International Journal of Database Theory and Application
Vol.8, No.6 (2015), pp.13-24
http://dx.doi.org/10.14257/ijdta.2015.8.6.02

Enhance the Reliability and Security of AES

Ruchi Garg and Mandeep Kaur

M. Tech Research Scholar, Assistant Professor
Department of Computer Science & Engineering, Department of Computer Science & Engineering
Kurukshetra Institute of Tech. and Management, Kurukshetra Institute of Tech. and Management,
Kurukshetral, India, Kurukshetra, India
Ruchigarg91@gmail.com, Mandeepgohtra84@gmail.com

Abstract

Security is playing a very important role in the field of authentication system,network system and Internet. The main goal of cryptography is to secure the data so that it cannot be accessed by any unauthorized user. Cryptography is an emerging tool, which is important for authentication. The AES is a 128 bit Symmetric block Cipher. This paper include enhancing reliability and security, use modified AES (Advanced Encryption Technique) which will be implemented step by step. For the process of encryption various classical techniques are used. These are substitution technique, rearrangement and transformation technique. Key expansion module is introduced in the encryption and decryption modules, which generates key for all iterations. In each iterative rounds addition of an arithmetic operator and a route transposition cipher is introduced in this modification. To increase the immunity against unauthorized attacks, the Key extended module doubles the number of iterative processing rounds.

Keywords: *Cryptography, AES, IAES*

1. Introduction

Cryptography is basically the process of hiding information [3]. Cryptography is the science of using mathematics to encrypt and decrypt data. Data that can be read and understood without any special measures is called plaintext. The method of distinguishing plaintext in such a way as to hide its substance is called encryption. Encrypting plaintext results in unreadable form called cipher text [1]. The process of reversing cipher text to its original plain text is called decryption [7]. The system which provides encryption and decryption is called cryptosystem [2].

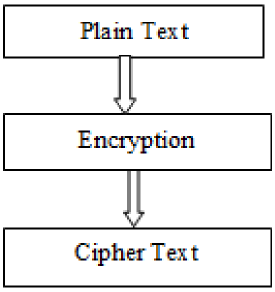


Figure 1. Process of Encryption

ISSN: 2005-4270 IJDTA

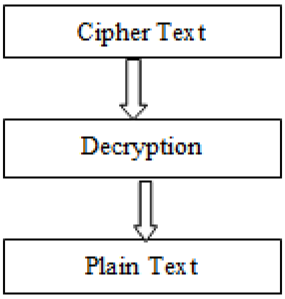


Figure 2. Process of Decryption

2. Cryptographic Goals

There are five main goals of cryptography. The principles of any security mechanism are confidentiality, authentication, integrity, Non repudiation, availability. These security mechanisms are usually referred to as the cryptographic goals [1]. These goals can be described as:

- *Confidentiality:* The principle of confidentiality specifies that only sender and receiver should be able to access the content of msg.
- *Authentication:* Authentication mechanism helps to establish proof of identities.
- *Integrity*: When content of message are not changed after the sender send it before it reach the receiver
- *Non Repudiation*: Non Repudiation mechanism to prove that the sender really sent this message.
- *Availability:* Availability state that resources should be available to authorized user.

3. Overview of Encryption Block and Stream Ciphers for Data Security

Every encryption and decryption has two aspects:- Algorithm and key. The Algorithm used for encryption and decryption is usually known to everybody. The Key used for encryption and decryption that make the process of cryptographic secure [1]. Two type of cryptographic algorithm used for encryption and decryption data:-

Symmetric key algorithm: In symmetric key or secret key only one key is used to encrypt and decrypt data [4]. For example: DES, AES, and RC2 *etc.*

Asymmetric key algorithm: In asymmetric key two keys are used *i.e.* Private and Public Keys. Public Key is used for encryption and Private Key is used for decryption [4]. For example: RSA and Digital Signature.

4. Advanced Encryption Standard (AES)

AES is based on a substitution-permutation network. AES has 128-bit block size and a key size of 128,192 or 256 bits [5]. AES operates on a 4×4 column-major order matrix of bytes. This is known as state. Mostly AES calculations are done in a special finite field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the plaintext into the cipher text. The numbers of cycles of repetition are as follows:

a. 10 cycles of repetition for 128 bit keys.
b. 12 cycles of repetition for 192 bit keys.
c. 14 cycles of repetition for 256 bit keys.

Each round of encryption process requires the following four types of operations: SubBytes, ShiftRows, MixColumns and XorRoundkey. Decryption is the reverse process of encryption and using *inverse* functions: Inv SubBytes, InvShiftRows and InvMixColumns [6].

The steps followed in AES are:

- Sub Bytes: This operation is a simple substitution method that converts every bit into a different value.
- Shift Rows: Each row is rotated to the right by a certain number of bytes.

Mix Columns: Each column is processed separately to produce a new column. The new column replaces the old one.

- AddRoundKey: This operation simply takes the existing state array.

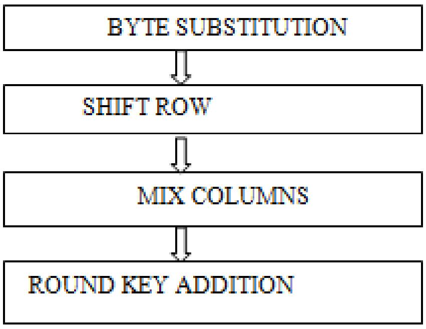


Figure 3. Steps of AES Algorithm

5. Methodlogy

CRYPTOOL is developed in 1998 by Prof. Bernhard Esslinger. The aim of CRYPTOOL is to explain the cryptographic Mechanisms. Then the study and analysis the performance of various ciphers is done using CRYPTOOL. Developing new Cipher ―IAES and Comparison of ―IAES with existing Cipher *i.e.* AES are done using Java. CrypTool is free software and an e-learning tool. It illustrating cryptographic concepts with graphical user interface.

Features:

1. Cryptographic methods can be applied and analyzed.
2. Comprehensive online help (understandable without a deep knowledge of cryptography).
3. It contains nearly all state-of-the-art cryptography functions.
4. Easy entry into modern and classical cryptography and last but not the least it‗s not a ‗hacker tool.

6. Challenges & Objectives

1. Study of various Stream and block ciphers.
2. Analysis of various Ciphers.
3. Performance evaluation of Ciphers.
4. Developing new Cipher –"IAES".
5. Comparison of "IAES" with existing Ciphers.

7. Problem Formulation & Analysis

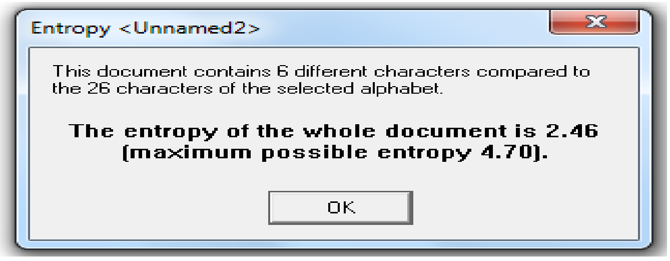
The objective of our work to study various Stream and block ciphers. Then we will do analysis of various Ciphers. Then based on the parameters we will evaluate performance of Ciphers. We will then develop a new cipher “IAES”. And will perform Comparison of “IAES” with existing Cipher AES. And this comparison is done on Cryptool. The simulation based information content test such as Entropy, Floating Frequency, Histogram, N-gram, Autocorrelation and Periodicity on ciphers is done. The simulation based Randomness test such as Frequency test, Pokers test, Serial test, Long run test on ciphers are done using CrypTool.

Information Content Test –It test information on the basis of some representations. It includes: Entropy, Floating Frequency, Histogram, N-Gram, Autocorrelation and Periodicity.

Table 1.1. Information Theory Test Mechanisms

Entropy	Calculate the entropy of a document.
Floating frequency	Calculate the floating frequency of a document.
Histogram	Calculate the character frequency of a document.
N-Gram	Analyze the frequency of N-Grams of a document.
Auto-correlation	Perform autocorrelation of characters in a document.
Periodicity	Analyze the periodicity of a document.

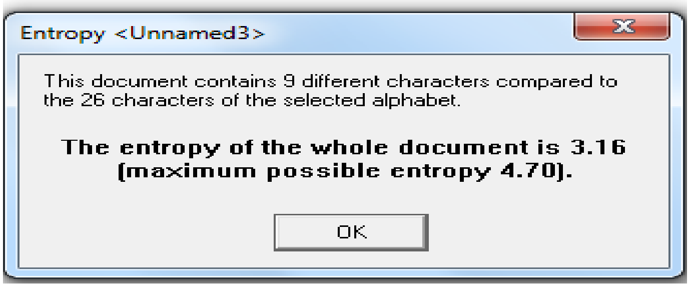
Entropy: The entropy of a document is an index of its information content. The entropy is measured in bits per character. The entropy that indicates its characteristic distribution. It measures the average amount of information which one can obtain through observation of the source or, conversely, the indeterminacy which prevails over the generated messages when one cannot observe the source. For documents which contain only upper case letters, the entropy lies between 0 bit/char and log(26) bit/char = 4.700440 bit/char *i.e.* in a document which consists of only one character and in a document in which all 26 characters occur equally often.


Entropy <Unnamed2>

This document contains 6 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 2.46 (maximum possible entropy 4.70).

Figure 4. Evaluation of Entropy of AES Cipher Text Using CrypTool



This document contains 9 different characters compared to the 26 characters of the selected alphabet.

The entropy of the whole document is 3.16 (maximum possible entropy 4.70).

Figure 5. Evaluation of Entropy of IAES Cipher Text Using CrypTool

Floating Frequency: It may be defined as a characteristic of its local information content at individual points in the document is called as the floating frequency of a document. The floating frequency defines how many different characters are to be found in any given 64-character long segment of the document

Histogram: The histogram of a document is expressed as the frequency distribution of the characters of this document in graphical form. The x-axis of the histogram contains all the characters in the character set. In a text window the character set contains the letters of the alphabet selected in Text Options, while in a window for hexadecimal inputs and outputs, the character set contains the numbers 0 to 255 The frequency of each character is shown (as a percentage) on the vertical axis. The data can also be displayed as a curve by deselecting Bar Chart in the View menu.

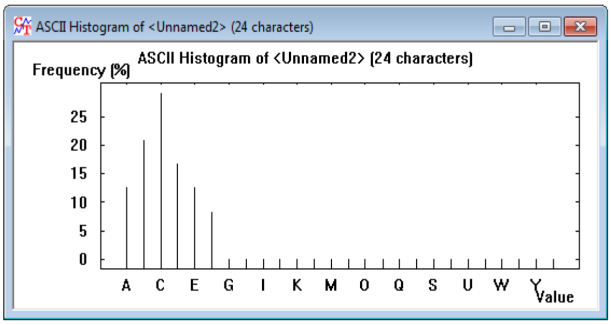


Figure 6. Evaluation of Histogram of AES Cipher Text Using CrypTool

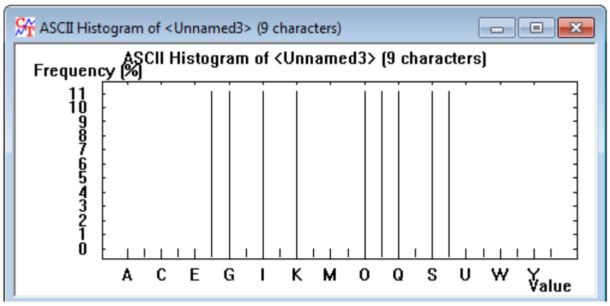
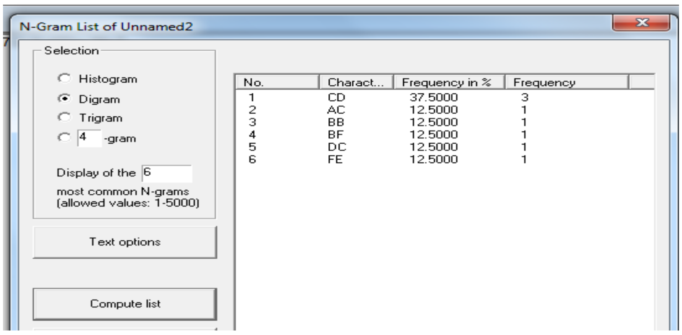


Figure 7. Evaluation of Histogram of IAES Cipher Text Using CrypTool

N-Gram: An n-gram is a string of n distinct characters. 2-grams and 3-grams are called bi- or diagrams and trigrams resp. 1-gram lists are called histograms. The n-gram list of a document contains all n-grams of the document together with their frequency, usually ordered descendingly by frequency. CrypTool limits n-gram lists to the 5000 most frequent n-grams. If we analyze a text document then only characters from the current alphabet are considered. Characters that do not belong to the current alphabet will "separate" the text. For example: if the space character does not belong to the current alphabet, then the text "ATTACK AT DAWN" have the trigrams ATT, TTA, TAC, ACK, DAW and AWN.



N-Gram List of Unnamed2

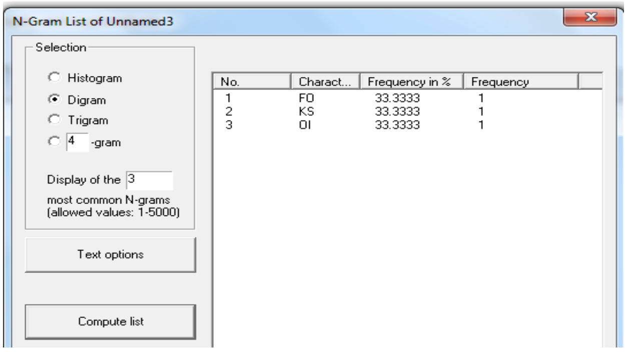
Selection

○ Histogram
● Digram
○ Trigram
○ 4 -gram

Display of the 6 most common N-grams (allowed values: 1-5000)

No.	Charact...	Frequency in %	Frequency
1	CD	37.5000	3
2	AC	12.5000	1
3	BB	12.5000	1
4	BF	12.5000	1
5	DC	12.5000	1
6	FE	12.5000	1

Figure 8. Evaluation of n-Gram of AES Cipher Text Using CrypTool



N-Gram List of Unnamed3

Selection

○ Histogram
● Digram
○ Trigram
○ 4 -gram

Display of the 3 most common N-grams (allowed values: 1-5000)

No.	Charact...	Frequency in %	Frequency
1	FO	33.3333	1
2	KS	33.3333	1
3	OI	33.3333	1

Figure 9. Evaluation of n-Gram of IAES Cipher Text Using CrypTool

Autocorrelation: The autocorrelation of a document is an index of the similarity of different sections of the document. It is sometimes possible to work out the key length of an encrypted document from its autocorrelation. The similarity between two sets of data is normally measured by their correlation. Correlation is valid here for a independently, uniformly distributed, binary random sequence:

"Binary random sequence" means that the event of the random sequence takes the values '0' or '1'. "Independent" means that the probability of the (n+1) st event is independent from all n previous events.

"Uniformly distributed" means for each event in the random sequence that the probability of '1' is equal to the probability of '0'.

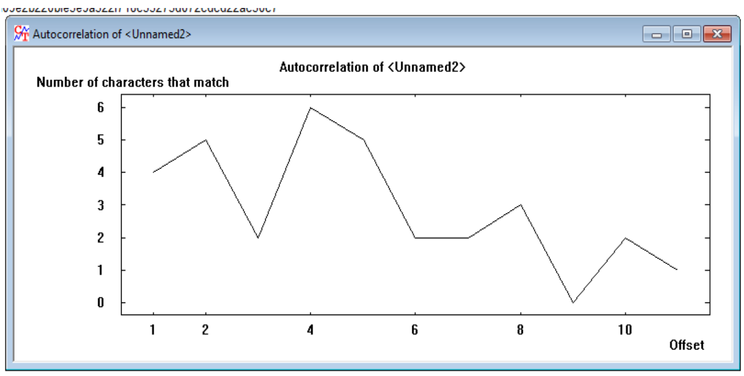


Figure 10. Evaluation of Auto Correlation of AES Cipher Text Using CrypTool

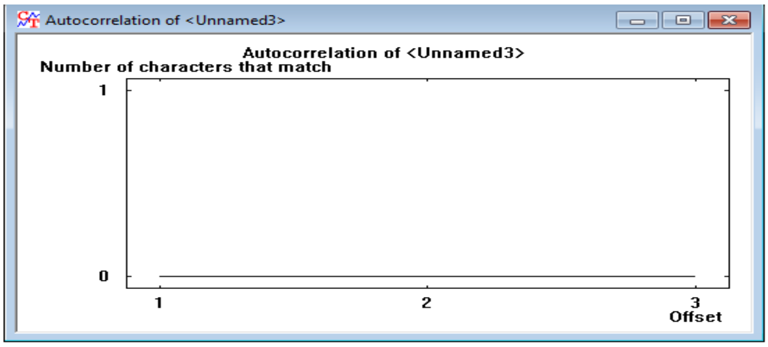

Autocorrelation of <Unnamed3>
Autocorrelation of <Unnamed3>
Number of characters that match
1
0
1
2
3
Offset

Figure 11. Evaluation of Auto Correlation of IAES Cipher Text Using CrypTool

Periodicity: Periodicity is the repetition of a certain sequence of characters of length k (k >= 1) from a certain position in the document – the offset. The periodicity must continue through to the end of the document. Therefore it is not enough that a patterns appears multiple times in a file to be a period. All periodic cycles are shown. It is only possible to have several cycles when they are nested within each other. The first byte of the document has the offset value 1.The periodicity analysis can be applied to text and binary documents.

Randomness Test --It checks the random quality of active document. It includes: Frequency test, Pokers test, Run test, Long Run test, and Serial test.

Table 1. 2 Random Test Mechanisms

Frequency test	Checks the random quality of the active document with the Frequency test.
Poker test	Checks the random quality of the active document with the Poker test.
Run test	Checks the random quality of the active document with the Run and Long-Run test.
Serial Test	Checks the random quality of the active document with the Serial Test.

Parameters to be considered:

Significant level (α): is the test of Hypothesis H0 gives the probability of incorrectly rejecting Hypothesis H0 although it is correct. Generally the value of "α" taken as

α=0.01 with Max. Test length= 6.635
α=0.05 with Max. Test length= 3.841
α=0.10 with Max. Test length=2.705

And value of max. Test length varies with particular test to be considered. Above is for frequency test.

Default offset & Test length: decides whether default values are test/user defined values. Generally, offset=0 & test length= file length.

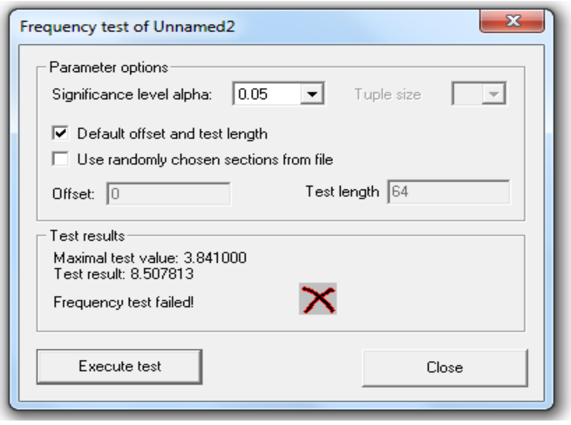
Use randomly chosen test block: user can use its own default value & test length of file.

Max. Test value: is the statistical value that is dependent on α.

Test outcome: is a statistical value generated by test which is compared with max. Test value.

Tuple: is an ordered ensemble of K elements

Frequency test:



Frequency test of Unnamed2

Parameter options

Significance level alpha: 0.05

Tuple size

☑ Default offset and test length

□ Use randomly chosen sections from file

Offset: 0

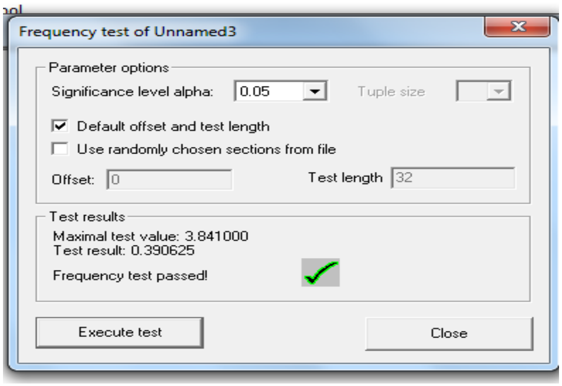
Test length 64

Test results

Maximal test value: 3.841000
Test result: 8.507813

Frequency test failed! ☒

Figure 12. Evaluation of Frequency Test of AES Cipher Text Using CrypTool



Frequency test of Unnamed3

Parameter options

Significance level alpha: 0.05

Tuple size

☑ Default offset and test length

□ Use randomly chosen sections from file

Offset: 0

Test length 32

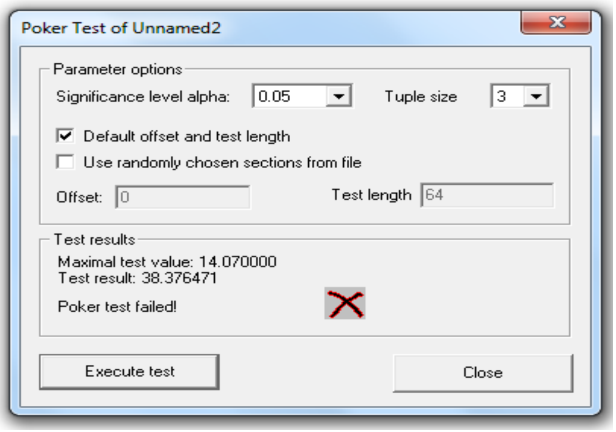
Test results

Maximal test value: 3.841000
Test result: 0.390625

Frequency test passed! ✓

Figure 13. Evaluation of Frequency Test of IAES Cipher Text Using CrypTool

Poker test:



Poker Test of Unnamed2

Parameter options

Significance level alpha: 0.05

Tuple size 3

☑ Default offset and test length

□ Use randomly chosen sections from file

Offset: 0

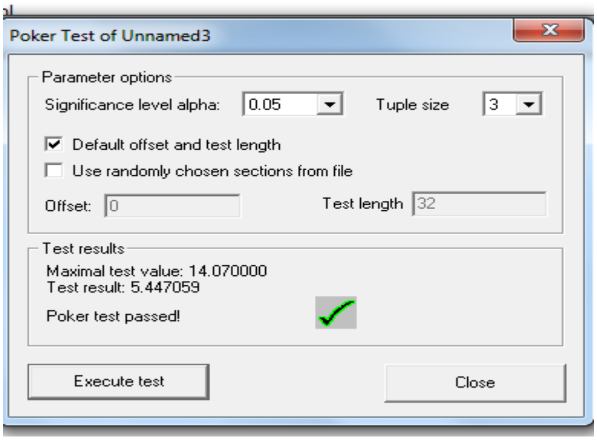
Test length 64

Test results

Maximal test value: 14.070000
Test result: 38.376471

Poker test failed! ☒

Figure 14. Evaluation of Poker Test of AES Cipher Text Using CrypTool



Significance level alpha: 0.05 Tuple size 3

☑ Default offset and test length

☐ Use randomly chosen sections from file

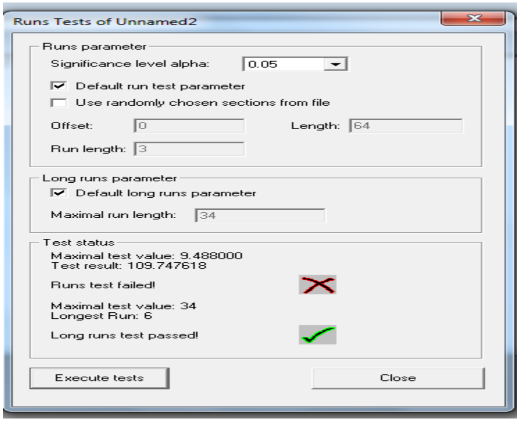
Offset: 0 Test length 32

Maximal test value: 14.070000
Test result: 5.447059

Poker test passed! ✓

Figure 15. Evaluation of Poker Test of IAES Cipher Text Using CrypTool

Run test:



Significance level alpha: 0.05

☑ Default run test parameter

☐ Use randomly chosen sections from file

Offset: 0 Length: 64

Run length: 3

☑ Default long runs parameter

Maximal run length: 34

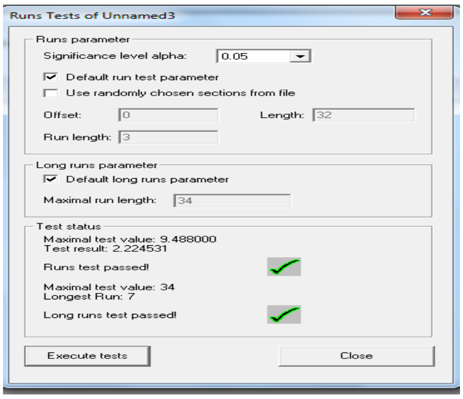
Maximal test value: 9.488000
Test result: 109.747618

Runs test failed! ✗

Maximal test value: 34
Longest Run: 6

Long runs test passed! ✓

Figure 16. Evaluation of Runs Tests of AES Cipher Text Using Cryptool



Significance level alpha: 0.05

☑ Default run test parameter

☐ Use randomly chosen sections from file

Offset: 0 Length: 32

Run length: 3

☑ Default long runs parameter

Maximal run length: 34

Maximal test value: 9.488000
Test result: 2.224531

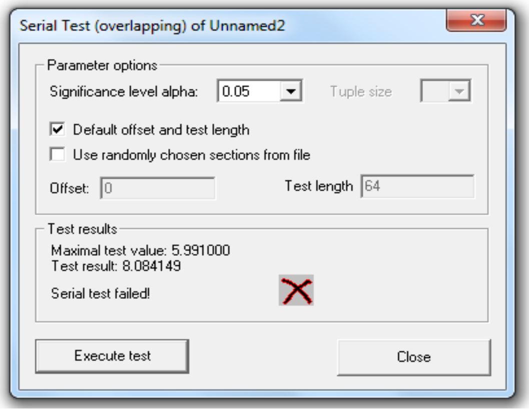
Runs test passed! ✓

Maximal test value: 34
Longest Run: 7

Long runs test passed! ✓

Figure 17. Evaluation of Runs Tests of IAES Cipher Text Using CrypTool

Serial test:



Serial Test (overlapping) of Unnamed2

Parameter options

Significance level alpha: 0.05 Tuple size

☑ Default offset and test length

□ Use randomly chosen sections from file

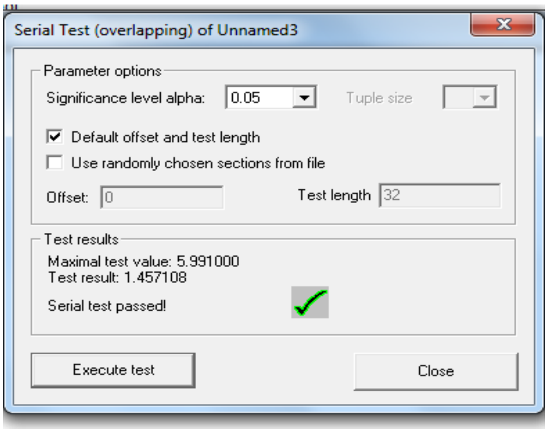
Offset: 0 Test length 64

Test results

Maximal test value: 5.991000
Test result: 8.084149

Serial test failed! ✗

Figure 18. Evaluation of Serial Test of AES Cipher Text Using CrypTool



Serial Test (overlapping) of Unnamed3

Parameter options

Significance level alpha: 0.05 Tuple size

☑ Default offset and test length

□ Use randomly chosen sections from file

Offset: 0 Test length 32

Test results

Maximal test value: 5.991000
Test result: 1.457108

Serial test passed! ✓

Figure 19. Evaluation of Serial Test of IAES Cipher Text Using CrypTool

8. Conclusion

In this paper we have compared cryptographic algorithms AES and IAES by using the tool CRYPTOOL 1.4.31 .The comparison is done by using the parameters Binary Histogram, Autocorrelation and Floating Frequency. Based upon these parameters it is concluded that IAES is better than AES. The IAES Encryption Technique was implemented successfully using 'JAVA' language. Various data were encrypted using different keys. The original data was properly received by a decryption of the cipher text. The modifications brought about in the code was tested and proved to be accurately encrypting and decrypting the data messages with even higher security and immunity against the unauthorized users. If the security and efficiency is of primary concern then one can use our proposed IAES algorithm. From the above discussion we can clearly see that the proposed algorithm has 70% better entropy of encrypted text any of the other compeering algorithms and hence can be incorporated in the process of encryption of any type of text. And it was found that the IAES cryptographic Technique is stronger than AES. Based on Randomness analysis test, IAES is much better than AES.

9. Future Scope

Our future work the algorithm should handle various kinds of data like images, videos, PDF *etc. i.e.* in future we can encrypt images, videos, PDF etc with the help of our IAES algorithm and can decrypt it also and can check the performance of it using CrypTool. For future work, we plan to expand our algorithm set to include different block ciphers, signature algorithms and hash functions. We will also expand our results to include results for prime fields, using bases other than polynomial bases and different coordinate systems such as projective coordinates.

References

[1] A. Khate, "Cryptography and Network Security", Tata MC Graw.

[2] D. Sukhija, "Performance Evaluation of Cryptographic Algorithms: AES and DES", (International Journal of computer science and mobile Computing), September **(2014)**.

[3] K. Kaur, "Performance Evaluation of Ciphers Using Cryptool", (international journal of Computer and science), August **(2012)**.

[4] S. J. Vashishtha, "http://www.ijcem.org/papers072012/ijcem_072012_09.pdf", July **(2012)**.

[5] W. Stallings, "Cryptography and Network security", Pearson prentice hall, 4th edition, **(2006)**.

[6] S. Pavithra and Mrs E. Ramadevi, "Performance Evaluation of Symmetric Algorithms", (Journals of Global Research in Computer Science), August **(2012)**.

[7] "http://ijctonline.com/ojs/index.php/ijct/article/view/426.pdf".

[8] W. Stallings, "Cryptography and Network Security 4th Ed", Prentice Hall, **(2005)**.

[9] K. S. Sandha, "Performance Evaluation of symmetric cryptography algorithms", September **(2011)**.

[10] M. Marwaha, "Comparative analysis of cryptographic algorithms", (International Journal of Advanced Engineering Technology) E-ISSN 0976-3945, **(2013)**.

Author

Ruchi Garg, M. tech. (CSE).