Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementation of AES Using S-Box Rotation

Bahar Saini
CSE& Kurukshetra University
Haryana, India

Abstract— AES algorithm is considered as a secured algorithm. Still, some security issue lie in the S-box and key used In this paper, we have tried to give focus on the S-box rotation so that we get highly secured information .As the standard AES consists of four stages while in the new design, it consists of five stages The extra stage is known as S-box rotation .Implementation of proposed work and Experimental results are to be discuss here.

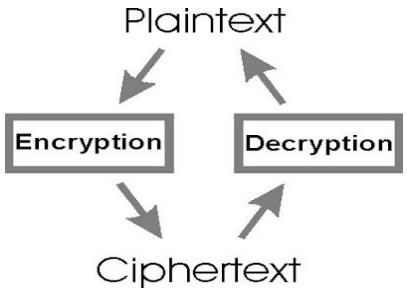
Keywords— AES ***(Advanced Encryption algorithm), Entropy, Confusion, Diffusion, Cryptography, S-box***

I. INTRODUCTION

In the current scenario of web, user information gets highest priority within the field of information communication. This information must be sent firmly so as to keep the web usage reliable. For this security of information, numerous ways have been discovered. Some admired ways are cryptography and steganography

1.1 CRYPTOGRAPHY

Cryptography is a Greek word that virtually means that the art of writing secrets. In practice, cryptography is that the task of transforming data into a type that's unintelligible, but at the same time allows the intended recipient to retrieve the original data using a secret key. Cryptographic algorithms (or ciphers, as they are often called) are special programs designed to protect sensitive data on open communication links. During encryption, ciphers transform the original plaintext message into unintelligible cipher text. Decryption is that the method of retrieving plaintext from cipher text.



1.2 AES (Advanced Encryption Algorithm)

AES is an iterated symmetric block cipher, which implies that:

- AES works by repetition a similar outlined steps multiple times.
- AES could be a secret key encryption algorithm.
- AES operates on a predetermined number of bytes

AES in addition as most encryption algorithms is reversible. This means that nearly similar steps are performed to finish both encryption and decryption in reverse order. The AES algorithm operates on bytes that make it easier to implement and justify.

This key is expanded into individual sub keys, a sub keys for every process round. This methodology is termed KEY EXPANSION. As AES is associate iterated block cipher. All that means is that the similar operations are performed many times on a fixed number of bytes.

There are four different stages in AES round. They are:

- *SubByte transformation*: (S-box substitution) provides non linearity and confusion, created by multiplicative inverse and transformation.
- *ShiftRow*: (rotations) provides inter-column diffusion wherever the bytes within the last three rows of the states are cyclically shifted.
- *MixColumn:* (linear combination) provides inter-byte diffusion wherever every column vector is multiplied by a fixed matrix. The bytes are treated as polynomials instead of numbers.
- *AddRoundKey*: (round key bytes XOR with every byte of the state and the round key) provides confusion [6].

The encryption method begins with an AddRoundKey stage, and followed by 9 rounds of SubBytes, MixColums, ShiftRows, and AddRoundKey transformation. The transformation are performed respectively and iteratively (Nr times) depending on the key length. The final round will only include three stages; ShiftRows, SubByte, and AddRoundKey. All of the operations are byte-oriented [6].

© 2014, IJARCSSE All Rights Reserved

1.3 Entropy

The entropy of a document is an index of its information content. The entropy is measured in bits per character. To calculate the information content one examines the probability distribution of this source.

Information content (M[i]):= log (1/p[i]) = -log (p[i])

Where p[i] is the probability that message M[i] is transmitted by the message source and log denotes logarithms to base 2.

With the aid of the information content of the individual messages, the average amount of information which a source with a specified distribution delivers can be calculated. The entropy of a source therefore indicates its characteristic distribution. The average amount of information which one can obtain through observation of the source or, conversely, the indeterminacy which prevails over the generated messages when one cannot observe the source is measured.

II. RELATED STUDY

Prof. Kalpesh Rakholiya et.al [1], the author describes cryptography, many symmetric key algorithms in detail and then proposes a new symmetric key algorithm. Algorithms for each encoding and decoding are provided here. The benefits of this new algorithm over the others are also explained.

Shivangi Goyal et.al [2], the author gave a brief outline of cryptography, whenever it's applied and its usage in various forms. It provides data, electronic signatures, confidentiality, integrity and advanced user authentication. The ways of cryptography use mathematics for securing the data.

Gurvinder Singh Sandhu et.al [3], the author compares and analyzes standard symmetric key encryption algorithms using numerous performance metrics. Their problems associated options are highlighted in so as to provide the researchers an improved problem formulation and come up with best solutions with in the area of cryptography and steganography.

Amritpal Singh et.al [4], the author projected the 2 main characteristics that determine and differentiate encryption algorithm from another are their effectiveness and speed in securing the data and their capability to secure the protected knowledge against attacks. In this paper a relative study between 4 such wide used encryption algorithms DES, AES, RSA and 3DES on the thought of their ability to guard and secure information against speed and attacks of encryption and decryption.

Nagesh Kumar et.al [5], the author provides a fair comparison between 3 most familiar symmetric key cryptography algorithms: AES, Blowfish and DES. The comparison is formed on the idea of those parameters: block size, key size and speed. Simulation program is implemented using Java programming

Julia Juremi et.al [6], the author presents a new AES-like style for key- dependent AES using S-box rotation. The algorithmic rule involves key expansion algorithm at the side of S-box rotation and this property can be used to make the S-box key-dependent, hence providing a more security to the block cipher. Fixed S-box permits attackers to study S- box and find weak points while by using key-dependent S-Box approach, it makes it difficult for invader to do any offline analysis of an attack of one particular set of S- boxes. The cipher structure is similar to the standard AES, only the S-box is made key-dependent without changing the value. This new style is tested using the NIST Statistical Test and will be further crypt analyzed with algebraic attack in order to allow its subversion or evasion.

Sumitra et.al [7], the main goal of author is to keep the data secure from unauthorized access because the Cryptography renders the message unintelligible to outsider by numerous transformations. Information Cryptography is that the scrambling of the content of information likes video, audio, text to make it.

Akanksha Mathur et.al [8], the author presented an algorithm for cryptography which is based on ASCII values of characters among the plaintext. This algorithm is used to encrypt knowledge by using ASCII values of the information to be encrypted. modified key are going to be used.

Kritika Acharya et.al [9], the author demonstrates the basic differences between the existing encryption techniques. Cryptography plays an important role in securing information. It is used to ensure that the contents of a message are confidentially transmitted and it would not be altered. Network security is very important component in information security as it refers to all hardware and software function, characteristics, operational procedures, features, access control ,accountability, and administrative and management policy..

Shaaban Sahmoud et.al [10], the author developed a further powerful algorithm for cryptography. This algorithm is based on AES to inducecompetely different sub keys from the initial key and using each sub key to encrypt.Author used AES to safegaurd their style from structural analysis.

III. PROPOSED WORK

The algorithm involves key expansion algorithm together with S-box rotation and this property can be used to make the S-box key-dependent, hence providing a more robust security to the block cipher. Fixed S-box permits attackers to check S-box and realize weak points whereas by using key-dependent S-Box approach, it makes it difficult for invader to do any offline analysis of an attack of one particular set of S-boxes. The cipher structure is similar to the original AES; solely the S-box is formed key-dependent without changing the value.

IV. RESULTS AND DISCUSSION

4.1 S-Box Rotation

In AES, rotation happens in key expansion, deciphering, and ciphering. Rotation is important for confusion and diffusion that play a vital role in any cryptography technique. Diffusion and confusion make breaking the key complicated and tough [11].

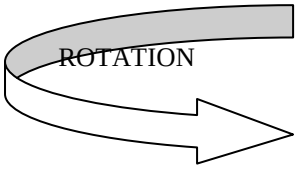
© 2014, IJARCSSE All Rights Reserved

The main purpose of rotation is to combine all information components in different columns of state. As such, rotation is vital for confusion and diffusion, that each play an important role in cryptography. Confusion means that to form the output dependent on the key. Ideally, every key bit influences every output bit.

Diffusion is creating the output dependent on previous input (plain and cipher text). Ideally, each previous input bit influences every output bit. One aim of confusion is to form it very difficult to seek the key even if one has a large number of plaintext-cipher text pairs produced with the same key. Therefore, every bit of the cipher text should rely on the whole key and in different ways on different bits of the key [11].

In the subByte phase, the information in the plain text is substituted by some pre-defined values from a substitute box. The substitute box is employed normally, is AES S-box. In this paper, we have done s-box rotation by rotating the fixed s-box matrix into transpose of fixed s-box matrix, a new matrix has been developed named rs-box i.e. we convert the rows of fixed s-box into column for new rs-box and the column of the fixed s-box into rows for new rs-box. With the assistance of new rs-box, a new proposed-AES has been developed. The fig shows the rotation to be done in s-box to get rs-box.

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$



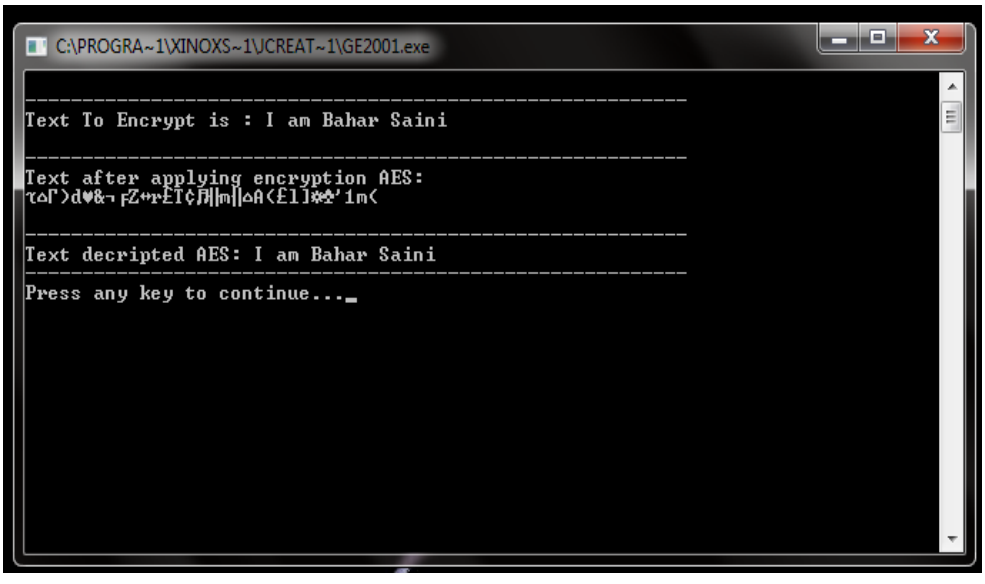
$S_{0,0}$	$S_{1,0}$	$S_{2,0}$	$S_{3,0}$
$S_{0,1}$	$S_{1,1}$	$S_{2,1}$	$S_{3,1}$
$S_{0,2}$	$S_{1,2}$	$S_{2,2}$	$S_{3,2}$
$S_{0,3}$	$S_{1,3}$	$S_{2,3}$	$S_{3,3}$

4.2 IMPLEMENTATION

The below fig represent the implementation of proposed work in java.

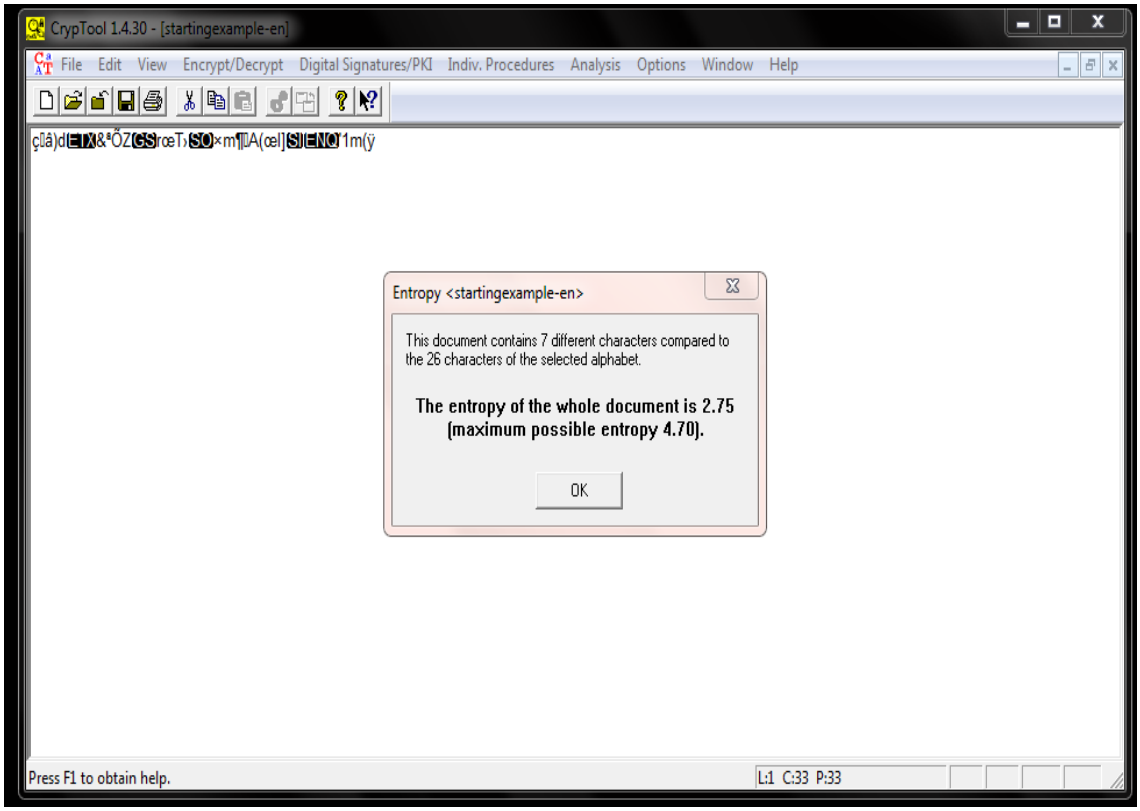
```
private static byte[][] rSubBytes(byte[][] state) {
byte[][] tmp = new byte[state.length][state[0].length];
            for (int col = 0; col < 4; col++)
            for (int row = 0; row < Nb; row++)
            tmp[col][row] = (byte) (rsbox[(state[col][row] & 0x000000ff)] & 0xff);
          return tmp;
            }
private static byte[][] SubBytes(byte[][] state) {
  byte[][] tmp = new byte[state.length][state[0].length];
                        for (int row = 0; row < 4; row++)
                        for (int col = 0; col < Nb; col++)
                        tmp[row][col] = (byte) (sbox[(state[row][col] & 0x000000ff)] &
0xff);
                      return tmp;
                    }
```

The program is compiled using the default setting in jdk1.6 development kit for java. After executing the program, following output is to be displayed on the screen. The resulting screen shot of the output is shown below



© 2014, IJARCSSE All Rights Reserved

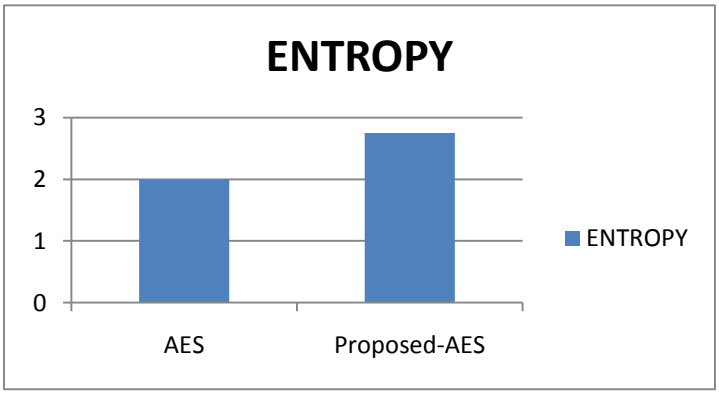
The result of the proposed AES has been analysed using cryptool 1.4.30. The entropy of the proposed AES is 2.75.



Now we have compared the entropy of both AES and proposed-AES. From the evaluation table, we see that entropy of proposed-AES is higher than AES.

	ENTROPY
AES	**2.00**
Proposed-AES	**2.75**

The bar graph among AES and proposed-AES has been shown as under



V. CONCLUSIONS

In this paper, a new design for enhancing the security of AES algorithm is proposed. This approach design will not contradict the security of the original AES algorithm by keeping all the mathematical criteria of AES remain unchanged. We try to improve the security of AES by making its S-box to be key-dependent using key expansion algorithm together with S-box rotation. We also show cryptanalysis of the results by using crypTool.

© 2014, IJARCSSE All Rights Reserved

REFERENCES

[1] Prof. Kalpesh Rakholiya, Research Expo International Multidisciplinary Research Journal Available online at www.researchjournals.in Volume – II, Issue – III September – 2012

[2] Shivangi Goyal International Journal of Science and Technology Volume 1 No. 3, March, 2012 IJST.

[3] Gurvinder Singh Sandhu, Vinay Verma, International Journal of Advance Research in Computer Science and Management Studies Volume 1, Issue 7, December 2013.

[4] Amritpal Singh, Mohit Marwaha, Baljinder Singh, Sandeep Singh, International Journal of computer & technology, Vol 9, No 3.

[5] Nagesh Kumar, Jawahar Thakur, Arvind Kalia, An International Journal of Engineering Sciences ISSN: 2229-6913 Issue Sept 2011, Vol. 4.

[6] Julia Juremi Ramlan Mahmod Salasiah Sulaiman Jazrin Ramli,International Journal of Cyber-Security and Digital Forensics (IJCSDF) 1(3):

[7] Sumitra, International Journal of Scientific and Research Publications, Volume 3, Issue 1, January 2013.

[8] Akanksha Mathur International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 09 Sep 2012.

[9] Kritika Acharya, Manisha Sajwan, Sanjay Bhargava International Journal of Computer Applications Technology and Research Volume 3 – Issue 2.

[10] Shaaban Sahmoud, Wiram Elmasy, Shadi Abudalfa, International Arab Journal of e-Technology., Vol.3, No.1, Jan2013.

[11] I.A.Ismil ,Galal H.Galal-Edeen, Sherif Khattab and Mohamed ABD Elhamid I.Moustafa El Bahtity, International Journal of Reviews in Computing, Vol. 12, 31st December 2012.

© 2014, IJARCSSE All Rights Reserved