Research on Password based key generation using enhanced AES

[1] Mehak Singla, [2]Lavina Maheshwari
[1]M.tech Research Scholar, [2]Assistant Professor
[1]Department of Computer Science & Engineering
[1]Global Research Institute Of Management & technology,Radaur,India

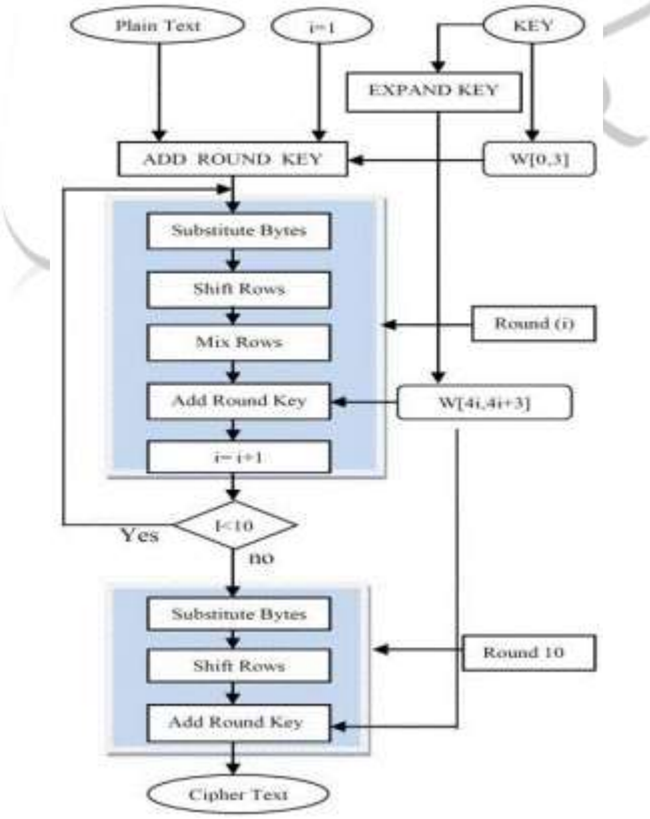
***Abstract* - AES(Advanced Encryption standard) is a symmetric-key block cipher, invented by two Belgian cryptographers Joan Daemen and Vincent Rijmen, published by the National Institute of Standards and Technology (NIST). It encrypts and decrypts a data block of the 128 bits. Security of data over the network is done by encryption/decryption process. But there are many security related issue has found in the Standard-AES.In this paper,we have tried our best to enhance the security of AES by introducing the three parameters i.e. Entropy,Floating Frequency, Autocorrelation.By using these three parameters,the Proposed-AES is considered more secure then the Standard-AES.**

Index Terms— **Entropy, Cryptography, Encryption, Decryption.**

I. Introduction

Science & Technology has ushered us with many inventions.No doubt,By these inventions life has become very easy,but on the other side it has given the birth of security related problem.To overcome this problem in network safety, the best answer is "Cryptography".It means maintaining the secrecy of confidential data to be transmitted by number of policies and algorithms.

1.1) AES (Advanced Encryption Standard): AES is a symmetric-key block cipher, invented by two Belgian cryptographers Joan Daemen and Vincent Rijmen, published by the National Institute of Standards and Technology (NIST). It encrypts and decrypts a data block of the 128 bits. It uses 10, 12 or 14 rounds. The key size which is 128,192 or 256 bits depends on the number of rounds.If each block length and key length are 128 bits, AES will perform nine processing rounds. If the block & key are 192 bits, AES will perform eleven processing rounds. If the block & key are 256 bits, then it performs thirteen processing rounds. Final step is very different in all the aspects that are 10th, 12th or 14th. Each processing rounds involves 4 steps:



(Figure 1.1: AES (Advanced Encryption Standard))

1. **Substitute bytes**: Uses a S-box to perform a byte by byte substitution of the block.

2. **Shift rows**: A simple permutation method.
3. **Mix column**: A substitution method where data in each of the column from the shift row is multiplied by algorithm's matrix data.
4. **Add round key**: The key for the processing round is XOR with the data.

The first three functions of an AES round are prepared to prevent cryptanalysis with the Methods of "confusion" and "diffusion." The fourth function is actually encrypts the data. AES formats plaintext into the 16 byte (128-bit) blocks, and treats each of the block as a 4x4 State array. It then performs the four operations in every round. The arrays contains the row & column information used in the various operations, especially MixColumns () & Shiftrows (). AES can be attacked by using the Timing analysis Attack. This only occurs when the malicious Alice runs the Sub-Bytes method on various data and observes the time it takes for every execution.

1.2) Entropy: The entropy is used to check the hardness of key.If the entropy is high,it means that your text file is more secure.If the value of entropy is less,it means that anyone can easily hack your personal information.Maximum possible entropy can be 4.70

1.3) Autocorrelation: Autocorrelation show the Number of characters that matches versus offset.It also mean that a text is compared to shifted copies of the similar text. The characters from both texts, that match each other in such a comparison, are determined.A frequency analysis is a complex calculation and thus it is advisable to use locally installed tools such as CrypTool for large texts.

1.4) Floating Frequency:Floating Frequency means number of different characters per 64 byte block versus section offset.It offers the best security when the graph is in zig-zag manner.

II. Related Study

Ashwak alabaichi et. at (2015) [6] enhanced the security system of their cryptography.In this Research paper, Author discusses the enhancement of the AES algorithm and also describes the whole process, which involves the generation of dynamic S-boxes for the Advanced Encryption Standard. The created S-boxes are more dynamic and key-dependent which built the differential and linear cryptanalysis more difficult. NIST uniqueness tests and correlation coefficient were conducted on the proposed dynamic AES algorithm, their outputs showing that it is superior to the original AES with security verified.

Yukti A et. al (2015) [31] implemented Network Security, nowadays, is the most important and challenging aspect in networking application. With the passage of time, increasing numbers of users generate and interchange a large amount of information in various fields. Networking security is the bundle of principles like prevention and monitoring of unauthorized data, any unwanted change in message, computer network denial and misuse of computer security. The network and data security is mandatory for data transmission to be secure which is the most challenging issue. Data security is done properly if all the following steps are fulfilled which are: communication channels should be secure, technique for encryption must be strong and the third party should be entrusted enough that he can maintain properly the database.

Ankit G et. al (2015) [5] implemented AES and stated that the Security on the Internet and on Local Area Networks is now at the forefront of computer network related problems. Network security consists of the provisions and policies adopted by a network administrator to monitor & prevent unauthorized access, modification, denial of a computer network, misarrange and network-accessible resources. Network security involves authorization of access to data in network, which is controlled by the help of network administrator. Each and every client who is working on the internet wants security of information but sometimes someone know that anyone else may be a intruder is collecting the information. The information is an asset that must be protected. Network security is the way by which digital information assets are protected, the goal of security is to protect confidentiality, to maintain integrity and to assure availability. To secure the entire network system and the information, one specific method is used which can be capable of providing the complete security solutions.

Dhaval Vegad et. al (2015) [9] focused on network security and said that in recent years network security has become an important issue. Encryption has come up as a better result and plays an important role in information security system. Many techniques are needed to protect the shared data. The recent work focus on cryptography to secure the data while transmitting in the network. Firstly the data which is to be transmitted from client to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. In this paper ,Author implemented a simple algorithm for both encryption and decryption.

Bahar Saini (2014) [7] had tried to give focus on the S-box rotation to get highly secured information .The standard AES comprises of four stages while in the new design, it consists of five stages The extra stage is known as S-box rotation.

III. Proposed Work

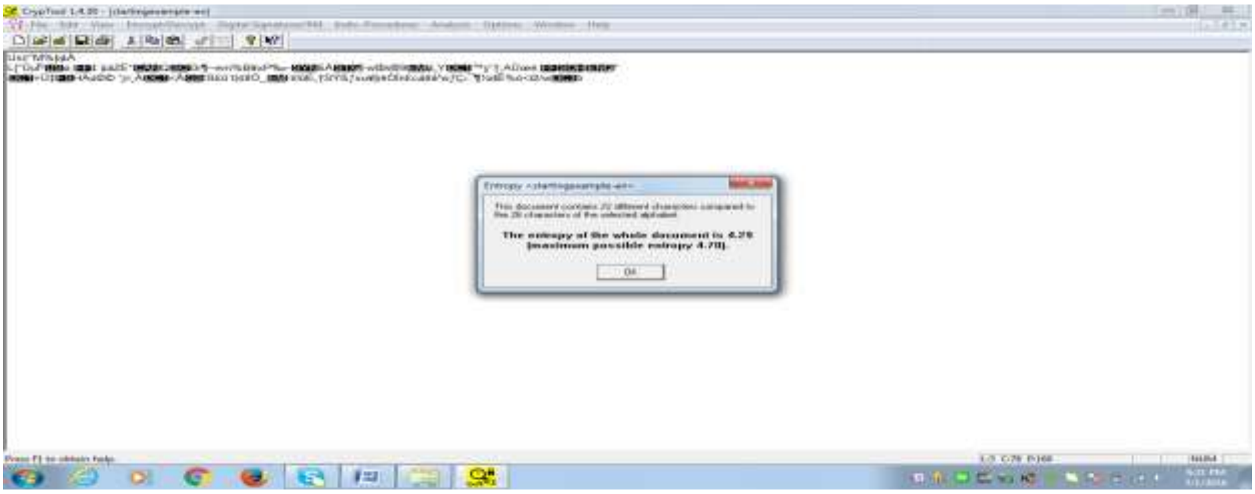
In our proposed work,we have used the three parameters which is entropy, floating frequency,Autocorrelation to enhance the security.The proposed work depends on a continuous parameters reconfiguration and a customization of each and every internal block. The customization depends on varying the four transformations (Shiftrows Transformation(SR) ,polynomial and affine transformations for S-Box (SB), MixColumn (MC) transformation). Internal AES blocks (SB, SR, and MC) are varied each round. Furthermore, these blocks are randomly interconnected during each session. The ciphered output will tested using cryptool

1.4.30. This method overcomes the problem of redundancy in the plain data and also strength against brute force attacks will increase. Ubuntu will be used to implement proposed AES.

IV. Results And Discussion

The result is implemented in ubuntu and it has been analyzed using CrypTool. The program is compiled using the default setting in ubuntu 10.04. In this result we have compared the proposed AES with original AES design.

Entropy of proposed AES shown below:(Entropy of the cipher text is to be calculated using crypTool) Which is better then the standard-AES



Entropy <startingexample-en>

This document contains 22 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 4.29 (maximum possible entropy 4.70).

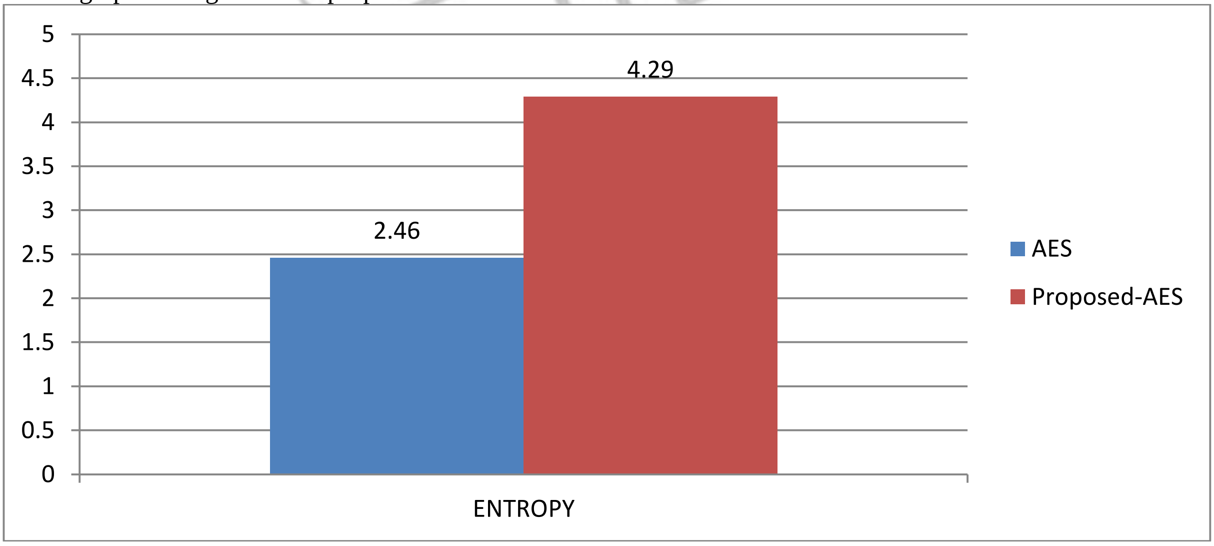
(Figure 4.1-Entropy of Proposed-AES)

Comparison Table between AES and Proposed-AES: Proposed AES is more secure then standard AES

(Table 4.1- Comparison between AES & Proposed-AES)

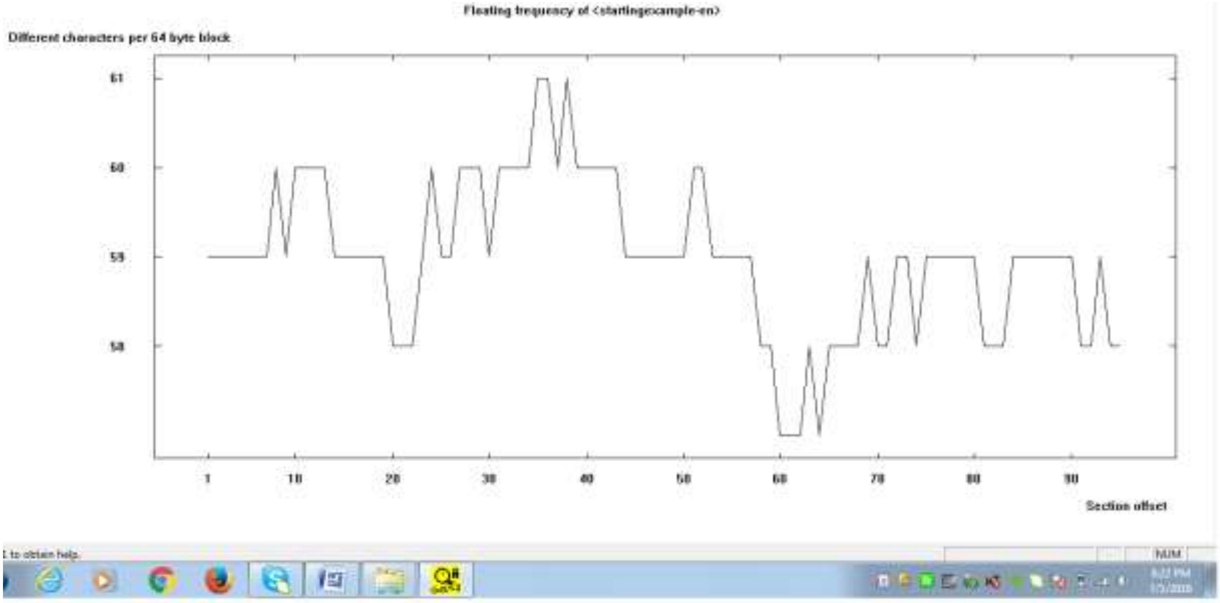
	ENTROPY
AES	**2.46**
Proposed-AES	**4.29**

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



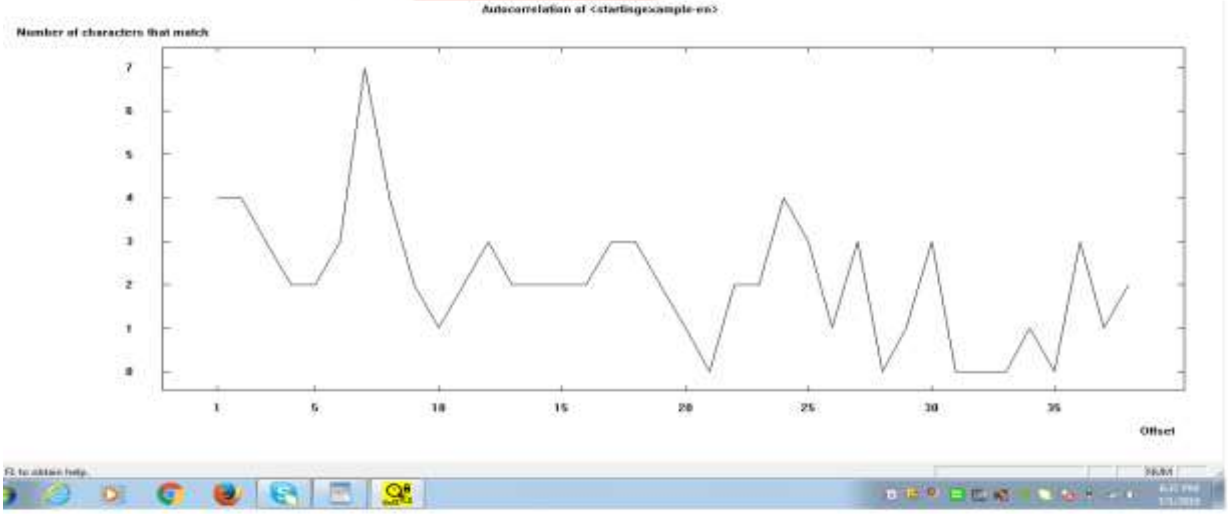
(Figure 4.2- Comparison graph AES & Proposed-AES)

Floating Frequency of proposed AES shown below: This graph show the different characters per 64 byte block versus section offset



(Figure 4.3- Floating Frequency)

Autocorrelation of proposed AES is shown below: This graph show the Number of characters that matches versus offset.



(Figure 4.4- Autocorrelation)

V. Conclusions

A new method for enhancing the security of AES algorithm is proposed. This approach design will not contradict the security of the standard AES algorithm by keeping all the mathematical criteria of AES remain unchanged. We try to make better 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. Here we have used the three parameters which is Floating-Frequency ,Autocorrelation and Entropy to evaluate the security.Also,Comparison between the entropy of proposed-AES and standard AES has shown above 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.

VI. References

[1] Ashwak alabaichi, Adnan Ibrahem Salih, “Enhance Security of Advance Encryption Standard Algorithm Based on Key-dependent SBox,” ISBN: 978-1-4673-6832-2©2015 IEEE

[2] Yukti,Aman Arora, “ Enhancement of AES”, International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Volume 5, Issue 7, July 2015.

[3] Ankit Garg, Kamal Kumar Sharma, Sharad Chauhan, “Performance Analysis of Password-Based AES Encryption and Decryption Using Cryptool,” International Journal for Advance

Research in Engineering and Technology, Volume 3, Issue X, Oct. 2015 ISSN 2320-6802.

[4] Dhaval Vegad, Husain Ullah Khan , Nimesh Ghosh," Character Based Encryption and Decryption using Modulo Arithmatic,",IJSTE - International Journal of Science Technology & Engineering | Volume 1 | Issue 10 | April 2015.

[5] Bahar Saini, "Implementation of AES Using S-Box Rotation", Volume 4, Issue 5, May 2014 ISSN: 2277 128X.