ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

An Enhanced Hybrid Cryptographic Algorithm for Security of Text

Bhavik A. Rana[1] , Sunil B. Wankhade[2]

P. G. Student, Dept. of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India[1]

Dept. of Information Technology, Rajiv Gandhi Institute of Technology, Mumbai, India[2]

ABSTRACT: The confidential information that desires to be transmitted over the internet is not at ease as that data may be available via manner of any-one. Protecting this non-public data over the internet is a tough task and the records security problems emerge as increasingly more critical. For stopping this non-public data visualize to anyone, we use the idea of cryptography. Cryptography is used for securing this private data. Cryptography is an artwork of hiding the data. There are many cryptographic algorithms used for imparting safety to information, but additionally same has some drawbacks.

In this paper, we present an idea to develop a hybrid cryptographic algorithm**.** The hybrid algorithm uses a combination of three well-known symmetric algorithms AES, DES and IDEA**.** The approach behind developing hybrid cryptographic algorithm is to provide higher security to the data**.** For this approach, AES algorithm is limited to 128-bit key i**.**e**.**, AES-128 is used in this algorithm**.**

KEYWORDS: AES, DES, ECB, IDEA, Hybrid, Cryptography, PKCS7 Padding, Key Manipulation, Security Enhancement**.**

I. INTRODUCTION

Transmission of information over the internet is very risky these days as there are many attackers available on the internet. The non-public information that needs to be surpassed on network will not be thriller if attacker can see this data and hence it's far available for all people who are present on network. This way data dispatched on internet isn't in any respect cozy. This manner information doesn't stay one of a kind and is available to all. This method the principle protection dreams aren't completed [11]. For accomplishing the ones goals, we secure the message using the term cryptography. Cryptography is a technique hidden writing of the information. Cryptography is used to benefit all of the protection goals because the plaintext isn't available to everyone till he/she is privy to the critical component i.e., key. This approach data is exclusive and handiest to be had for folks that understand the crucial thing [2].

There are many cryptographic algorithms available over the net to protect the message. Algorithms can be Symmetric-key (Secret key) algorithm or Asymmetric-key Algorithm. Symmetric-key algorithm makes use of single key for encryption and decryption of the information [9]. Symmetric-key cryptography is likewise called Private-key cryptography as the important thing (key) used for encryption and decryption is stored personal [3]. Asymmetric-key algorithm used two one-of-a-kind keys i.e. Non-public key and public key for encrypting and decrypting information. Asymmetric-key cryptography is likewise called as Public-key cryptography as the important thing (key) used for encrypting the information is kept public while the key used for decrypting information is personal [4].

Advance Encryption Standard (AES) algorithm is the most popular and commonly used in recent times. AES is a Symmetric-block cipher, which means that it makes use of Similar key for encryption and decryption reason. The input block consists for AES is 128-bit and the important thing (key) for AES may be 128-bit, 192-bit or 256-bit [12]. The variety of rounds for AES depends on the key size as an instance, for 128-bit key length the quantity of rounds is 10, for 192-bit key length the range of rounds are 12 and for 256-bit key length the variety of rounds are 14 [7]. Each round of AES includes 4 changes which encompass Substitute Bytes, Shift Rows, Mix Column and ADD Round Key. All the 4 transformations are finished in each round except for the last round due to the fact in final round Mix Column transformation isn't carried out.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

Data Encryption Standard (DES) is the most common algorithm known. DES is a symmetric block cipher that is based on Fiestal network structure which divides the entered input in halves. DES uses the identical key for encryption and decryption reason. DES takes input of 64-bit [8]. The key length for DES is 64-bit out of which 8 bits are used for parity checking, which means the important thing (key) size turns into 56-bit. There are general 16 rounds for DES algorithm. The working of 16 rounds is done on the basis of equation (1) and (2).

$L_i = R_{i-1}$ (1)

$R_i = L_{i-1} \oplus F\ (R_{i-1}, K_i)$ (2)

Where L_i indicates left part of round i and R_i indicates right part of round i.

International Data Encryption Algorithm (IDEA) is the advance version of DES algorithm. IDEA is not popular and common like DES and AES because it was patented and must be licensed before it can be used. IDEA is a symmetric block cipher 0. It takes input of 64-bit block. IDEA is stronger than DES. The key length for IDEA block is 128-bit. There are total of eight rounds in IDEA and 1 output transformation round.
There also are some of the hybrid algorithms that integrated Symmetric-key Algorithms like DES and IDEA, DES and AES or combination of one Symmetric-key Algorithm and one Asymmetric-key Algorithm like simple Symmetric-key algorithm and Rivest-Shamir-Adleman (RSA) algorithm. These hybrid algorithms may be used for encryption and decryption of string, a file or an image [5]. Some hybrid algorithms had been used for safety of digital motion image, at the same time as a few had been used for data protection [6].

II. PROPOSED SYSTEM ARCHITECTURE

The proposed algorithm is created using the combination of three symmetric-key cryptography algorithms i.e., mixture of AES, DES and IDEA. The algorithm designed here is used for offering higher security to the data. The algorithm also uses the key manipulation technique for all the individual algorithm. Key manipulation means the key that is given by user is not directly passed to algorithm engine instead of that the key first go with some changes and then passed to the algorithm. The proposed algorithm uses the concept of Onion cryptography in which ciphertext generated from one algorithm is passed as plaintext for another algorithm.

A. Overall Structure

The process of encrypting the text for hybrid cryptography algorithm is shown in Fig. 1. The steps for same are as follows:

Step 1: User inputs the plaintext which is divided into 64-bit blocks.

Step 2: The key for every algorithm is taken and are manipulated as per rules and then passed to algorithm engine as needed.

Step 3: This 64-bit block is passed to DES engine to generate 192-bit ciphertext as DES works with ECB mode and also use PKCS7 padding.

Step 4: The ciphertext that is generated by DES engine is given as input to IDEA engine. Again, the ciphertext is divided into 64-bit blocks for providing input of 64-bit block to IDEA that generates the output of 352-bit ciphertext as IDEA also works with ECB mode and also uses PKCS7 padding.

Step 5: The ciphertext that is generated by IDEA engine is given as input to AES engine. Again, the ciphertext is divided into 128-bit blocks for providing input of 128-bit block to AES that generates the output of 512-bit ciphertext as AES also works with ECB mode and also uses PKCS7 padding.

The hybrid algorithm described here uses three keys. Key 1 is of 64-bit which is given to DES, key 2 is of 128-bit which is given to IDEA and key 3 is of 128-bit which is given AES.

The Decryption process for the hybrid algorithm is the reverse of the Encryption process. The steps for same are as follows:

Step 1: 512-bit ciphertext is taken as input and passed to AES block which gives the output of 352-bit deciphertext.

Step2: The deciphertext generated by AES engine is passed to IDEA block which generates the deciphered 192-bit deciphertext.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

Step 3: The deciphertext generated by IDEA engine is passed to DES block which generates the 64-bit plaintext.
Step 4: Finally, the 64-bit plaintext is shown to user.

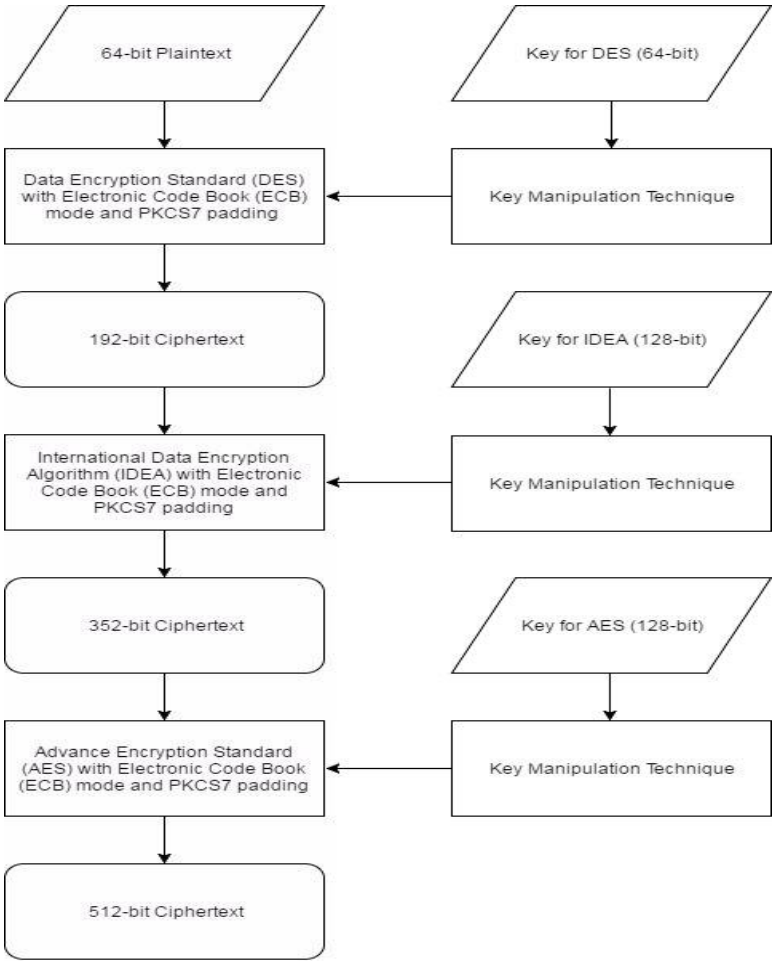

Figure 1: Encryption process of hybrid cryptography algorithm.

B. Rounds

The proposed system model is a combination of three algorithms which includes AES, DES and IDEA. The total number of rounds for DES algorithm are 16, total number of rounds for IDEA algorithm are 8.5 and total number of rounds for AES algorithm, can vary from 10, 12 or 14 depending on the key size of 128-bit, 192-bit or 256-bit. But for our algorithm the AES is restricted to only 128-bit key or AES-128 is used which means rounds for AES algorithm four proposed system model are 10 [10]. As the proposed system is the linear combination of all the three algorithms, the total number of rounds are the addition of rounds of all the algorithms present. Therefore, the total number of rounds for hybrid algorithm is 16 + 8.5 + 10 = 34.5.

C. Electronic CodeBook (ECB)

The proposed algorithm here uses the ECB mode with every algorithm present here. Which means the block of ciphertext generated from every algorithm is again encrypted using this mode. In the proposed algorithm, this mode works 3 time for the same plaintext as the input block has to go through three different algorithms and every algorithm works with ECB mode. Input block is first passed to DES engine after which the ciphertext block is encrypted with ECB mode, the output of this ECB mode is passed to IDEA

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

algorithm and again this ciphertext is encrypted with ECB mode, the output of same is given as input to AES and again the ciphertext is encrypted with ECB mode. This way ECB mode works thrice for the same input.

D. Public Key Cryptography Standards 7 (PKCS7) Padding

The PKCS7 padding is used for the padding the block as per the size. The PKCS7 padding is the standard padding used for padding the blocks as per cryptographic standards. This padding works for the block size in between from 1 byte to 255 bytes.

The PKCS7 padding works similar like ECB mode in the proposed algorithm. This means PKCS7 padding also works thrice for the proposed algorithm. PKCS7 padding also works for every algorithm just like ECB mode.

E. Key Manipulation

There are three keys required for the proposed hybrid algorithm. The keys that are taken from the users for all the three algorithms are not directly passed to the respective engines. The keys are first modified with some specific set of rules and then passed to the respective engines.

This means the keys taken from the user are not directly passed to respective engines. The keys are first manipulated and then passed to respective engines. The sender and receiver need to just pass the same keys as per decided and modifications are done by the system as per given rules.

III. EXPERIMENTAL RESULTS

The experimental results for the hybrid algorithm are divided into two parts which are discussed here. Frist part consists of the main interface, which is shown in Fig. 2. In which the user has the option for deciding on the algorithm from AES, DES, IDEA or Hybrid. The ciphertext generated by encryption process of the hybrid algorithm is shown in Fig. 2.

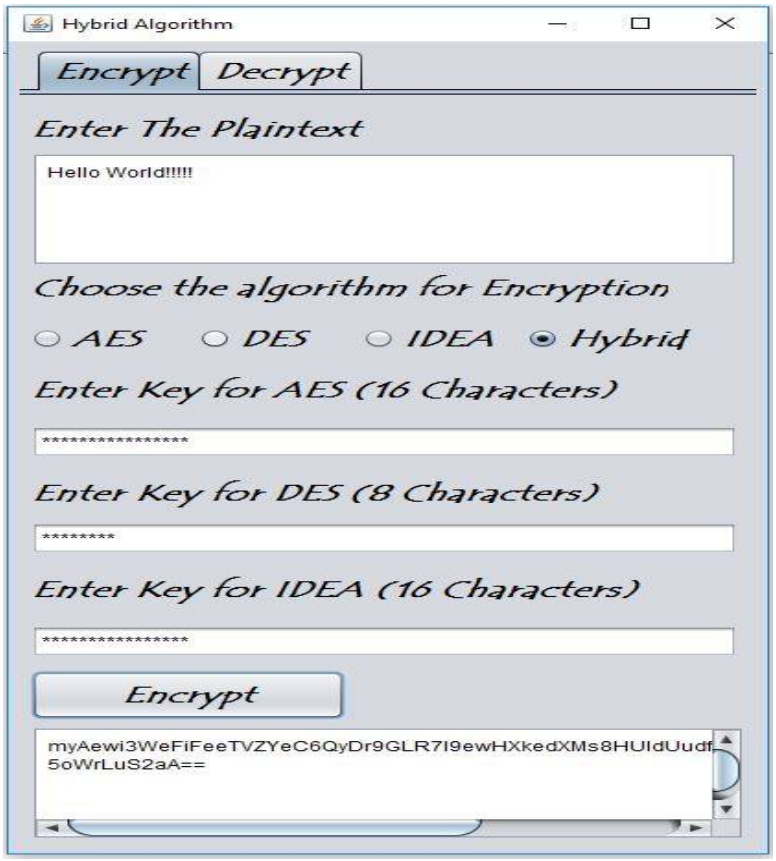

Figure 2: Output of encryption process of hybrid algorithm.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

The second part of experimental results consists of the comparison of different parameters considered for the cryptanalysis. There are total our parameters that are considered here and compared one parameter of each individual algorithm with hybrid algorithm. The plaintext given to all the different algorithms is "Hello World!!!!!" to generate ciphertext. The parameters considered here are described below:

A. Entropy

The entropy is used to outline the randomness of the calculated ciphertext. The higher the entropy value, the more randomness is blanketed. The loss of entropy could have the poor impact on performance and protection. The comparison of entropy value of IDEA algorithm and Hybrid algorithm is shown in Fig. 3.

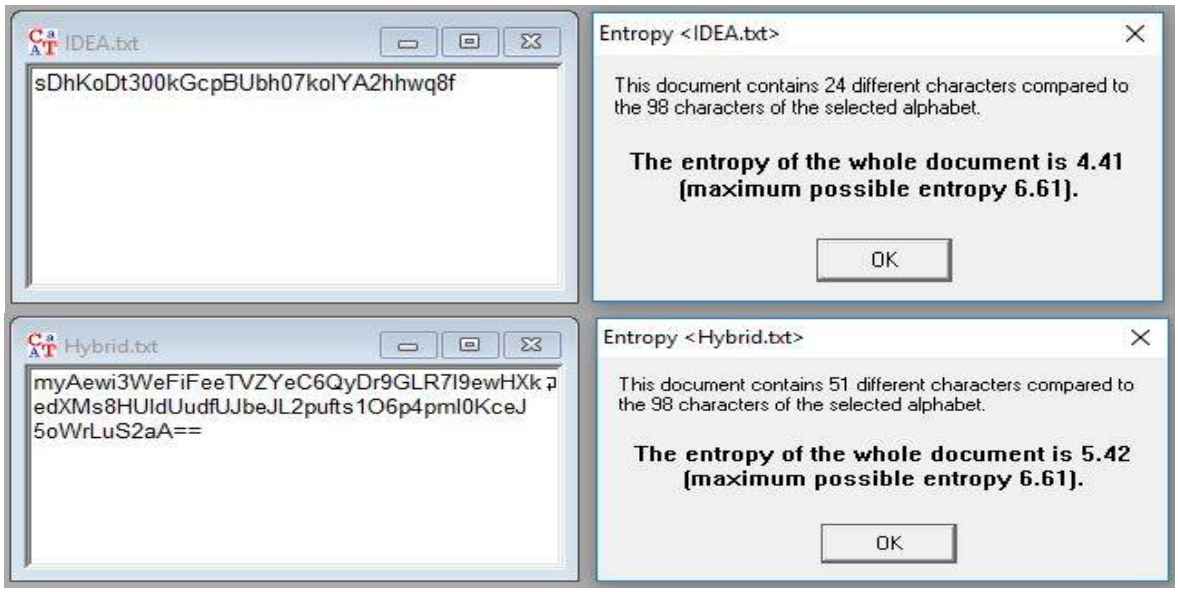

Figure 3: Comparison of Entropy value.

As consistent with the consequences, the hybrid algorithm described right here gives the highest entropy value for the ciphertext.

B. Histogram

The histogram is the graph for the individual's character within the ciphertext and the frequency of an individual which means that how normally the character appeared in the generated ciphertext. On the X-axis of histogram all the alphabets including upper and lower case, special characters, space, etc. are included. The Y-axis shows the frequency in percentage of the character is present in the ciphertext. The comparison of histogram graph of DES algorithm and Hybrid algorithm is shown in Fig. 4.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

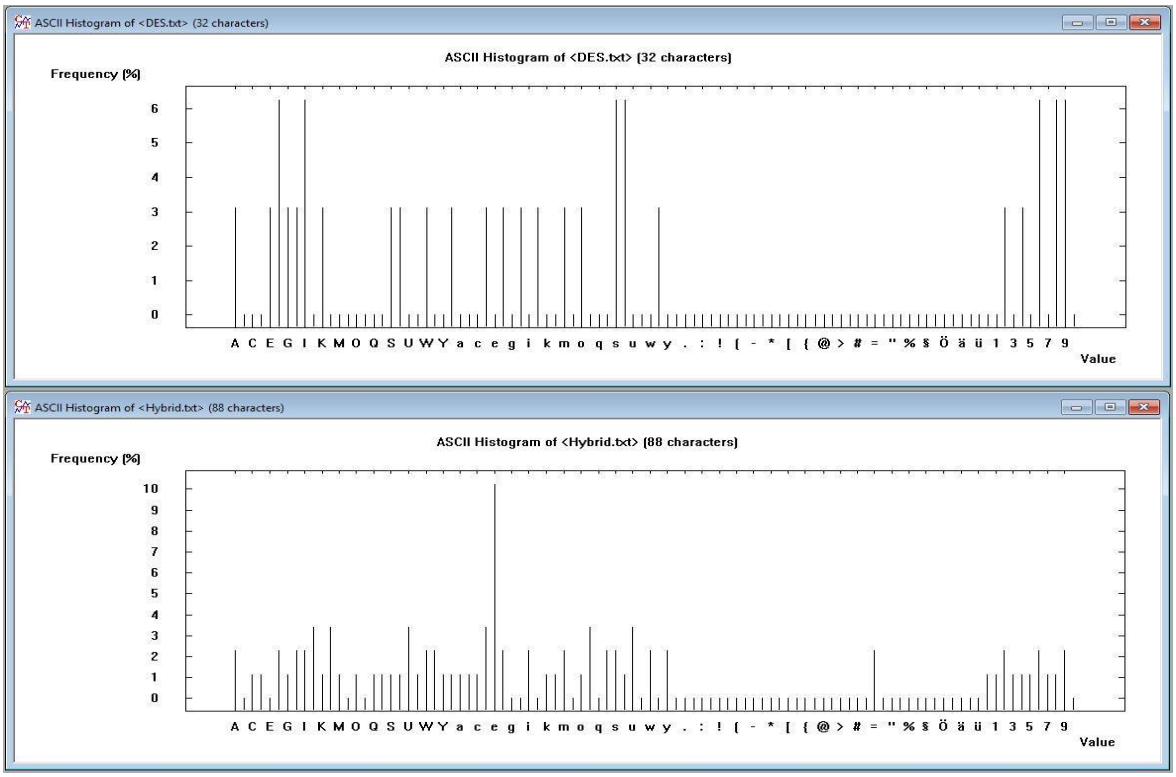

Figure 4: Comparison of Histogram Graph.

C. Autocorrelation

The autocorrelation is an index of the similarity of different sections. It is sometimes possible to work out the key length of an encrypted document from its autocorrelation. The autocorrelation function $c(t)$ measures the similarity of sequence (s[i]) = s[1]s[2]… to sequence (s[i+t])=s[t]s[t+1]… which is shifted by t places. A sequence of length n is examined, and the following parameters are defined:

A(t):= number of members of sequences (s[i]) and (s[i+t]) in the segment under consideration which agree.

D(t):= number of members of sequences (s[i]) and (s[i+t]) in the segment under consideration which do not agree.

The autocorrelation function $C(t) = (A(t)-D(t)) / n$.

On the X-axis, the offset value is given and on the Y-axis number of characters that match is given. The comparison of autocorrelation graph of AES algorithm and Hybrid algorithm is shown in Fig. 5.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

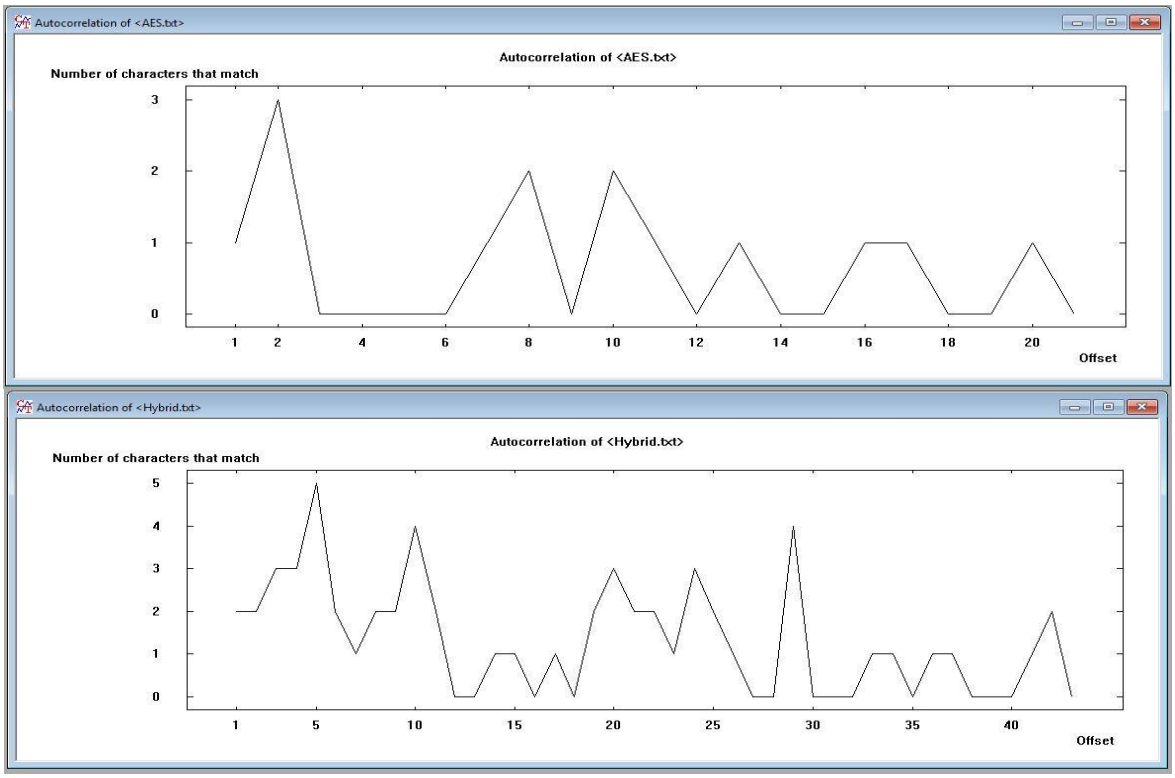

Figure 5: Comparison of Autocorrelation Graph.

D. Floating Frequency

The floating frequency is a characteristic of its local information content at individual points. The floating frequency specifies how many different characters are to be found in any given 64-character long segment of the document. The function considers sequences of text in the active window that are 64 characters long and counts how many different characters are to be found in this "window". The "window" is then shifted one character to the right and the calculation is repeated. This procedure results in a summary in which it is possible to identify the places with high and low information density. A document of length n > 64 bytes has n-63 such index numbers in its characteristics. The diagrammatic representation of floating frequency for hybrid algorithm is given in Fig. 6.

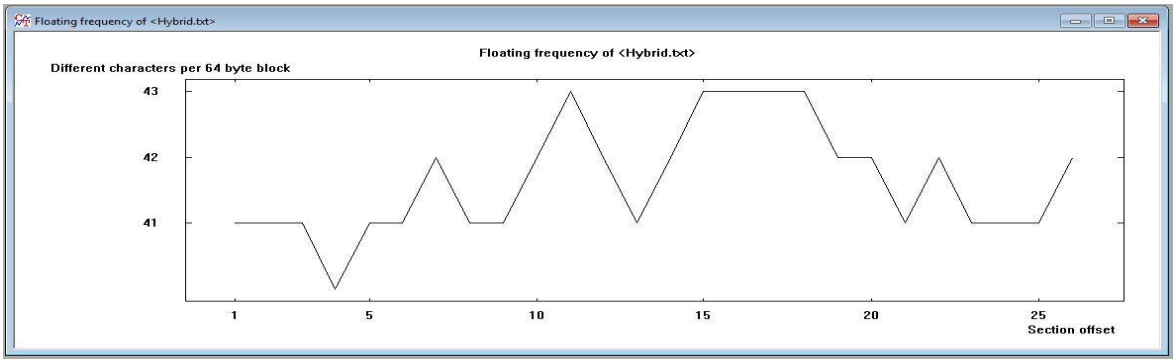

Figure 6: Floating Frequency graph.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 6, Issue 10, October 2017

IV. CONCLUSION

The paper suggests the combination of AES, DES and IDEA algorithm to generate the hybrid cryptography algorithm. The motive of creating this hybrid algorithm is to provide higher safety to the string. The time that is needed for to attack the hybrid algorithm is the entire time of attacking all the three algorithms as we use three keys for the encryption and decryption cause.

The hybrid algorithm uses the key manipulation technique for all the algorithm, which means the key given by the user is not directly passed to algorithm engine but the key is first modified and then passed to the different algorithm engines.

The results section describes the detailed results of how the hybrid algorithm works. Also, the comparison of results between hybrid algorithm with different algorithm are also shown in the results section.

As the hybrid algorithms combines 3 different cryptographic algorithms, the security of the information is stepped forward. The proposed algorithm uses three different keys of various length for encryption and decryption process which maximize the time for the Brute-Force attack.

REFERENCES

[1] Mr. Mahavir Jain,Mr. Arpit Agrawal, "Implementation of Hybrid Cryptography Algorithm", in *International Journal of Core Engineering & Management(IJCEM) Volume 1, Issue 3, June 2014.*

[2] Jignesh R Patel, Rajesh S. Bansode, Vikas Kaul, "Hybrid Security Algorithms for Data Transmission using AES-DES", in *International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.2, February 2012.*

[3] P.G. Gopika, N. Hariharan and S. Perumal Sankar, "Hybrid AES Algorithm Using 16 Fiestel Based Network with Distinct Keys", in *Middle-East Journal of Scientific Research 24 (4): 1325-1329, 2016, ISSN 1990-9233 © IDOSI Publications, 2016. DOI: 10.5829/idosi.mejsr.2016.24.04.23301.*

[4] Bhavik Rana, Sunil Wankhade, "Enhancing the Security of Text Using Hybrid Cryptographic Algorithm", in *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE), Vol. 5, Issue 4, pp 8151-8157, April 2017(ISSN(Online): 2320-9801 ISSN (Print): 2320-9798).*

[5] M.B. Vishnu, S.K. Tiong, Member IEEE, M. Zaini, Member IEEE, S.P. Koh, "Security Enhancement of Digital Motion Image Transmission Using Hybrid AES-DES Algorithm", in *Proceedings of APCC2008 copyright © 2008 IEICE 08 SB 0083.*

[6] Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni, "Enhancing Data Security by using Hybrid Cryptographic Algorithm", in *International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013.*

[7] Anurhea Dutta, Prerna Bharti, Swati Agrawal, Surekha K S, "Hybrid AES-DES Block Cipher: Implementation using Xilinx ISE 9.1i", in *UACEE International Journal of Advancements in Electronics and Electrical Engineering Volume 1: Issue 2 [ISSN: 2319 – 7498].*

[8] Wang Tianfu, K. Ramesh Babu, "Design of a Hybrid Cryptographic Algorithm", in *International Journal of Computer Science & Communication Networks, Vol 2(2), 277-283 277 ISSN:2249-5789.*

[9] Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis", in *International Journal of Computer Applications, Volume 61– No.20, January 2013(0975 – 8887).*

[10] Md Asif Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Information Security", in *International Journal of Computer Sciences and Engineering (IJCSE), Volume 2, Issue 4 (*2347-2693*).*

[11] A. P Shaikh, V. Kaul, "Enhanced Security Algorithm using Hybrid Encryption and ECC", in *IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 3, Ver. IV, PP 80-85(May-Jun. 2014) (e-ISSN: 2278-0661, p- ISSN: 2278-8727).*

[12] Sridhar C. Iyer, R.R. Sedamkar, Shiwani Gupta, "A Novel Idea on Multimedia Encryption using Hybrid Crypto Approach" in *7th International Conference on Communication, Computing and Virtualization 2016, Available online at www.sciencedirect.com*