An Enhancement on Block Cipher Key for Advanced Encryption Standard

Ratnesh Kumar Jain, Shiv Kumar, Babita Pathik

Abstract: ***The United State Government has standardized algorithm for encrypting and decrypting data which is known as AES (Advanced Encryption Standard). Information security is becoming very essential in data storage and transmission with the rapid growth of digital data exchange in an electronic way Cryptography play a vital role in information security system against different attacks which uses algorithms to scramble data into unreadable text which is only decrypted by those who has the associated key. It is of two types one for Symmetric and Asymmetric. Symmetric system has 288 bit block 128 bit commotional AES algorithm for 288 bit using 6x6 matrixes after implementation these points system is throughput at both sites encryption and decryption.***

Keywords: (Advanced Encryption Standard), United State, AES, Information security, Cryptography.

I. INTRODUCTION

The AES is introducing by the National Institute of Standards and Technology (NIST) of the United States has been rapidly used and replaces DES as the new symmetric encryption algorithm [2]. The AES algorithm is a part of symmetric block cipher AES worked with data blocks of 128 bits using a cipher key of length 128, 192, or 256 bits. Each data block consists of a 4x4 structure of bytes called the state, on which the fundamental operations of the AES algorithm are completed process [2].The proposed algorithm differs from conventional AES as it has 288 bits block area and key area both. Number of rounds is constant and equal to ten in this algorithm. The key expansion and substitution box generation are done in the same way as in conventional AES block encrypted. AES has 10 laps for 128-bit keys, 12 laps for 192-bit keys, and 14 laps for 256-bit keys [3].

1.1. The AES Algorithm

AES is a symmetric square figure with a piece size of 128 bits Key lengths can be 128 bits, 192 bits, or 256 bits; 8 called AES-128, AES-192, and AES-256, individually. AES-128 utilizations 10 rounds, AES-192 utilizations 12 rounds, and AES-256 utilizations 14 rounds. The main action of AES performs four transformation e.g. Sub Bytes (), Shift Rows (), Mix Columns (), Add Round Key ().

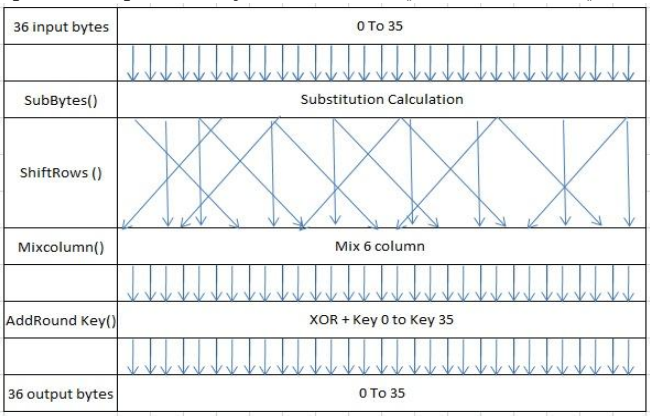
The initial three elements of an AES round are intended to cryptanalysis through the strategies for "disarray" and "dissemination."

The fourth capacity really scrambles the information. Dissemination implies designs in the plaintext are scattered in the cipher text. Perplexity implies the relationship between the plaintext and the cipher text is clouded.

A simpler way to view the AES transformation order is:

1. Scramble each byte (Sub Bytes).
2. Scramble each row (Shift Rows).
3. Scramble each column (Mix Columns).
4. Encrypt (Add Round Key).

A term connected with AES is "the State," a 'middle cipher,'11 or the cipher text before the last round has been connected. AES designs plaintext into 16 byte (128-piece) squares, and regards every piece as a 6x6 State cluster. It then performs four operations in each round. The exhibits contains line and section data utilized as a part of the operations, particularly Mix Columns() and Shift rows()



1.2. Algorithm Specification

For the AES algorithm**,** the length of the input block, the output block and the State is 128 bits. This is represented by ***Nb*** = 4, which reflects the number of 32-bit words (number of columns) in the State. [13].

For the AES algorithm**, the length of the Cipher Key, *K*, is 128, 192, or 256 bits.** The key length is represented by ***Nk*** = 4, 6, or 8, which reflects the number of 32-bit words (number of columns) in the Cipher Key. For the AES algorithm, the number of rounds to be performed during the execution of the algorithm is dependent on the key size. The number of rounds is represented by ***Nr***, where ***Nr*** = 10 when ***Nk*** = 4, ***Nr*** = 12 when ***Nk*** = 6, and ***Nr*** = 14 when ***Nk*** = 8. The only Key-Block-Round combinations that conform to this standard are given in Figure 1.1. For implementation issues relating to the key length, block size and number of rounds.

Revised Version Manuscript Received on January 11, 2017

Ratnesh Kumar Jain, M.Tech. Scholar, Department of CTA, Lakshmi Narayan College of Technology Excellence, Bhopal (M.P). India.

Dr. Shiv Kumar, Professor & Head, Department of Computer Science & Engineering, Lakshmi Narayan College of Technology Excellence, Bhopal (M.P). India.

Babita Pathik, Assistant Professor, Department of Computer Science & Engineering, Lakshmi Narayan College of Technology Excellence, Bhopal (M.P). India.

Figure 1.1: Key Lengths, Block Size and Number of Rounds

	Key Length (Nk Words)	Block Size (Nb Words)	Number of Round (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14
AES-288	4	4	10

II. PROBLEM STATEMENTS

There are various problems and issues with the AES.

2.1. Key Length Requirements

An execution of the AES calculation might bolster no less than one of the three key lengths determined in Sec. 5: 128, 192, or 256 bits (i.e., Nk = 4, 6, or 8, separately). Usage may alternatively bolster a few key lengths, which may advance the interoperability of calculation executions.

2.2. Higher encryption and decryption time

The encryption and decoding time for different AES principles is high. On the off chance that expansive square of information is closed for AES-128, AES-192, and AES-256 so encryption time for each piece is expanded and decoding time per bit is diminished.

2.3. Throughput Rate

The throughput of different AES benchmarks is less and presumed that the throughput at encryption closures of AES-128, AES-192 and AES-256. The unscrambling procedure of ordinary AES is high.

2.4. Security problem in high data rate

The Security of the AES model is inspected by playing out the different tests: Strict Avalanche Criterion and Bit Independence Criterion. SAC tells about the likelihood of the bit change while the BIC states the connections that yield bit have. Both of the criteria are examined and the AES calculation falls inside the normal level of security. Thus, one might say that the AES model is very little secured and can't be considered for correspondence where high information rate is required.

III. PROPOSED WORK

3.1. Encryption Algorithm

Toward the begin of encryption, 288 piece information is duplicated to the State exhibit of 6x6 frameworks. The information bytes are filled first in the section then in the columns. At that point after the underlying round key expansion, ten rounds of encryption are performed. The initial nine rounds are same, with little distinction in the last round. As showed in fig.7.1 each of the initial nine rounds comprises of 4 changes: SubBytes, ShiftRows, MixColumns and Add Round Key. In any case, in last round Mixcolumns change is not utilized.

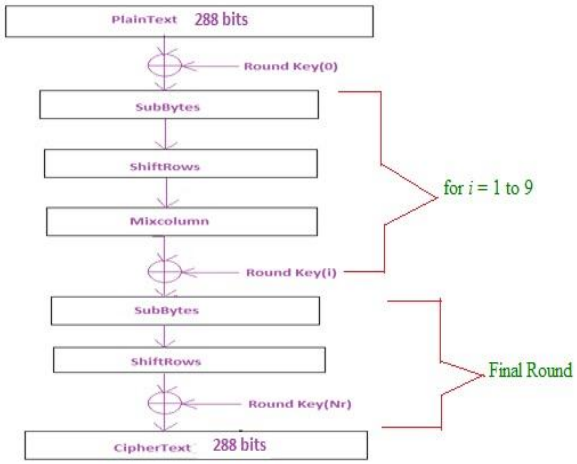


Figure : Encryption Structure of the AES algorithm

3.1.1. SubBytes Transformation

A nonlinear byte substitution that operates independently on each byte of the state using a substitution table.

3.1.2. *ShiftRows Transformation*

A Circular Shifting operation on the rows of the state with different number of bytes.

3.1.3. MixColumns Transformation

The operation that mixes the bytes in each column by the multiplication of the state with a fixed polynomial modulo x^6+1.

3.1.4. AddRoundKey Transformation

In AddRoundKey transformation, a roundkey is added to the State by bitwise Exclusive-OR (XOR) operation.

3.1.5. Decryption Algorithm

Decryption is the process of extracting the plaintext from cipher text.

3.1.6. InvSubBytes Transformation

This operation is same as it is the Encrytion process but the only difference is the inverse of the substitution box is used there since the substitution box which we used in the encryption is invertible.

3.1.7. InvShiftRows Transformation

InvShiftRows Operation inverse the shiftrows operation in the encryption process by right shifting the element in the row [1].

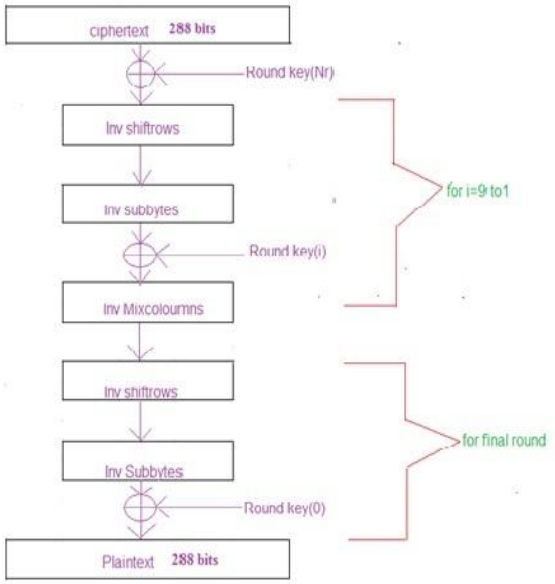


Figure :Decryption Structure of the AES algorithm

3.2.3. InvMixColumns Transformation

InvMixColumns is the backwards change of MixColumns. This is an intricate system as it includes extremely the byte augmentation under GF (2^8). The entire state is to be duplicated with pre-characterized grid called converse polynomial lattice.

3.3 Key Expansion Key expansion in AES is again a big task to perform, as it has several transformations. The key is expanded in the same manner as in conventional AES.

IV. RESULT ANALYSES

Parameter / Factor	AES-288	AES-128	AES-192	AES-256
Key Size(bits)	288	128	192	256
State(2D array)	6x6	4x4	4x4	4x4
Block Size(Bits)	128	128	128	128
Round(Iteration)	10	10	12	14
Encryption Time (bits/ms) (no. of bits encrypted/time)	1500/ 100	1500/ 150	1500/ 170	1500/ 200
Decryption Time(bits/ms) (no. of bits decrypted/time)	1500/ 250	1500/ 150	1500/ 170	1500/ 220
Throughput (KBPS) (encryption side)	9	8	8	6
Throughput (KBPS) (decryption side	3	8	7	6
Encryption Speed	15% more Than AES 128	AES-128	5% more than AES 128	10% more than AES128
Decryption Speed	45% slower Than AES 128	AES-128	25% slower Than AES 128	40% slower Than AES 128

V. CONCLUSIONS

This proposed work will present a new AES model having bigger block size which is 288 bits rather than conventional 128 bits AES. Also, the block is made by 6 rows and 6 columns unlike the AES‟s 4x4 matrixes. As the size of the matrix has increased all the transformations of the AES don't need to change except the mix column transformation. During mix column transformation, the expansion takes place in form of matrix multiplication under finite field. Having a bigger block, hence, requires a new matrix of size 6x6, to enable matrix multiplication. Here proposing this work for large block of data AES-288 encryption time per bit will be reduced and decryption time per bit will be increased than conventional AES. We will compare the throughput of various AES standards and the throughput at encryption end of AES-288 will be more than AES-128, AES-192 and AES-256. The decryption process of AES-288 would be slower than conventional AES. The Security of the proposed model will be examined by performing the test: Strict Avalanche Criterion and Bit Independence Criterion. SAC tells about the probability of the bit change while the BIC states the correlation that output bit possess. Both of the criteria are analyzed the proposed algorithm and find out desired level of security. Proposed model can be secured and considered for communication where high data rate is required.

REFERENCES

1. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November.
2. Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001.
3. Amish Kumar , Mrs. Namita Tiwari,"Efficient implementation and avalanche effect of AES" International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 3/4, August 2012.
4. Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu, National Tsing Hua University,"A high throughput low cost AES processor" IEEE Communications Magazine 63-804/03 © 2003 IEEE.
5. Chong Hee Kim,"Improved Differential Fault Analysis on AES Key Schedule" IEEE Transaction on Information Forensics and Security, Vol. 7, No. 1, Feb 2012.
6. Diaa Salama Abdul. Elminaam, Hatem M. Abdul Kader and Mohie M. Hadhoud," Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices" International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October, 2009.
7. Irbid, Jordan, "A new approach for complex encrypting and decrypting data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.
8. J. Nechvatal, et. al., Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.
9. Mohan H.S and A Raji Reddy,"Performance analysis of AES and MARS encryption algorithm" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.
10. Navraj Khatri, Rajeev Dhanda , Jagtar Singh ,"Comparison of power consumption and strict avalanche criteria at encryption/Decryption side of Different AES standards""International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 4, August 2012.
11. Xinmiao Zhang and Keshab K. Parhi,"Implementation approaches for the advanced encryption standard algorithm", IEEE Transactions 1531-636X/12©2002IEEE.