
Encryption, Decryption, Advanced Encryption Standard, Math Trick, Security.

1. INTRODUCTION
Secure communication is very important and one of the basic requirement in today's era. Providing security and protect the information is the major challenge in this world. To provide security for the information several algorithms and tool should implemented. Cryptography is the main ingredient for the secure communication and free from attacks, it protects the sensitive information. The information that sent at on end remains confidential and only the intended user on the other receive the information and the information may include not only text but also audio, video that are widely used in our day-to-day life. Cryptographic algorithms are efficient, low cost, and very secure and so on.

Cryptographic algorithms provide very important role proving security against various attacks. There are different encryption algorithms and each algorithm has its own benefits and limits. Original message or any information that can be recite straightforwardly without any difficulty is baptized as the plain text or clear text. In the encryption process plain text is converted to indecipherable form and this message is hidden from third party [1][4][8]. Encryption algorithm characterized into symmetric and asymmetric encryption algorithm. The process that converts ciphertext to its original content is baptized as decryption.

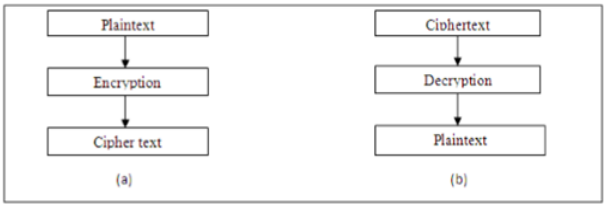

Fig 1 (a) : Encryption Process (b) Decryption Process

Confidentiality, Integrity and Availability are the basic principles of information security and are depicted in Fig 2:

Fig 2: Fundamentals of Information Security

Confidentiality: confidentiality is generally proportionate to security and refers to the assurance of secret data from unapproved clients by utilizing encryption methods and furthermore to ensure that real users can in fact access that data. Authentication methods, get to control systems including check utilizing usernames and passwords guarantee that the private information stays open just to the assigned client.

Integrity: integrity guarantees that data isn't changed or altered by unapproved clients while in transit. let us suppose a condition where an individual starts a financial exchange to exchange an amount of $500 to his companion, while the exchange is in mid-manner a sham adjusts the incentive from $500 to $ 5000 and changes the recipient name to his very own name and possess account number. This can cause a serious problem to the bank and the sender.

Availability: It refers to guarantee that data is accessible consistently when required by genuine clients. All of data has' value, just when approved clients get to it at right times. A most regular attack utilized by programmers these days is to crash the servers of sites utilizing a DDoS attacks, where a server keeps satisfying attacker's requests and at one point, gets over-burden because of plenty of solicitations, which thus prompts web server crash and interfere with the administrations.

Authentication: Authentication ensures identification. It is a mechanism that is used to determine whether someone is in fact that person what he has declared to be. The procedure of confirmation includes more than one evidences of personality like something the real client knows (i.e. a PIN), roughly he has (i.e. a physical device such as an identity card or debit card), something he is (i.e. fingerprint or iris).

Non repudiation: It guarantees that the parties involved in an online transaction cannot deny receiving a successful transaction nor can they deny having initiated the transaction It is the capacity to prove that an activity has occurred at a specific time. Lack of non-repudiation can cause difficult

issues. Envision a situation where the recipient in a bank transaction says that he has not gotten the ideal amount of cash and sender in not equipped for giving the evidence of successful completion of the exchange.

2. BACKGROUND STUDY

Advanced Encryption Standard (AES) is a well- known symmetric cipher system plus generally utilizes a same key for both encryption and decryption. This key is baptized secretkey. AES is block cipher takes i/p stream into block for processig. It can be 128, 192, 256 -bit's. However, the standard's is that, the input block size will constantly be fixed at 128 -bits' and the key size will stay any of 128, 192 and 256. AES follow's the substitution permutation network structure and so it partakes numerous working rounds depending on the key size. AES works in 10- rounds for 128 -bits key, 12- rounds for 192 -bits key and 14- rounds for 256 -bits key. [2][3].

Internally, cipherkey is prolonged into 11, 13 or 15 keys individually for 10, 12 or 14 rounds. Input is represented as 4x4 matrix called statearray. formerly the state _array is XOR'd with foremost round key is known as AddRound-Key. Each round comprises four unique steps but, the last round encloses three- stages. So, steps of AES are [3]:

1. Key-expansions: Rijndael-key schedule expands all-around keys from cipher key.
2. Starting-round: AddRound-Key – The state-array is XOR'd by the earliest roundkey.
3. Rounds: Each round except last- round's plays out these four stages.

- Sub Bytes on state_array utilizing s -box.
- A change Shift Rows on state_array.
- Mix Columns on state array.
- AddRound-Key thru state_array.

4. Last round: This round doesn't enclose Mix Columns and it executes succeeding three-stages.

- Sub Bytes on state_array utilizing s-box.
- A stage Shift Rows on state_ array.
- AddRound-Key with state_array.

Sub-Bytes mean's substitution of byte of the state_array via seeking in lookup table is called as substitution box or S-box. S-box is a 16x16lookup table and it encompasses 256 distinct qualities. The S-box table encloses every single imaginable incentive for 8-bit succession that implies in decimal 0 to 255.

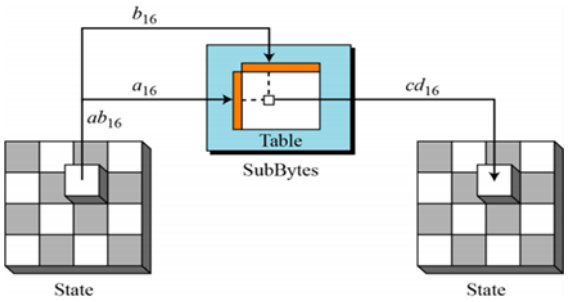

Fig 3: Sub Bytes Transformation Step

ShiftRows phase execute moving of bytes amongst the columns of a state_array. The state_array contains 4-rows and 4-column'. This progression executes left move of firm equalizer in various rows consistently. For 128 bit and 192 bit information block. ShiftRows procedures given below:

- Foremost row is unaltered.
- Second row moves 1 byte to left.
- Third row moves 2 bytes to left.
- Fourth row moves 3 bytes to left.

In over-all, row 's' is leftward moved episodically for (s-1) bytes.

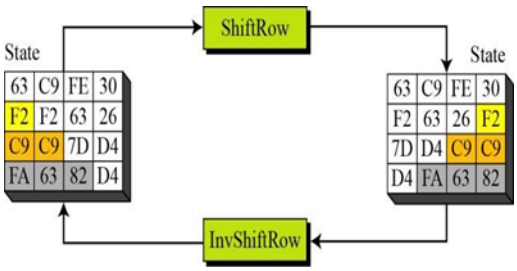

Fig. 4: Shift Rows Transformation Step

Mix Columns: Like earlier phase, actuality of this phase is to provide diffusion of the bits over multiple rounds. This is accomplished thru acting out multiplication one column at a time. Respectively, values' in the column is multiplied against every row value of a standard matrix. The consequences of these multiplication XOR'd together [5].

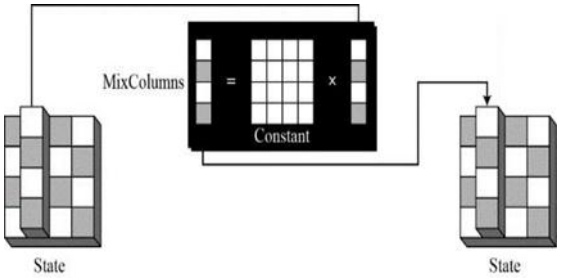

Fig. 5: Mix Columns Transformation Step

AddRound-Key: each byte of the state is pooled thru the round key, each round key is resultant from the cipherkey by means of a key program.

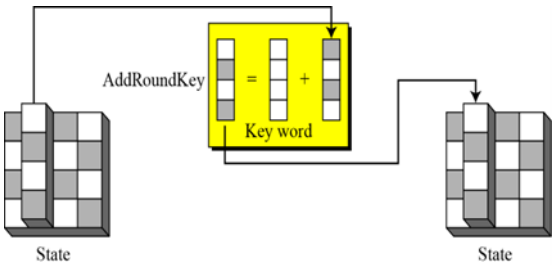

Fig. 6: Addround-key Transformation

3. PROPOSED SYSTEM FOR AES

In our proposed work, the additional operation is added called as Math Trick.

Math trick: Implementation of the math trick is to converting hex decimal to decimal. Initially the plaintext or the original message is in the hexadecimal; it is to be converted to

decimal. Along with the plaintext we must take the key also, it also to be converted to decimal. Later the decimal value of the plain text and decimal value of the key is to be added. Then that value is to be converted to hex decimal.

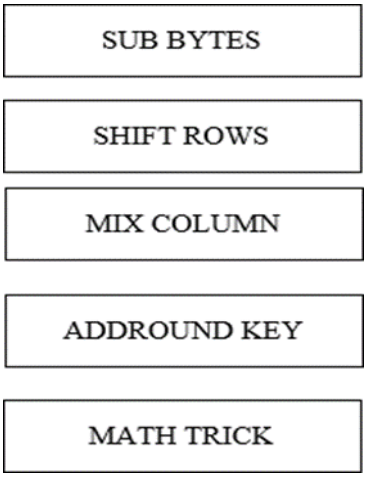

Fig 7: Transformation step in AES

Following figure indications, the flow of the steps of the MATH TRICK.:

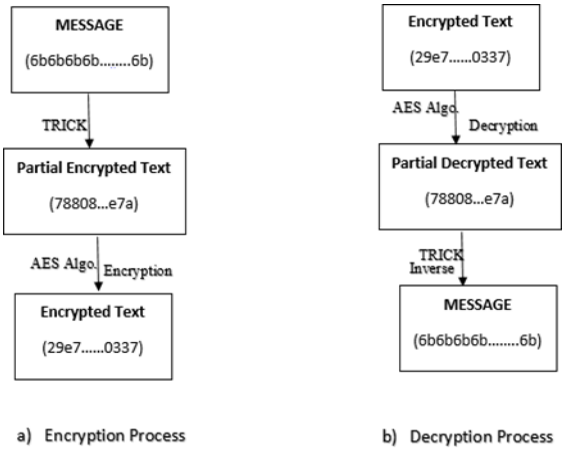

Fig 8: Encryption and Decryption process

Brute force technique: AES is now a secured method yonder from entirely crypt- analysis. For crypt-analysis, hacker's dependably attempted to discover the cipherkey in which the cipher content can be decode. In principle, brute force is the utmost well-known crypt-analysis, which can be utilized alongside every single cryptographic calculation. In brute force attack, hacker's look through the cipher- key amongst all conceivable mix of keys. They figure each conceivable mix of keys and play out a trace decoding for testing on the probability that it is the precise key. Presently the inquiry is that, to what extent time is required for brute force to locate the genuine key? The ideal opportunity for brute force attack relies upon the key size. In the event that the key size is little, it tends to be discovered all around rapidly. But the key size is longer, at that point it might be requiring long investment to locate the real key. In our proposed method number of brute force operations needed to decrypt is increased (key combination) as compared the normal method or the existing method as shown in the fig below.

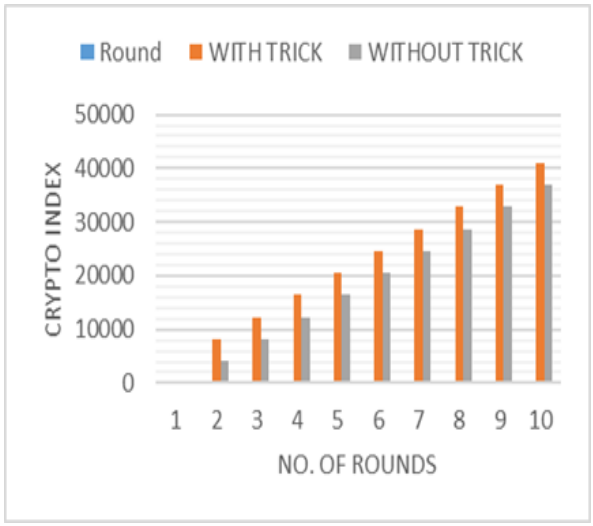

Fig 9: Graph shows the number of brute force operations needed to decrypt in both scenarios

Time security**:** calculated based on the encryption time and decryption time.

The encryption time: Is the time that an encryption calculation takes towards deliver a cipher content from a plain text.

The decoding time: Is the time that a decoding calculation takes to deliver a plain text from cipher content. In the proposed method after adding with one of the operations called as math trick the time taken for the encryption as well as time taken for the decryption is decreases. Hence, we can say that our proposed method is moderately secured compared to the existing method.

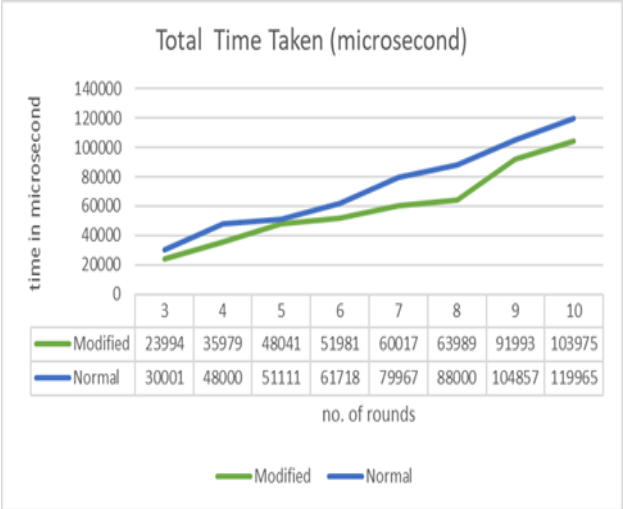

Fig 10: Total time taken (enc+dec) modified vs. normal method

Avalanche effect: It is an alluring property of any encryption calculation, which a little alteration either in the plain text or the key ought to create a critical amendment in the ciphertext content. Specifically, an amendment in one-bit of the plaintext or one-bit of the key should create a change in numerous bits of the cipher text. Solitary reason for the avalanche effect impact is that by changing just one bit there is huge change then it is tougher to make an inquiry of ciphertext, when attempting to think of an assault. [9][17].

Table 1. Avalanche Effect for Fixed Key 128 Bit

No	Plaintext	Cipher text(hex)	Bit Variance	Avalanche(%)
1	6b6b6b6b6b6b6b6b 6b6b6b6b6b6b6b6b	29e7e1b343001e89 f6bc151b30030337	66	51.56
2	6b6b6b6b6b6b6b6b 6b6b6b6b6b6b6b6c	f0ea443157507a15 c5633c2c5bb22006	64	50
3	6b6b6b6b6b6b6b6b 6b6b6b6b6b6b6b6d	e1c8ed567fd1db94 547d9df85a0a6046	64	50
4	6b6b6b6b6b6b6b6b 6b6b6b6b6b6b6b6e	1f723e263ff4255d 542fb4411545166a	64	50.78
5	6b6b6b6b6b6b6b6b 6b6b6b6b6b6b6b6a	9a3dd42e03110011 4a95a5259168f3d0	71	55.47

From table 1, 128-bit' of AES keep up a decent degree. For checking the security, we manage avalanche effect. To decide avalanche effect in table 2 we take fixed 128-bit' key and diverse plaintext brace thru contrast of 1-bit' in each pair it demonstrates a decent level of bit change.

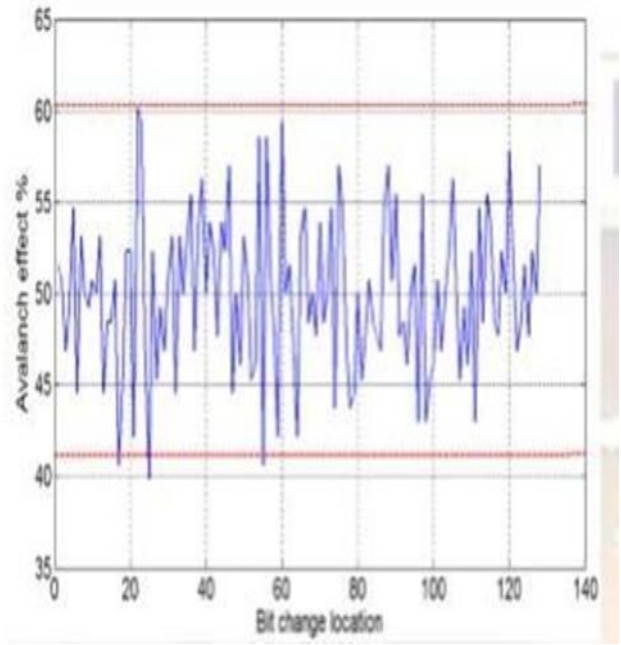

Fig 11: Avalanche effect due one-bit variations in secret key

Fig.11 is the avalanche effect of the proposed AES of 128-bit' because of one-bit alteration in secret key. It signifies avalanche effect deceits somewhere in the range of 50%and 61%, implies that it's hard to make expectations about the information, being given just the output. This mirrors the invulnerability of our calculation to linear and discrepancy cryptanalysis**.**

4. CONCLUSION

With the quick advancement of computerized information trade, security data turns out to be much significant in information storage and transmission. Because of the expanding utilization of information in mechanical procedure, it is fundamental to shield the secret picture information from unapproved access. we have proposed an innovative proposal and improved the security by including Math Trick in the current AES, the time security of the planned arrangement expands contrasted with the current framework. The avalanche effect dependably fluctuates with every execution and progressively secure against brute force technique.

5. REFERENCES

[1] Guy-Armand Yandji, Lui Lian Hao, Amir-Eddine Youssouf, Jules Ehoussou, "RESEARCH ON A NORMAL FILE ENCRYPTION AND DECRYPTION" in proceedings of IEEE 2011.

[2] Al-Mamun, Abdullah, Shawon SM Rahman, Tanvir Ahmed Shaon, and Md Alam Hossain. "SECURITY BY MODIFYING SBox WITH AN ADDITIONAL BYTE."

[3] "Specification for the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197 November 26, 2001 K. Elissa,

[4] Saberi, I. Shojaie, B. ; Salleh, M. "Enhanced Key Expansion for AES-256 by using Even-Odd method", Research and Innovation in Information Systems (ICRIIS), 23-24 Nov. 2011

[5] Liam Keliher ,"Substitution-Permutation Network Cryptosystems Using Key-Dependent Boxes", http://www.researchgate.net/publication/2822741, ARTICLE • NOVEMBER 1997

[6] Krishnamurthy G N and V Ramaswamy, "Making AES Stronger: AES with Key Dependent S-Box." International Journal of Computer Science and Network Security,VOL.8 No.9, September 2008

[7] Mohan H. S. and A Raji Reddy, "Performance Analysis of AES and MARS Encryption Algorithms", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011

[8] Manisha S. Mahindrakar' "Evaluation of Blowfish Algorithm based on Avalanche Effect", International Journal of Innovations in Engineering and Technology (IJIET), Vol. 4 Issue 1 June 2014

[9] Akash Kumar Mandal1, Mrs. Archana Tiwari, "Analysis of Avalanche Effect in Plaintext of DES using Binary Codes", International Journal of Security, Privacy and Trust Management, Volume 1, Issue 3, September –October 2012

[10] SriramRamanujam and MarimuthuKaruppiah, "Designing an algorithm with high Avalanche Effect", International Journal of Computer Science and Network Security, VOL.11 No.1, January 2011

[11] K.Anchugam and M.Tamilselvi "New Data Encryption Standard Algorithm" , International Journal of Computer Science and Network Security, VOL.13 No.4, April 2013

[12] M.Abirami, S. Chellaganeshavalli, "Performance Analysis of AES and Blowfish Encryption Algorithm", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 2, Issue 11, November 2013

[13] AbdulkarimAmerShtewi, BahaaEldin M. Hasan and Abd El Fatah .A. Hegazy," An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems", International Journal of Computer

Science and Network Security, VOL.10 No.2, February 2010

[14] Nidhi Singhal and J.P.S.Raina, Comparative Analysis of AES and RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology-July to Aug Issue 2011

[15] M.Abirami, S. Chellaganeshavalli, "Performance Analysis of AES and Blowfish Encryption Algorithm", International Journal of Innovative Research in Science,Engineering and Technology, Vol. 2, Issue 11, November 2013

[16] Chandra Prakash Dewangan,Shashikant Agrawal, A Novel Approach to Improve Avalanche Effect of AES Algorithm, International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 8, October 2012

[17] Amish Kumar , Mrs. Namita Tiwari, "EFFECTIVE IMPLEMENTATION AND AVALANCHE EFFECT OF AES", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.

[18] Sweta K Parmar, K.C Dave, "Implementation of data Encryption and Decryption Algorithm for Information security", Proceedings of SARC-IRAJ International Conference, 14th July 2013, Delhi, India, ISBN: 978-93-82702-21-4.