ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Enhancing the Security of Text Using Hybrid Cryptographic Algorithm

Bhavik Rana, Sunil Wankhade

P. G. Student, Dept. of Computer Engineering, RGIT, Mumbai University, Mumbai, India

Faculty, Dept. of Information Technology, RGIT, Mumbai University, Mumbai, India

ABSTRACT: The confidential data that desires to be transmitted over the net isn't always secure as that facts can be available by way of any-one. Protecting this personal data over the internet is a difficult venture and the data security troubles grow to be more and more important. For preventing this personal information, we use the idea of cryptography. Cryptography is used for securing this confidential data. Cryptography is an artwork of hiding the information. There are many cryptographic algorithms used for presenting safety to data, but also equal has some drawbacks.

In this paper, we present an approach to develop a hybrid cryptographic algorithm. The hybrid model uses a combination of 3 symmetric algorithms AES, DES and IDEA. The idea behind developing hybrid cryptographic algorithm is to offer higher security to the data. For our motive, AES algorithm is limited to 128-bit key i.e., AES-128 is used on this approach.

KEYWORDS: AES, DES, ECB, IDEA, Hybrid, Cryptography, Security Enhancement.

I. INTRODUCTION

Transmission of data over the internet is very risky in recent times as there are many attackers present on the internet**.** The personal data that needs to be passed on network will no longer be mystery if attacker can see this data and hence it's far available for all people who are present on network**.** This way records sent on net isn't always in any respect comfy**.** This means data doesn't stay exclusive and is to be had to all**.** This method the main safety desires are not carried out**.** For attaining those goals, we at ease the message using the term cryptography**.** Cryptography method hidden writing of the statistics**.** Cryptography is used to gain all of the security desires because the plaintext isn't to be had to everybody till he/she is aware of the important thing i**.**e**.**, key**.** This approach records are confidential and most effective to be had for folks that understand the important thing**.**

There are many cryptographic algorithms present over the internet to secure the message. Algorithms can be Symmetric-key (Secret key) algorithm or Asymmetric-key Algorithm. Symmetric-key algorithm uses single key for encryption and decryption of the data. Symmetric-key cryptography is also called Private-key cryptography as the key used for encryption and decryption is kept private. Asymmetric-key algorithm used two different keys i.e. private key and public key for encrypting and decrypting data. Asymmetric-key cryptography is also called as Public-key cryptography as the key used for encrypting the data is kept public while the key used for decrypting data is private0.

There are also some of the hybrid algorithms that combine two 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 can be used for encryption and decryption of string, a normal file or an image file. Some hybrid algorithms were used for security of digital motion image [2], while some were used for data security [3].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

II. RELATED WORKS

Cryptographic algorithms are used to provide the safety to the message. But the usage of the single cryptographic algorithm has its own drawback. Combining this cryptographic algorithm offers more safety. We now talk how exclusive researchers used this combination to provide the safety over internet. M.B. Vishnu et. al. [2] counseled the combination of the 2 symmetric-key cryptographic algorithms i.e. combining DES and AES for securing digital motion image. They presented the layout and implementation of symmetrical hybrid primarily based 128-bit key AES-DES algorithm. The idea of a hybrid based AES-DES can be construed on the subject of primary DES Feistel equations. The repetition of these equations is primarily based on the wide variety of rounds as adapted through the Feistel network, which inside the case of DES was standardized at sixteen. Jigar Chauhan et. al. [3] suggested the same aggregate of algorithms for imparting statistics security. They presented the layout and implementation of symmetrical hybrid based totally 128-bit key AES-DES algorithm for security enhancement. The idea of a hybrid primarily based AES-DES may be construed with reference to fundamental DES Feistel equations. The repetition of those equations is based totally on the variety of rounds as adapted through the Feistel network, which within the case of DES became standardized at 16. P.G. Gopika et. al. [4] counseled the hybrid AES algorithm which employ AES with Feistel network and distinct keys. They proposed 16 rounds for AES-128. Their algorithm used AES key generation method for general AES 128 and a predefined key for Feistel network. The basic idea of the hybrid AES the usage of Feistel primarily based network with distinct secrets to combine AES into every iteration of the Feistel network of DES. Anurhea Dutta et. al. [5] cautioned a system the combines AES-DES that's carried out in in VHDL the usage of Xilinx ISE 9.1i platform and centered on a XILINX XC3S400 based FPGA technology. They used the AES-128 for a block of 256-bit plaintext. The primary idea of the proposed hybrid model is to combine AES in every generation of the fiestal network of DES. Wang Tianfu, and K. Ramesh Babu [6] has used the combination of AES-DES algorithm but in different way. The alternate bit of plaintext is passed to alternate AES and DES block. Jignesh R Patel et. al. [7] extensively utilized the mixture of AES-DES algorithms however barely in unique way. They took 128-bit plaintext, divided plaintext into halves 64-Bit each, then passed each the 64-bit plaintext to 2 unique DES block and upon getting the two ciphertext block, they combined it to get128-bit block which changed into then surpassed to AES. Mr. Mahavir Jain and Mr. Arpit Agrawal [8] counseled something different than the above algorithms. They blended DES-IDEA to create hybrid algorithm. It is a layout for switch records with better security.

III. METHODOLOGIES

A. Advance Encryption Standard (AES)

AES is a Symmetric-block cipher, which means that it uses same key for encryption and decryption reason. The input block length for AES is 128-bit and the key for AES may be 128-bit, 192-bit or 256-bit. The range of rounds for AES depends on the key size as an example, for 128-bit key length the quantity of rounds is 10, for 192-bit key size the range of rounds are 12 and for 256-bit key size the range of rounds are 14 [10]. The working of universal structure for AES is explained underneath.

Each round of AES consists of 4 adjustments which encompass Substitute Bytes, Shift Rows, Mix Column and ADD Round Key. All the 4 transformation are done in each round except for the last round because in last round Mix Column transformation isn't carried out.

Substitute Bytes is the procedure wherein the bytes are changed through different bytes that are represented through authentic bytes from the S-box table. The S-container isn't the random value but there's a described method for creating the S-box. For this round, each byte is mapped with the brand-new byte wherein the left part of byte represents the row in the S-box table and the right part of the byte represents the column within the S-box table. For example, the byte {25} selects 2^{nd} row and 5^{th} column of the S-box table which will contain the value {3F}.

In Shift Rows transformation, every row is shifted via a few bits. This method every row does left-round shift as consistent with determined by means of the AES. It is just an easy permutation and it really works because the 1^{st} row isn't always altered, the 2^{nd} row is shifted via 1 byte to the left in round way, 3^{rd} row is shifted with the aid of 2 bytes to the left in circular way and the 4^{th} row is shifted by 3 bytes to the left in round manner.

In Mix Column Transformation, the output after Shift Rows Transformation is increased with the predefine matrix of AES. This degree is largely a substitution. Every detail of the product matrix is the sum of products of factors of one row and one column. The Mix Column transformation of a single column j ($0 \leq j \leq 3$) for the output is given in eq. (1), (2), (3) and (4).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

$$s`_{0,j} = (2 \bullet s_{0,j}) \oplus (3 \bullet s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \quad \text{eq. (1)}$$
$$s`_{1,j} = s_{0,j} \oplus (2 \bullet s_{1,j}) \oplus (3 \bullet s_{2,j}) \oplus s_{3,j} \quad \text{eq. (2)}$$
$$s`_{2,j} = s_{0,j} \oplus s'_{1,j} \oplus (2 \bullet s_{2,j}) \oplus (3 \bullet s_{3,j}) \quad \text{eq. (3)}$$
$$s`_{3,j} = (3 \bullet s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \bullet s_{3,j}) \quad \text{eq. (4)}$$

Where • indicates multiplication over the finite field GF (2^8).

In the very last transformation, the Round Key is XORed with the output of Mix Column transformation and so it is referred to as Add Round Key Transformation. The operation is column wise operation for 4 bytes of output of Mix Column transformation and 1 row of the round key. This transformation is saved simple but it impacts each byte of the output of Mix Column transformation.

B. *Data Encryption Standard (DES)*

DES is a symmetric block cipher which is based on Fiestal network structure which divides the input in two halves. DES uses the same key for encryption and decryption purpose. DES takes input of 64-bit. The key size for DES is 64-bit out of which 8 bits are used for parity checking, which means the key size becomes 56-bit. There are total 16 rounds for Des algorithm [11]. The overall working of DES is explained further.

The working of 16 rounds is done on the basis of eq. (5) and (6).

$$L_i = R_{i-1} \quad \text{eq. (5)}$$
$$R_i = L_{i-1} \oplus \boldsymbol{F}(R_{i-1}, K_i) \quad \text{eq. (6)}$$

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

The internal working of the single round of DES is primarily based on fiestal network in which first the input of 64-bit plaintext is split into two halves of 32-bit plaintext. Similarly, the key of 56-bit is divided into halves of 28-bit. For the value of subsequent round left element is given the fee of right component and the important thing operation is performed on proper part which incorporates first the expansion table which converts 32-bit records to 48-bit information. Also, both halves of key do the left round shift after which both are given to permuted choice box 2 which converts 56-bit key to 48-bit. After that the right part of plaintext is XORed with the important thing. This output is given to S-box which converts this 48-bit information to 32-bit records. Then, this output is given to the permutation container. Finally, the cost for right half of is generated by way of XORing output of permutation field with left half facts. This is executed for 16 rounds.

C. *International Data Encryption Algorithm (IDEA)*

IDEA is a symmetric block cipher. IDEA is the advance version of DES algorithm. It takes input of 64-bit block. IDEA is stronger than DES. The key size for IDEA block is 128-bit. There are total of 8 rounds in IDEA and 1 output transformation round [12]. The working of IDEA is explained next.

IDEA uses 6 keys for each round uses 4 keys for output transformation round. The working of round is in multiple steps which include multiplications, addition and XOR operations. The input 64-bit block is divided into 4 16-bit blocks and 128-bit key is divided into 8 16-bit blocks. The 8 keys get exhausted in 2nd round, so for generating further keys left circular shift of 25 bits is done. Hence, IDEA uses total of 48 keys for 8 rounds and additional 4 keys for output transformation round i.e., total of 48+4=52 keys are generated for IDEA. Each round has a total of 14 steps and the output transformation round has 4 steps [9].

IV. PROPOSED SYSTEM

The proposed algorithm is a combination of three symmetric-key cryptography algorithms i.e., mixture of AES, DES and IDEA to create hybrid cryptography algorithm. The algorithm design right here is used for offering higher protection to the data.

A. *Overall Structure*

The Encryption process for hybrid cryptography algorithm is shown in Fig. 1. The steps for encryption process of hybrid cryptography algorithm are as follows:

Step 1: 64-bit plaintext is taken from user input.

Step 2: This 64-bit plaintext is passed to DES block to generate 192-bit ciphertext as DES works with ECB mode and also use PKCS7 padding.

Step 3: The output that is generated by DES is given as input for IDEA engine. Again, the output is divided into 64-bit blocks for providing input of 64-bit block that generates the output of 352-bit ciphertext as IDEA also works with ECB mode and also uses PKCS7 padding.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Step 4: Finally, the output from Step 3 is given to AES block which generates 512-bit ciphertext as AES also works with ECB mode and also uses PKCS7 padding.

The hybrid algorithm 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 Decryption process for the hybrid algorithm is shown in Fig 2. The steps for encryption process of hybrid cryptography algorithm are as follows:

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

Step 2: The output of Step 1 is passed to IDEA block which generates the deciphered 192-bit deciphertext.

Step 3: The output of Step 2 is passed to DES block which generates the 64-bit plaintext.

Step 4: Finally, the 64-bit plaintext is shown to user.

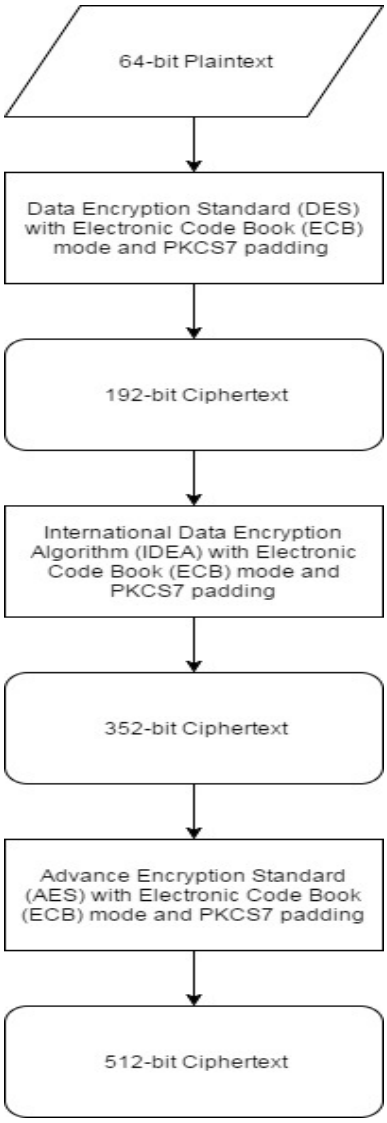

Figure 1: Encryption process of hybrid cryptography algorithm.

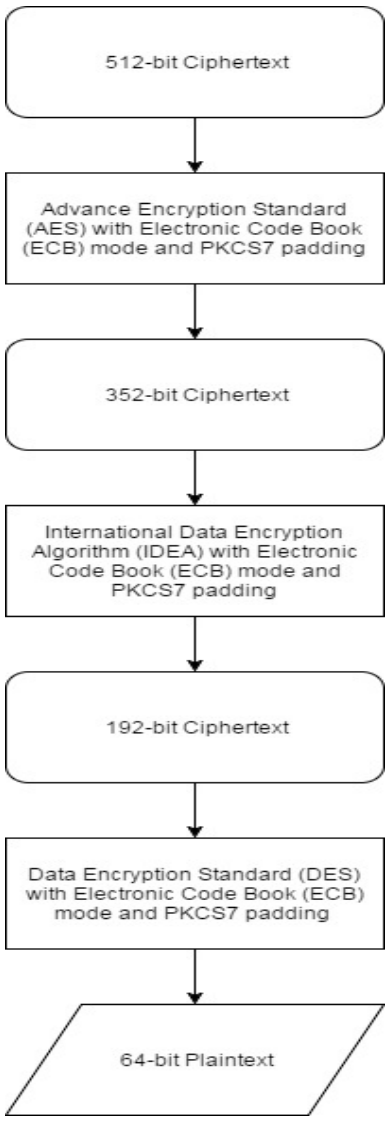

Figure 2: Decryption process of hybrid cryptography algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

V. EXPERIMENTAL RESULTS

The experimental results for the hybrid algorithm are discussed in this. Starting from the main interface, this is shown in Fig. 3. In which the user has the option for choosing the algorithm from AES, DES, IDEA or Hybrid.

The output of encryption process of the hybrid algorithm is shown in Fig. 3. And the output of the decryption process is shown in Fig. 4.

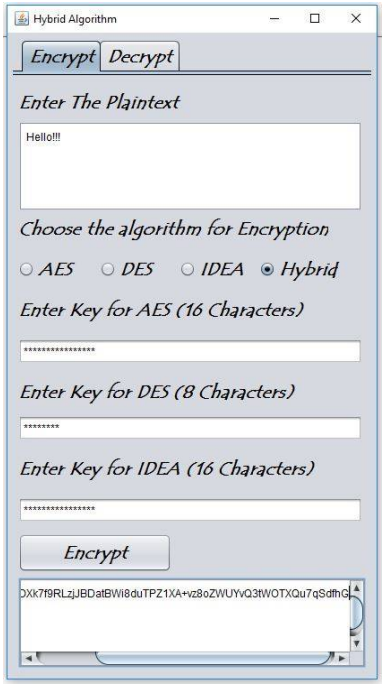

Figure 3: Output of encryption process of hybrid algorithm.

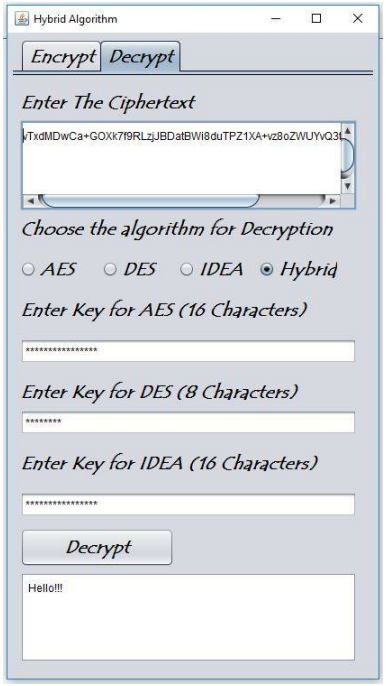

Figure 4: Output of decryption process of hybrid algorithm.

The results and analysis on the output (ciphertext) generated by the hybrid algorithm is shown in Fig. 5(a), Fig. 5(b), Fig. 5(c). Fig. 5(a) shows the Entropy value of Hybrid algorithm, Fig. 5(b)shows the Histogram graph of Hybrid algorithm, Fig. 5(c)shows the Auto-correlation graph of Hybrid algorithm. The plaintext given to all the different algorithms is "Hello!!!" to generate ciphertext.

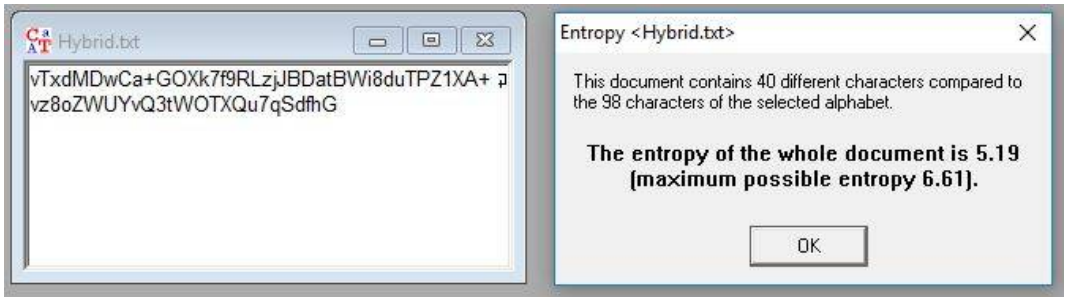

Figure 5(a): Entropy value of Hybrid algorithm.

The entropy is used to define the randomness of the calculated ciphertext. The higher the entropy value, the more randomness is included. The lack of entropy can have the negative impact on performance and security. As per the results, the hybrid algorithm described here offers the highest entropy value for the plaintext.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

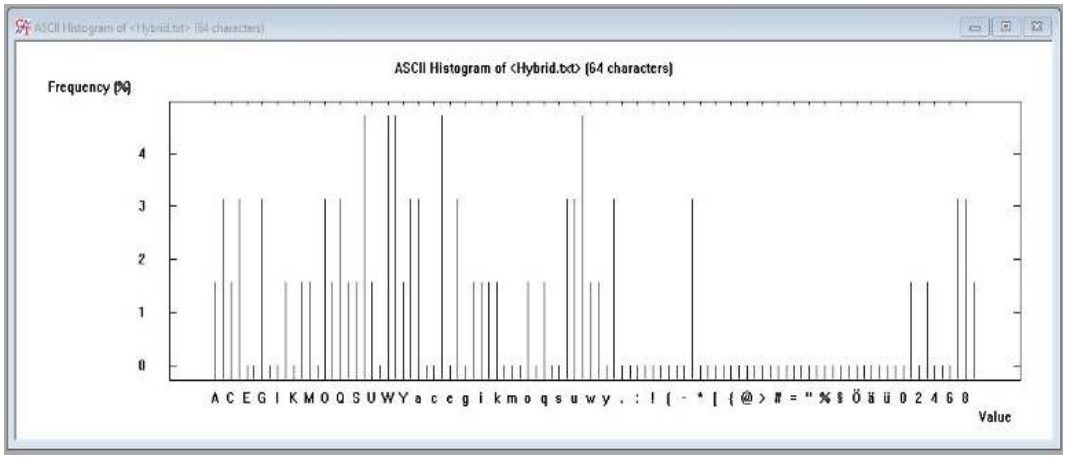

Figure 5(b): Histogram graph of Hybrid algorithm.

The histogram is the graph for the character's present in the ciphertext and the frequency of a character which means how many times 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 ciphertext generated using hybrid algorithm gives the total value of 64characters for plaintext.

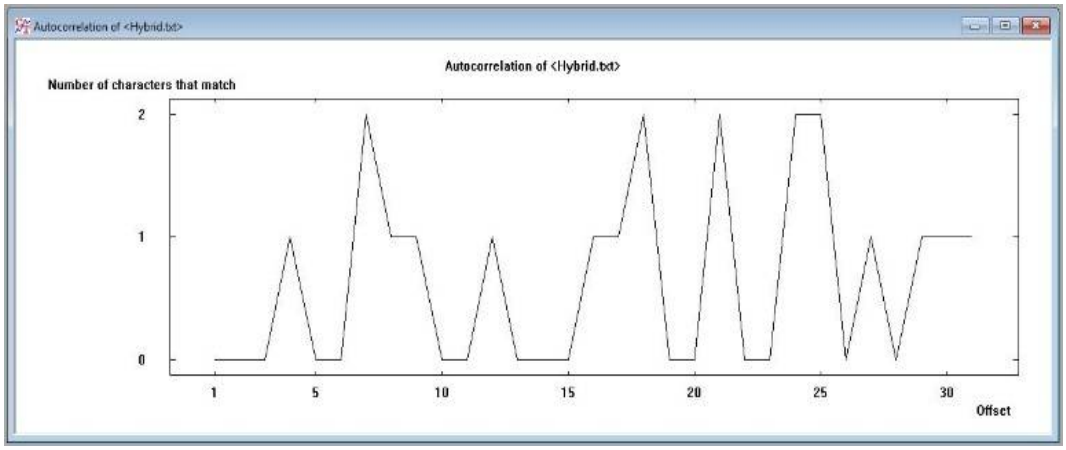

Figure 5(c): Auto-correlation graph of Hybrid algorithm

The autocorrelation is an index of the similarity of different sections. The similarity between two sets of data is normally measured by their correlation. Correlation C between two sequences of length n is calculated from the number A of agreeing and the number D of non-agreeing sequence members according to eq. (7).

$$C: = (A-D) / n \qquad \text{eq. (7)}$$

On the X-axis, the offset value is given and on the Y-axis number of characters that match is given. The ciphertext generated using hybrid algorithm gives the total value of 64 characters for plaintext.

The comparison of different parameter used for result analysis for all the algorithms are shown in Table 1. The table shows the different values of entropy, input characters, output characters. The input taken here was "Hello!!!" which contains 8 characters.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

TABLE I. COMPARISION OF DIFFERENT PARAMETERS OF RESULT ANALYSIS FOR DIFFERENT ALGORITHMS

Algorithms / Parameters	AES	DES	IDEA	HYBRID
Input Characters	8	8	8	8
Output Characters	24	24	24	64
Entropy (out of 6.61)	4.25 (20/98 different characters)	4.05 (18/98 different characters)	4.50 (23/98 different characters)	5.19 (40/98 different characters)

VI. CONCLUSION

The paper indicates the mixture of AES, DES and IDEA algorithm to acquire the hybrid cryptography algorithm. The reason of creating this hybrid algorithm is to offer better protection to the string. The time that requires to attack the hybrid system is the whole time of attacking all of the 3 algorithms as we use three key for the encryption and decryption reason.

The different result analysis for all the different algorithms is shown in table 1. The calculated values for different algorithm and hybrid algorithm are shown. The hybrid algorithm provides more security than individual algorithms for the same plaintext. The algorithm discussed here can provide better security rather than using individual algorithm at a time. The comparison of different parameters used for result analysis are highlighted in table.

As the hybrid algorithms combines 3 distinct cryptographic algorithms, the security of the statistics 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.

In the proposed system, the mode of input is string. Converting this string into binary mode and then passed for encryption and decryption purpose.

REFERENCES

[1] Bhavik Rana, Sunil Wankhade "A Comparative Study of Hybrid Cryptographic Algorithms" in *International Journal of Modern Engineering Research (IJMER), vol. 6, Issue 10, Ver. 2, pp 71-75, October 2016 (ISSN: 2249-6645).*

[2] 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.*

[3] 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.*

[4] 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.*

[5] 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].*

[6] 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.*

[7] 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.*

[8] 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.*

[9] Bhavik Rana, Sunil Wankhade "Hybrid Cryptographic Algorithm for Enhancing Security of Text" in *International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017), Volume: 5, Issue: 3, pp-339 – 344 ISSN: 2321-8169*, published in I*nternational Journal on Recent and Innovation Trends in Computing and Communication IJRITCC | March 2017.*

[10] AES.pdf [online]. Available: http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf

[11] DES.pdf [online]. Available: http://www.facweb.iitkgp.ernet.in/~sourav/DES.pdf.

[12] IDEA.pdf [online]. Available FTP: ftp://180.211.120.110/04%20IT%20Department/RNK/SE/International%20Data%20Encryption%20Algorithm.pdf