Developing New Cipher with Bigger Block Size Using S-Box Rotation

Nidhi Sharma
Assistant Prof. (CSE Dept.)
sharma.sunidhi.2000@gmail.com

Ritu Bala
M. Tech Scholar (CSE Dept.)
preet26266@gmail.com

Abstract: **Cryptography encodes info in such a way that no-one will scan it, except the one who holds the key. Additional advanced crypto techniques make sure that the knowledge being transmitted has not been changed in transit. With the advent of electronic commerce and portable devices for communication, cryptology has become an exceedingly important science in the present day. The diversity of applications in which crypto-algorithms have to operate has increased and hence the requirements for efficient algorithms have grown. AES algorithm is considered as a secured algorithm. Still, some security issue lies in the S-box and key used. In this paper, the focus is given on S-box rotation together with the key expansion algorithm with so that we design a new AES like design that makes the information highly secured. Implementation is done using Java and the program is compiled using the default setting in jdk1.6 development kit for java. Also all the analyses are to be done using CrypTool 1.4.30. CrypTool is free software and an e-learning tool illustrating cryptographic concepts with graphical user interface.**

Keywords: Cryptography, AES, S-Box, Autocorrelation, Entropy.

I. INTRODUCTION

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. Data integrity is quite a issue in security and to maintain that integrity we tends to improve as to provides the better encryption processes for security. Network security is sometimes more than what people always thought it to be malware, virus, Trojan, hackers. Network security could be caused by unintentional human error and it could be compromised by human nature as well. Various other issues have been analyzed such as scalability i.e. Key size and block size variation is referred as scalability, Encryption ratio i.e. Measures amount of data that is to be encrypted and Key length Value i.e. it plays a vital role that shows how data is encrypted. From these problem analysis, we focus primarily on two objectives: Firstly, Comparison of various encryption algorithms and then finds best available one algorithm for the network security. Secondly, to develop new AES-like design for key dependent AES using S-box rotation. For required research we are working on well-known cryptographic algorithm "AES". Cryptography is that the study of Secret (crypto)-Writing (-graphy). It is the science or art of encompassing the principles and methods of transforming an intelligible message into coded type or unreadable type and that coded type then transforming the message back to its original type. Because the field of cryptography has advanced; cryptography these days is assumed as the study of techniques and applications of securing the integrity and authenticity of transfer of data under difficult circumstances.

AES (ADVANCED ENCRYPTION ALGORITHM)

The Advanced Encryption Standard is the United State Government standard for symmetric encryption. AES is a block cipher that encrypts a 128-bit block (plaintext) to a 128-bit block (cipher text), or decrypts a 128-bit block (cipher text) to a 128-bit block (plaintext).AES uses a key (cipher key) whose length can be 128, 192, or 256 bits. Hereafter encryption/decryption with a cipher key of 128, 192, or 256 bits is denoted AES- 128, AES192, AES-256, respectively. AES-128, AES-192, AES-256 process the data block in, respectively, 10, 12, or 14 iterations of a pre-defined sequence of transformations, which are also called "rounds" (AES rounds) for short. The rounds are identical except for the last one, which slightly differs from the others (by skipping one of the transformations). The rounds operate on two 128-bit inputs: "State" and "Round key". Each round from 1 to 10/12/14 uses a different Round key. The 10/12/14 round keys are derived from the cipher key by the "Key

Expansion" Algorithm. The key could be generated and scheduled in each round to get the encrypted data. Table 2 shows the number of rounds as a function of key length.

Table I: Different AES specifications

AES Version	**Key Length (Nk words)**	**Block Size (Nb words)**	**Number of Rounds (Nr rounds)**
AES126	4	4	10
AES192	6	4	12
AES256	8	4	14

There are four basic operations carried out in each round of the AES algorithm, they are

i) Sub-byte

ii) Shift row

iii) Mixed column

iv) Add Round Key

Block Cipher and S-Box

If block ciphers are used for encryption, messages are divided into data blocks of a fixed length and each block is treated as one message in either M or C. For many older block ciphers the block size is 64 bits (e.g., DES), while the block size for new designs is usually 128 bits (e.g., AES). Usually, a block cipher consists of a round function that is iterated for several rounds. In each round, an appropriate transformation is applied using a subkey derived from the original secret key. These subkeys are generated by the key scheduling algorithm of the cipher. Every round makes cryptanalysis of the cipher more difficult, thus improving security. Inevitably, every round added to the cipher also makes the cipher slower as more computations are required. The transformation SubBytes is a nonlinear byte substitution that operates on each byte of the State using a table (S-box). The numbers of the table is computed by a finite field inversion followed by an affine transformation. The resulting table is called an S-box. Block cipher systems depend on the S-boxes, which are fixed and have no relation with the secret key. So only changeable parameter is the secret key. Since the only nonlinear component of AES is S-boxes, they are an important source of cryptographic strength.

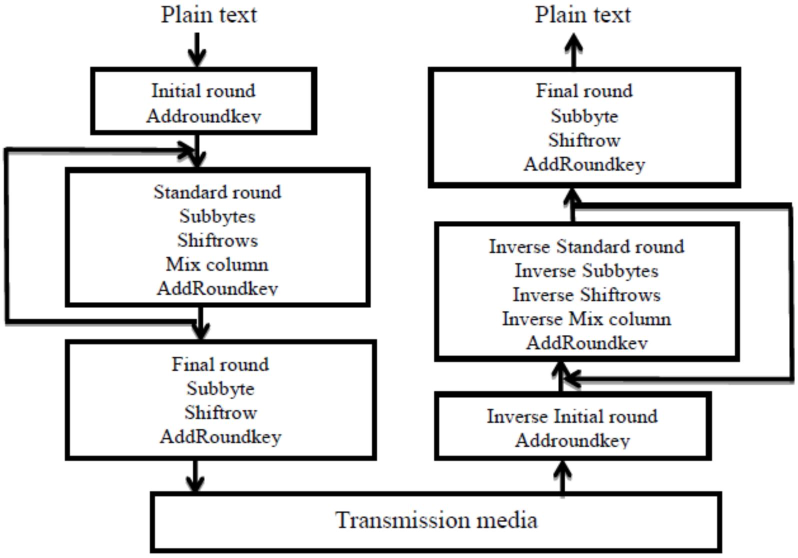


Figure 1: AES

II. RELATED WORK

Several researchers and scholars work in different areas and related parameters in order to improve security in the proposed system.

Ritu Pahal et al [1], used symmetric cryptographic technique AES (Advance encryption standard) having 200 bit block as well as key size. And the same conventional 128 bit conventional AES algorithm is implemented for 200 bit using 5*5 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.

Alan Kaminsky et al [2], said that since its release in November 2001, the Advanced Encryption Standard (NIST FIPS-197) has been the subject of extensive cryptanalysis research. The importance of this research has intensified since AES was named, in 2003, by NSA as a Type-1 Suite B Encryption Algorithm (CNSSP-15). As such, AES is now authorized to protect classified and unclassified national security systems and information. This paper provides an overview of current cryptanalysis research on the AES cryptographic algorithm. Discussion is provided on the impact by each technique to the strength of the algorithm in national security applications. The paper is concluded with an attempt at a forecast of the usable life of AES in these applications.

Amritpal Singh et al [3], In today world importance of exchange of data over internet and other media type is eminent; the search for best data protection against security attacks and a method to timely deliver the data without much delay is the matter of discussion among security related communities. Cryptography is one such method that provides the security mechanism in timely driven fashion. Cryptography is usually referred to as "the study of secret", which is most attached to the definition of encryption. The two main characteristics that identify and differentiate encryption algorithm from another are their capability to secure the protected data against attacks and their speed and effectiveness in securing the data. This paper provides a comparative study between four such widely used encryption algorithms DES, of DES, 3DES, AES and RSA on the basis of their ability to secure and protect data against attacks and speed of encryption and decryption.

Shaaban Sahmoud et al [4], in this paper author developed a more powerful algorithm for cryptography. This algorithm is based on AES to generate different sub keys from original key and using each sub key to encrypt one AES block. We used AES to protect our design from structural analysis, became AES is very resistance to this type of attacks. From other side generating many keys from symmetric key resists modern attacks on symmetric-key cryptography. Experiment results are shown in this paper to demonstrate the effectiveness of our design.

Chittaranjan Pradhan et al [5], Advanced Encryption Standard (AES) algorithm is considered as a secured algorithm. Still, some security issues lie in the S-Box and the key used. In this paper, author has tried to give focus on the security of the key used. Here, the proposed modified algorithms for the AES have been simulated and tested with different chaotic variations such as 1-D logistic chaos equation, cross chaos equation as well as combination of both. For the evaluation purpose, the CPU time has been taken as the parameter. Though the variations of AES algorithms are taking some more time as compared to the standard AES algorithm, still the variations can be taken into consideration in case of more sensitive information. As we are giving more security to the key used for AES algorithm, our proposed algorithms are very much secured from unauthorized people.

Shivangi Goyal et al [6], this paper gives a brief summary of cryptography, where it is applied and its usage in various forms. Cryptography is a way of safeguarding the crucial data from unauthorized access. It has emerged as a secure means for transmission of information. It mainly helps in curbing intrusion from third party. It provides data confidentiality, integrity, electronic signatures, and advanced user authentication. The methods of cryptography use mathematics for securing the data (encryption and decryption).

N.Lalitha et al [7], in this paper author propose a data hiding technique using AES algorithm. Steganography and Cryptography are two popular ways of sending vital information in a secret way. Cryptography was introduced for making data secure. But alone cryptography cannot provide a better security approach because the scrambled message is still available to the eavesdropper. There arises a need of data hiding. So here we are using a combination of steganography and cryptography for improving the security. There are many cryptography techniques available; among them AES is one of the most useful techniques. In Cryptography, I have using AES algorithm to encrypt a message using 128 bit key the message is hidden. In this proposed technique, we use advance hill cipher and AES to enhance the security level which can be measured by some measuring factors. The result of this work shows that this advance hybrid scheme gives better results than previous techniques.

Sweta K. Parmar et al [8], Security is the most challenging aspects in the internet and network application. Internet and networks applications are growing very fast, so the importance and the value of the exchanged data over the internet or other media types are increasing. Information security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Encryption technique plays a main role in information security system. This paper gives a comparison of various encryption algorithms and then finds best available one algorithm for the network security.

Akanksha Mathur et al [9], presented an algorithm for data encryption and decryption which is based on ASCII values of characters in the plaintext. This algorithm is used to encrypt data by using ASCII values of the data to be encrypted. The secret used will be modifying o another string and that string is used as a key to encrypt or decrypt the data. So, it can be said that it is a kind of symmetric encryption algorithm because it uses same key for encryption and decryption but by slightly modifying it. This algorithm operates when the length of input and the length of key are same.

Mohammad Soltani et al [10] in this paper, author suggested a new robust cryptography algorithm to increase security in the Symmetric-key producing algorithm. The main features of cryptography algorithm defined in this article are the ability to encrypt the secret file in successive stages, changing the physical structure of the secret file, no limitation for the number of keys, Creating five keys at each stage of cryptography, storing a part of secret file at one of the keys at each stage of cryptography, Interdependence of all keys in all stages of encrypting and decrypting, To make the keys interdependent and to encrypt the secret file by each of them, there are 2 independent algorithms to select the type of algorithm needed to make the keys interdependent by the user, bigger changes in the physical structure of the encrypted file In case of wrong decryption and to make the resulting keys and encrypted file unique after the cryptography process.

III. PROPOSED WORK

In our proposed work, we use s-box rotation with key expansion algorithm developing new Cipher (A new AES model having bigger block size rather than conventional (128, 192 and 256 bits AES); this property can be used to make the S-box key-dependent, hence providing a better security to the block cipher.

Objectives of the Present Work

The object of this proposal is an AES cipher using key-dependent S-boxes. The fact that the S-boxes are unknown is one of the main strength of our cipher system, since both linear and differential cryptanalysis require known S-boxes. The algorithm involves key expansion algorithm together with S-box rotation with bigger block size rather than conventional (128, 192 and 256 bits AES 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.

Implementation

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. 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. 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 research, 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 s-box.

IV. RESULTS AND DISCUSSION

The result is implemented in java and it has been analyzed using CrypTool. In this result we have compared the proposed AES with original AES design.

Evaluation Parameters

1) Entropy

The entropy of a document is an index of its information content. The entropy is measured in bits per character. The information content of a message M[i] is defined by

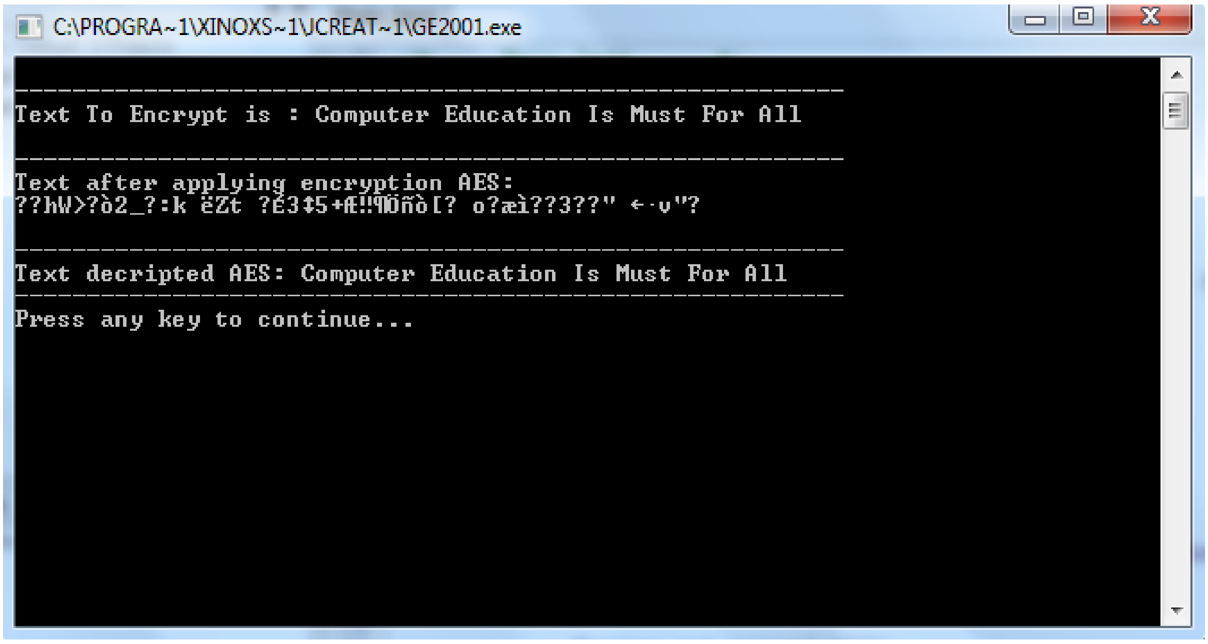
Information content (M[i]):= log(1/p[i]) = -log(p[i])

Where p[i] is the probability that message M[i] is transmitted by the message source and log denotes logarithms to base 2 (as indeed it does elsewhere in this document).

RESULTANT SCREENSHOTS

a) Proposed-AES

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:



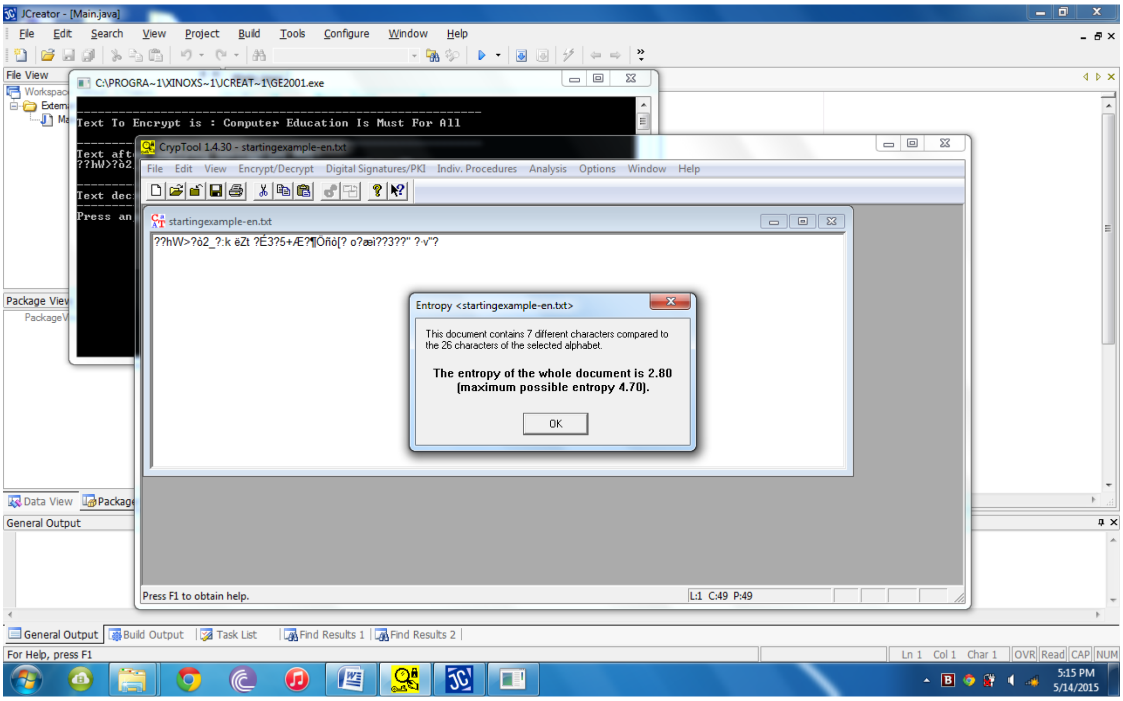
```
-----------------------------------------------------------
Text To Encrypt is : Computer Education Is Must For All

-----------------------------------------------------------
Text after applying encryption AES:
??hW>?ò2_?:k ëZt ?É3‡5+Æ‼¶Öñò[? o?æì??3??" ←·υ"?

-----------------------------------------------------------
Text decripted AES: Computer Education Is Must For All
-----------------------------------------------------------
Press any key to continue...
```

Screenshot 1: Proposed AES

The result of the proposed AES has been analyzed using cryptool 1.4.30.Here, initially we enter the text to be encrypted. After that AES is applied on the input text that makes the data secret. The decryption process again decrypts the text. The entropy is measured in bits per character.


JCreator - [Main.java]
File Edit Search View Project Build Tools Configure Window Help
C:\PROGRA~1\XINOXS~1\JCREAT~1\GE2001.exe
CrypTool 1.4.30 - startingexample-en.txt
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en.txt
Entropy <startingexample-en.txt>
OK
Press F1 to obtain help.
General Output
For Help, press F1

```
------------------------------------------------------------
Text To Encrypt is : Computer Education Is Must For All
```

```
??hW>?ò2_?:k ëZt ?É3?5+Æ?¶Öñò[? o?æì??3??" ?·v"?
```

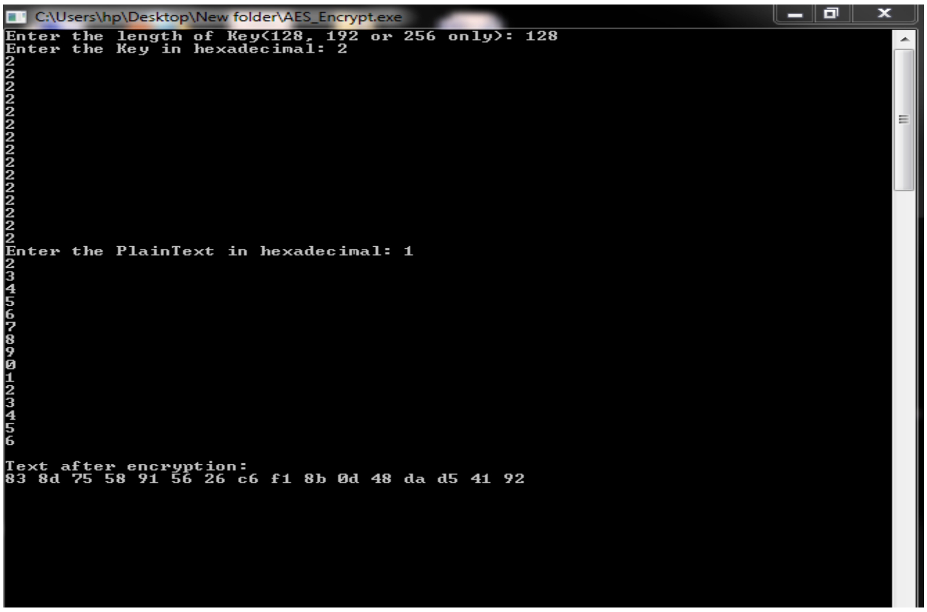
This document contains 7 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 2.80 (maximum possible entropy 4.70).

Screenshot 2: The entropy of the proposed AES is 2.80

b) AES

After executing the program, following output for encryption is to be displayed on screen. Firstly we enter the length of key (128,192 or 256), then enter the key in hexadecimal and lastly enter the plain text in hexadecimal. Now we get the text after encryption. The resulting screen shot of the output is shown below:

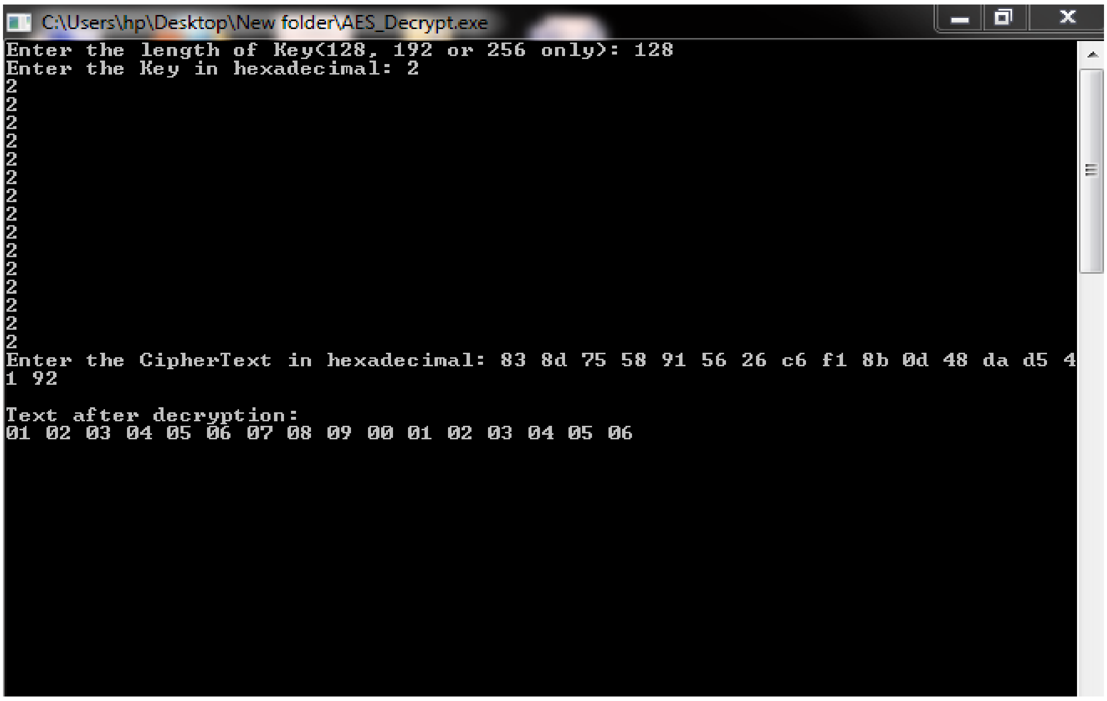


```
Enter the length of Key(128, 192 or 256 only): 128
Enter the Key in hexadecimal: 2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
Enter the PlainText in hexadecimal: 1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6

Text after encryption:
83 8d 75 58 91 56 26 c6 f1 8b 0d 48 da d5 41 92
```

Screenshot 3: AES Encryption

The screenshot shows the encrypted text using AES. After executing the decryption program, enter the length of key (128,192 or 256) then enter the key in hexadecimal.

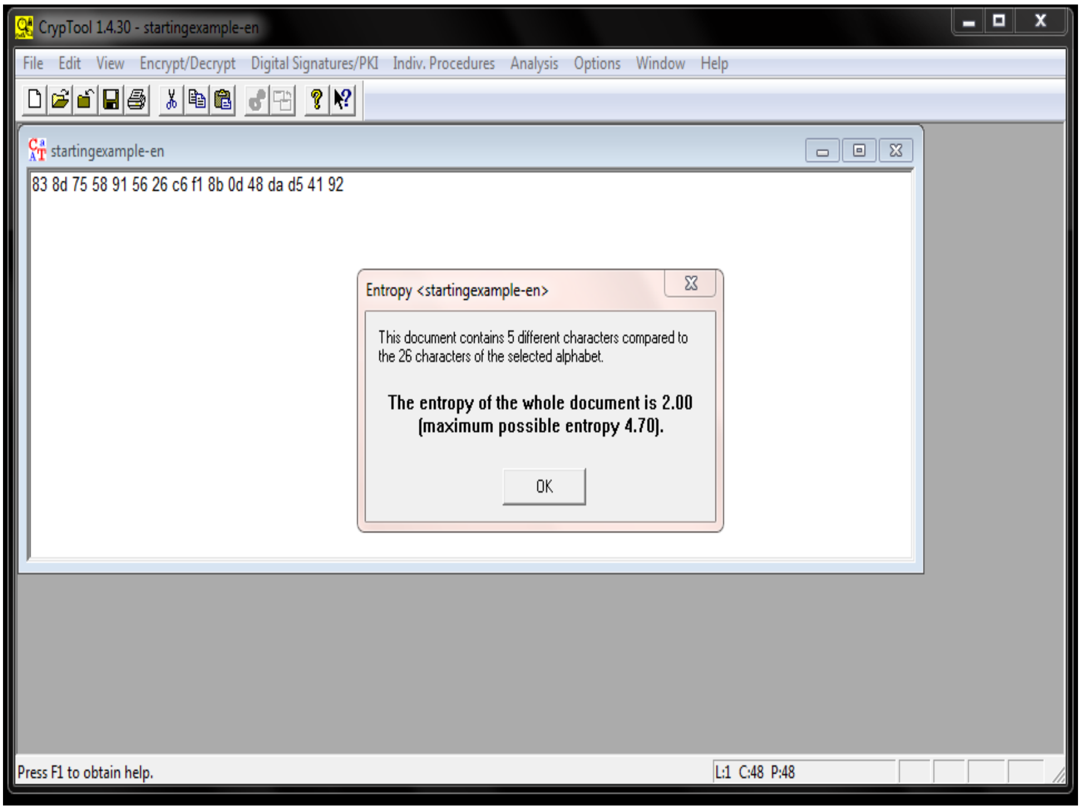


```
Enter the length of Key(128, 192 or 256 only): 128
Enter the Key in hexadecimal: 2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
2
Enter the CipherText in hexadecimal: 83 8d 75 58 91 56 26 c6 f1 8b 0d 48 da d5 4
1 92

Text after decryption:
01 02 03 04 05 06 07 08 09 00 01 02 03 04 05 06
```

Screenshot 4: AES Decryption

Same key is used here as it is used in encryption and lastly enters the cipher text in hexadecimal i.e. text after encryption. Now we get the text after decryption. Resulting screenshot is given above. Entropy of the cipher text is to be calculated using crypTool. The following screenshot display the entropy which is 2.00.


CrypTool 1.4.30 - startingexample-en
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
Entropy <startingexample-en>
OK

83 8d 75 58 91 56 26 c6 f1 8b 0d 48 da d5 41 92

This document contains 5 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 2.00 (maximum possible entropy 4.70).

Press F1 to obtain help. L:1 C:48 P:48

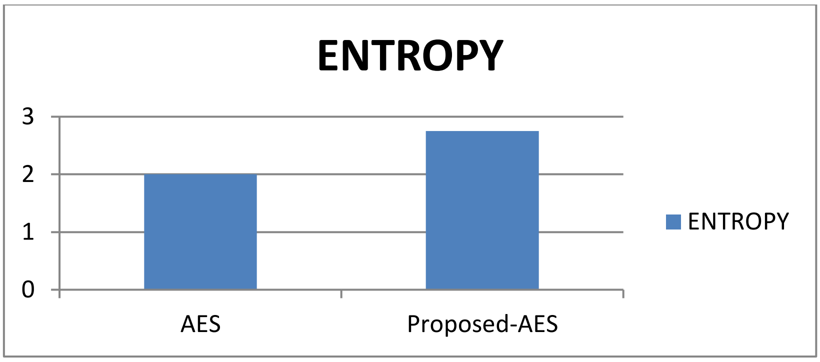
Screenshot 5: Entropy of AES

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.

Table II: Comparison between AES and Proposed-AES

	ENTROPY
AES	2.00
Proposed-AES	2.80

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



Graph 5.1: AES and proposed AES

V. CONCLUSION

Cryptography is the science of information and communication security. It is the science of secret codes, enabling the confidentiality of communication through an insecure channel. It protects against unauthorized parties by preventing unauthorized alteration of use. It uses a cryptographic system to transform a plaintext into a cipher text, using most of the time a key. Cryptography has an important role in the security of data transmission and is the best method of data protection against passive and active fraud. 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 crypt tool. Here we have done comparison between the entropy of proposed-AES and standard AES design and from the results we see that entropy of proposed-AES is higher than that of standard AES design, so proposed-AES is more secure than standard AES design.

REFERENCES

[1] E. F. Brickell, “A fast modular multiplication algorithm with application to two key cryptography”, in Advances in Cryptology: Proceedings of Crypto ’82. 1982

[2] R. Berger, S. Kannan, and R. Peralta. “A framework for the study of cryptographic protocols”, Advances in Cryptology: Proceedings of Cryto ’85 (Lecture Notes in Computer Science 218). Berlin, West Germany: Springer-Verlag, 1985

[3] Thomas Beth and Dieter Gollmann, “Algorithm Engineering for Public Key Algorithms”, IEEE Journal on selected areas in communication, VOL. 7. NO 4. May 1989

[4] Jorstad, Norman D.; “Cryptographic Algorithm Metrics “; Institute for Defense Analyses Science and Technology Division; 1997

[5] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis”, CRYPTO, LNCS 1666, pp.388-397, Springer, 1999.

[6] N. Sklavos and O. Koufopavlou, “Architectures and VLSI Implementations of the AES-Proposal Rijndael,” IEEE Trans. on Computers, vol. 51, Issue 12, pp. 1454-1459, 2002.

[7] Krishnamurthy, G. N., and Ramasvamy, V.: “Making AES Stronger:AES with Key Dependent S-Box”, IJCSNS International Journal of Computer Science and Network Security, vol.8, 2008 .

[8] Debnath Bhattacharyya, Poulami Das, Samir Kumar Bandyopadhyay and Tai-hoon Kim, “Text Steganography: A Novel Approach”,International Journal of Advanced Science and Technology”, Vol 3,2009

[9] D. S. Abdul. Elminaam, M. Abdul Kader, M. M. Hadhoud “Performance Evaluation of Symmetric Encryption Algorithms” IBIMA Volume 8, 2009

[10] I.A.Ismail,S.F. EI-Zoghdy,”A Secure Nominative Proxy Signature Scheme for Distributed Shared Object systems”,IJANA,Vol 2, Issue 1,2010

[11] V. S. Shankar Sriram, Abhishek Kumar Maurya, G.Sahoo,”A Novel Multiple Key Block Ciphering Mechanism with Reduced Computational Overhead”,International Journal of Computer Applications”, Vol.1 (No.17):25–30, February 2010

[12] Ferguson, N., Schneier, B., and Kohno T., “Cryptography Engineering: Design Principles and Practical Applications”. New York: John Wiley and Sons, 2010.

[13] Nagamalleswara Rao. Dasari, Vuda Sreenivasarao, “Performance of multiserver authentication and key management with user protection in network”,International Journal on Computer Science and Engineering, VOL.2, Issue 5, 2010

[14] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani “New Comparative Study between DES, 3DES and AES within Nine Factors” Journal of Computing, Volume 2, Issue 3, 2010

[15] Shasi Mehlrotra Seth, Rajan Mishra “Comparative Analysis of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, 2011.

[16] 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, 2011.

[17] “Identification in Voice over IP (VOIP) Networks”,Journal of Basic and Applied Scientific Research, 2011

[18] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha, “Throughput Analysis of Various Encryption Algorithms”, International Journal of Computer Science and Technology, Vol. 2, Issue 3, 2011