AN ENHANCEMENT ON BLOCK CIPHER KEY WRAPPING ALGORITHM OF THE ADVANCED ENCRYPTION STANDARD

Ratnesh Kumar Jain*

Prof. Dileep Singh**

Abstract:

AES is the Advanced Encryption Standard, a United States government standard algorithm for encrypting and decrypting data. With the fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission. Cryptography has come up as a solution which plays a vital role in information security system against various attacks. This security mechanism uses some algorithms to scramble data into unreadable text which can be only being decoded or decrypted by party those possesses the associated key. Two types of cryptographic techniques are being used: symmetric and asymmetric. In this paper we have used symmetric cryptographic technique AES (Advance encryption standard) having 288 bit block as well as key size. And the same conventional 128 bit conventional AES algorithm is implemented for 288 bit using 6*6 Matrix. After the implementation, 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.

* M.Tech, IV SEM, Department of Computer Science & Engineering, Gyan Ganga Institute of Technology & Management, Bhopal

** Head of the Department, Department of Information Technology, Gyan Ganga Institute of Technology & Management, Bhopal

1. Introduction

The AES algorithm defined by the National Institute of Standards and Technology (NIST) of the United States has been widely accepted to replace DES as the new symmetric encryption algorithm [2]. The AES algorithm is a symmetric block cipher that processes data blocks of 128 bits using a cipher key of length 128, 192, or 256 bits. Each data block consists of a 4 × 4 array of bytes called the state, on which the basic operations of the AES algorithm are performed [2].The proposed algorithm differs from conventional AES as it has 200 bits block size and key size 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 cipher. AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [3].

Existing Method:

1.1 The AES Algorithm

AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits;8 called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds.

The main loop of AES9 performs the following functions:

- **SubBytes()**
- **ShiftRows()**
- **MixColumns()**
- **AddRoundKey()**

The first three functions of an AES round are designed to thwart cryptanalysis via the methods of "confusion" and "diffusion." The fourth function actually encrypts the data. Claude Shannon described the concepts of confusion and diffusion in his seminal 1949 paper, "Communication Theory of Secrecy Systems:" "Two methods … suggest themselves for frustrating a statistical analysis. These we may call the methods of *diffusion* and *confusion*."10 Diffusion means patterns in the plaintext are dispersed in the ciphertext. Confusion means the relationship between the plaintext and the ciphertext is obscured.

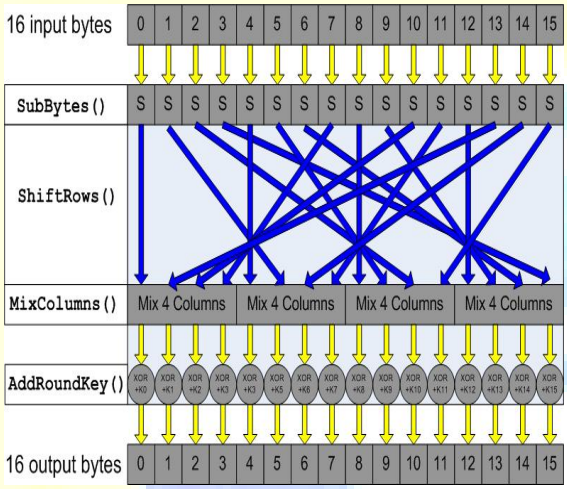
A simpler way to view the AES function order is:

1. Scramble each byte (SubBytes).
2. Scramble each row (ShiftRows).

3. Scramble each column (MixColumns).

4. Encrypt (AddRoundKey).

A term associated with AES is "the State," an 'intermediate cipher,'11 or the ciphertext before the final round has been applied. AES formats plaintext into 16 byte (128-bit) blocks, and treats each block as a 4x4 State array. It then performs four operations in each round. The arrays contains row and column information used in the operations, especially MixColumns() and Shiftrows().



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 Fig. 4.

For implementation issues relating to the key length, block size and number of rounds, see Sec.

	Key Leng	Block Size	Number of Rounds

	th (*Nk words*)	(*Nb words*)	(*Nr*)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

2 Problem Statements

There are various problems and issues with the AES.

2.1 Key Length Requirements

An implementation of the AES algorithm shall support *at least one* of the three key lengths specified in Sec. 5: 128, 192, or 256 bits (i.e., ***Nk*** = 4, 6, or 8, respectively). Implementations may optionally support two or three key lengths, which may promote the interoperability of algorithm implementations.

2.2 Higher encryption and decryption time

The encryption and decryption time for various AES standards is very high. If large block of data is concluded for AES-128, AES-192, AES- 256 so encryption time per bit is increased and decryption time per bit is decreased .T

2.3 Throughput Rate

The throughput of various AES standards is less and concluded that the throughput at encryption ends of AES-128, AES-192 and AES-256. The decryption process of conventional AES is very high.

2.4 Security problem in high data rate

The Security of the AES model is examined by performing the various tests: 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 and the AES algorithm falls within the average level of security. Hence, it can be said that the AES model is not much secure and cannot be considered for communication where high data rate is required.

3 Proposed Work

3.1 Encryption Algorithm

At the start of encryption, 288 bit input is copied to the State array of 6*6 matrixes. The data bytes are filled first in the column then in the rows. Then after the initial round key addition, ten rounds of encryption are performed. The first nine rounds are same, with small difference in the final round. As illustrated in fig.2 each of the first nine rounds consists of 4 transformations:

SubBytes, ShiftRows, MixColumns and AddRoundKey. But in final round Mixcolumns transformation is not used.

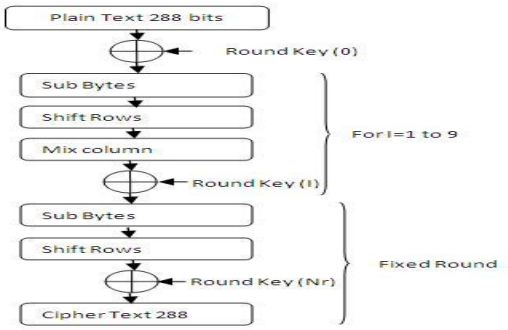


Fig.2: Encryption Structure of the AES algorithm

3.1.1 SubBytes Transformation— In this transformation, each of the byte in the state matrix is replaced with another byte as per the S-box (Substitution Box). The S-box is generated by firstly calculating the respective reciprocal of that byte in GF (2^8) and then affine transform is applied. The S-box used for this transformation.

3.1.2 ShiftRows Transformation— In this transformation, the bytes in the first row of the State do not change. The second, third, fourth and fifth rows shift cyclically to the left by one byte, two bytes, three bytes and four bytes respectively.

3.1.3 MixColumns Transformation— It is the operation that mixes the bytes in each column by the multiplication of the state with a fixed polynomial matrix [2]. It completely changes the scenario of the cipher even if the all bytes look very similar. The Inverse Polynomial Matrix does exist in order to reverse the mix column transformation.

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

3.2 Decryption Algorithm

Decryption is the process of extracting the plaintext from cipher text. The Decryption structure of proposed algorithm as shown in fig.3 is obtained by inverting the encryption structure which is shown above. Corresponding to the transformations in the encryption, InvSubBytes, InvShiftRows, InvMixColumns, and AddRoundKey are the transformations used in the

decryption as shown in Fig3. below. The roundkeys are the same as those in encryption generated by Key Expansion, but are used in reverse order [1].

3.2.1 InvSubBytes Transformation—InvSubBytes is the inverse transformation of SubBytes, in which the inverse *S*-box is applied to individual bytes in the State. The inverse *S*-box is constructed by first applying the inverse of the affine transformation in (1), then computing the multiplicative inverse in GF(2^8). The inverse S-box used for this transformation.

3.2.2 InvShiftRows Transformation—InvShiftRows is the inverse transformation of ShiftRows. In this transformation, the bytes in the first row of the State do not change; the second, third, and fourth and fifth rows are shifted cyclically by one byte, two bytes, three bytes and four bytes to the right respectively [1].

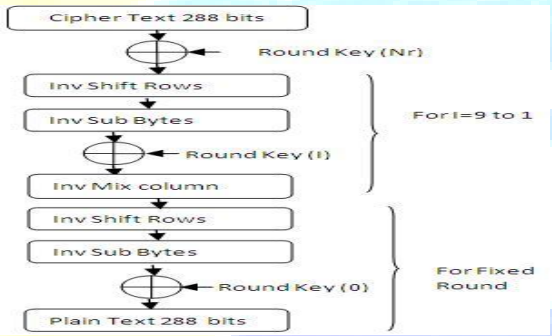


Fig.3: Decryption Structure of the AES algorithm.

3.2.3 InvMixColumns Transformation— InvMixColumns is the inverse transformation of MixColumns. This is a complex procedure as it involves severely the byte multiplication under GF (2^8). The whole state is to be multiplied with pre-defined matrix called inverse polynomial matrix.

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.

4 Conclusion

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 4 rows and 4 columns. 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 diffusion takes place in form of matrix multiplication under finite field. Having a bigger block, hence, requires a new matrix of size 6* 6, 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.

5 References

[1] Xinmiao Zhang and Keshab K. Parhi,"Implementation approaches for the advanced encryption standard algorithm", IEEE Transactions 1531-636X/12©2002IEEE.

[2] 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 0163-6804/03 © 2003 IEEE.

[3] 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.

[4] "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publication 197, November 26, 2001.

[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] Irbid, Jordan, "A new approach for complex encrypting and decrypting data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.

[7] 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

[8] 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.

[9] 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.

[10] J. Nechvatal, et. al., Report on the Development of the Advanced Encryption Standard (AES), National Institute of Standards and Technology, October 2, 2000.

[11] A. Lee, NIST Special Publication 800-21, Guideline for Implementing Cryptography in the Federal Government, National Institute of Standards and Technology, November 1999