ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

Enhancing Data Security by using Hybrid Cryptographic Algorithm

Jigar Chauhan [1], Neekhil Dedhia [2], Bhagyashri Kulkarni [3]
[1], [2], [3] University of Mumbai

Abstract*— This project presents an approach to develop a Hybrid Cryptographic Algorithm. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. The algorithm is designed using combination of two symmetric cryptographic techniques which are AES and DES. This Project presents the design and implementation of a symmetrical hybrid based 128 bit key AES-DES algorithm as a security enhancement. Understanding the need to minimize algebraic attacks into the AES, this paper proposes the idea on integrating AES within the Feistel network of DES, hence resulting into the development of the Hybrid AES-DES algorithm.

Index Terms— **AES, Cryptography, DES, Feistel Structure, Hybrid Algorithm, Security.**

I. INTRODUCTION

A Computer Network is an interconnected group of autonomous computing nodes, which use a well-defined, mutually agreed set of rules and conventions known as protocols, to interact with one-another meaningfully and allow resource sharing preferably in a predictable and controllable manner. Communication has a major impact on today's business. It is desired to communicate data with high security. With the rapid development of network technology, internet attacks are also versatile, the traditional encryption algorithms (single data encryption) is not enough for today's information security over internet, so we propose this hybrid Cryptographic Algorithm [1].

II. METHODOLOGIES

A. AES

Advanced Encryption Standard (AES)[6] is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware. Unlike its predecessor, DES, AES does not use a Feistel network. AES has a fixed block size of 128 bit and a key size of 128, 192, or 256 bit, whereas Rijndael has specified with block and key sizes in multiples of 32 bit, with a minimum of 128 bit. The block size has a maximum of 256 bit but the key size has no theoretical maximum. [3]. AES operates on a 4×4 column-major order matrix of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are down in a special finite field. The steps of AES are as follows:
Substitute bytes — Uses an S-BOX to perform a byte-by- byte substitution of the block.

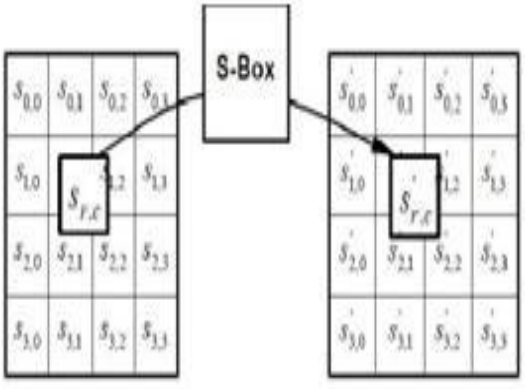

Fig. 1 AES Byte Substitution Process [7]

Shift rows— a simple permutation.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

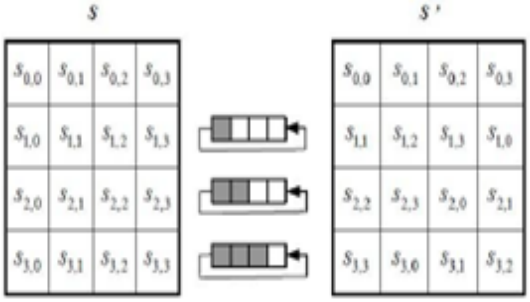

Fig. 2 AES Byte Shift Row Process [7]

Mix columns — transformation operates on the State column-by-column, treating each column as a four-term polynomial, the columns are considered as polynomials

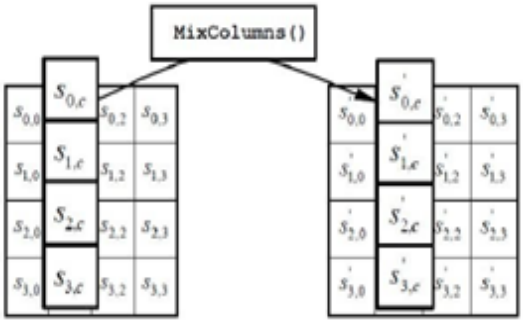

Fig. 3 AES Mix Column Process [7]

Add round key — a simple bitwise XOR of the current block with a portion of the expanded key.

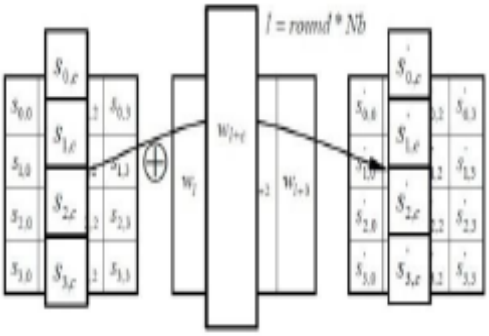

Fig. 4 AES Add Round Key Process [7]

B. DES

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bit and transforms it through a series of complicated operations into another cipher text bit string of the same length.DES [6] also uses a key to customize the transformation, so that decryption can only be performed by those who know the particular key used to encrypt. In the case of DES, the block size is 64 bit [4], but only 56 bit are used and the remaining 8 bit can be used for parity, and then discarded in the algorithm. Therefore, the effective key length of DES is 56 bit. The algorithm's overall structure is shown in Fig. 5: there are 16 identical same processes, termed rounds. There is also an initial and final permutation, known as IP and FP (the FP is inverse function of IP (IP—revocation FP operations, and vice versa)). Before the main rounds, the block is divided into two 32 bit half block and processed at same times; this crossing process is known as the Feistel scheme. Feistel scheme is used to ensure the similarity of both the encryption and decryption processes. The only difference is the sub-key, which is reversed and used in decryption process and remaining part it is the same. This design simplifies the algorithm implementation, especially for hard implementation. The symbol denotes the (XOR) operation.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

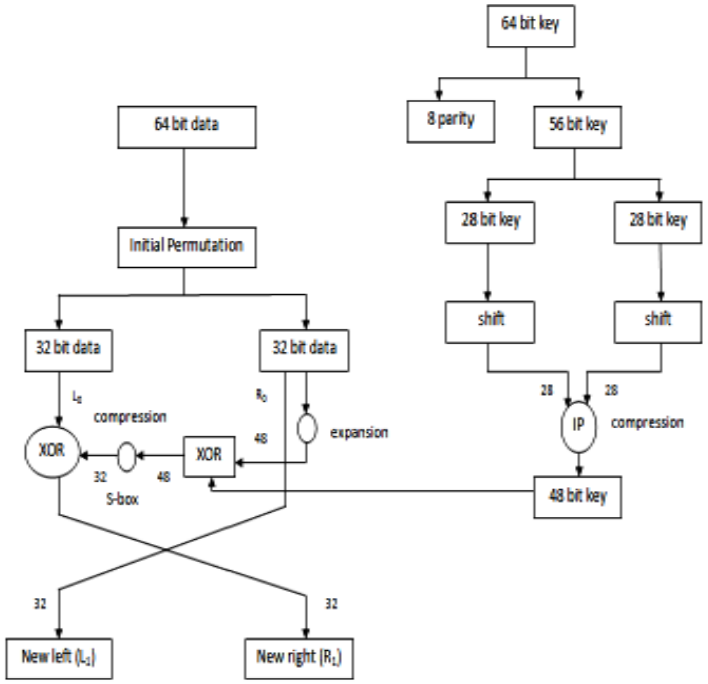

Fig. 5 Overall Structure of DES [2]

III. DESIGN ISSUES OF HYBRID CRYPTOGRAPHIC ALGORITHM

It is a design for transfer data with better security. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. This hybrid algorithm is designed for better security by combinations of AES and DES.

A. Overall structure

Fig. 6 shows the overall structure of the hybrid algorithm.

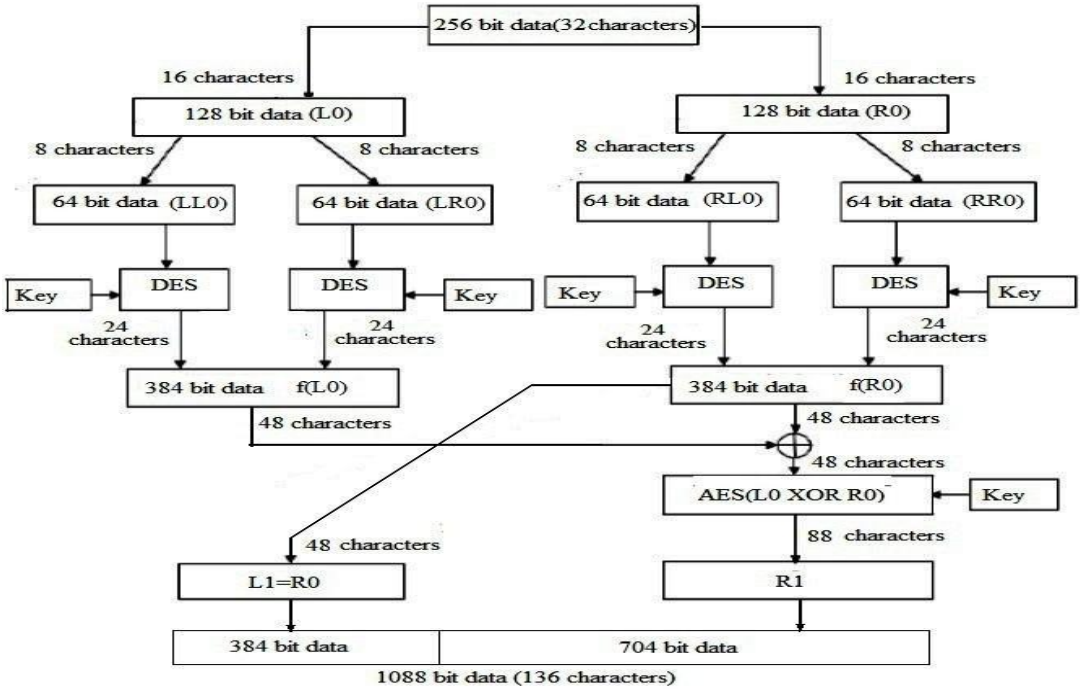

Fig 6: Hybrid Encryption Flow [1]

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

B. Concept of Hybrid AES DES

Mathematically, the idea of a hybrid based AES-DES can be construed with reference to basic DES Feistel equations. The repetition of these equations is based on the number of rounds as adapted by the Feistel network, which in the case of DES was standardized at 16. However, by incorporating the AES within this yield the following results.

L1 =f (R0) ---------- (1)

R1 =AES (f (L0) XOR f (R0)) --------- (2)

The user gives the plain text where the plain text is divided into two halves L0 and R0 of 128 bits each. Each half is then again divided into two halves that is we get LL0 and LR0 from L0 and RL0 and RR0 from R0 of 64 bits each respectively. DES algorithm is then applied to all the halves which are generated that is LL0, LR0, RL0 and RR0 using the key given by the user himself/herself. There is also a provision of using two different keys. If the user selects two keys option at the time of encryption the two different keys are used, one key is used DES encryption and the other key is used for AES encryption. If the user selects one key option at the time of encryption then the same key is used for DES and AES encryption. The output of DES encryption text is of 192 bits each. Since DES encryption is applied on four quarters each quarter generates an output of 192 bits. The output of LL0 and LR0 is clubbed together to form f (L0) and the output of RL0 and RR0 is clubbed together to form f (R0). The length of f (L0) and f (R0) is 384 bits each. Once we have got f (L0) and f (R0) they both are then XOR with each other i.e. f (L0) XOR f (R0). The length of the output will be same as the length of the input that is 384 bits. The result is then given to the AES algorithm where the result is encrypted using the key provided by the user. The key can be same or different as mentioned above. The output length of the AES encrypted text is 704 bits. The f (R0) can be termed as L1 and the AES encrypted text can be termed as R1. Both L1 and R1 are then clubbed together to give the cipher text of 1088 bits. The Decryption process is exactly reverse of the encryption process. Figure 7 shows the Hybrid Decryption flow.

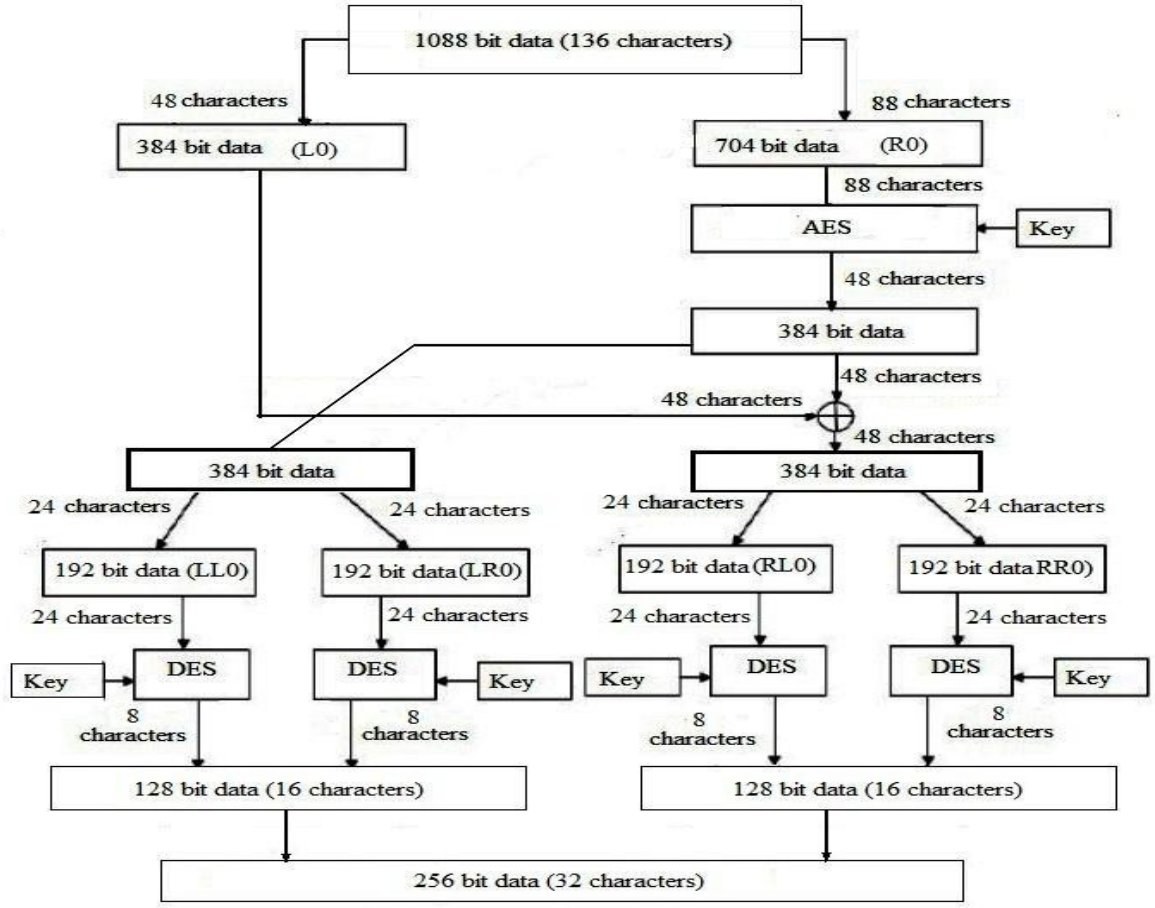

Fig 7: Hybrid Decryption Flow

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

IV. RESULTS

The AES, DES and Hybrid Algorithm have been implemented in Java and the following results were obtained. In Fig. 8 shows the Main interface. It include two tabs one for encryption and the other for decryption. The user can encrypt/decrypt message according to his choice. The user can also select the algorithm to encrypt from AES, DES or Hybrid. If the user selects Hybrid then again he has a choice of using one or two keys. The Menu button in the menu bar gives features like Fie Encryption, Image Encryption, File/Image Decryption and Random Key Generation.

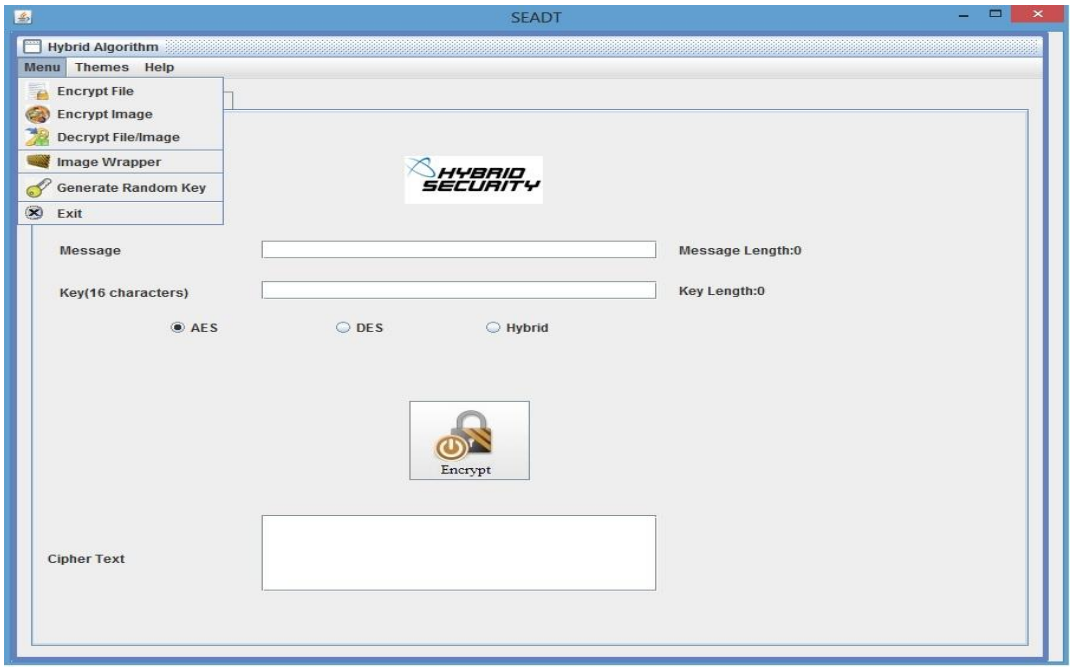

Fig 8: Main Interface

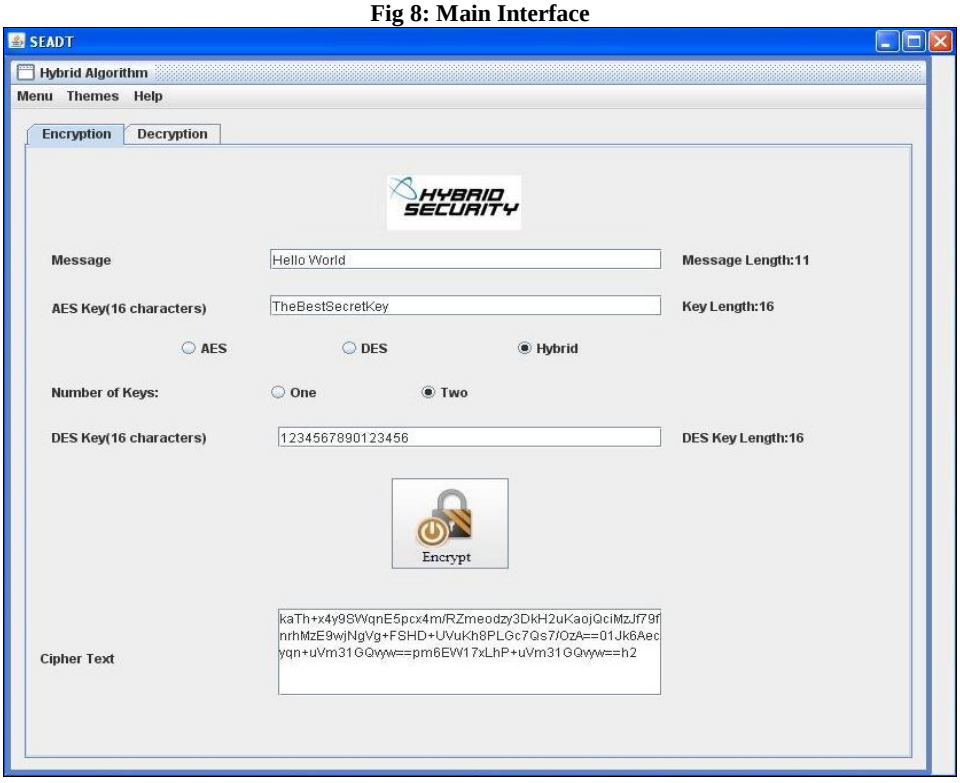

Fig 9: Message Encryption using Hybrid Algorithm

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

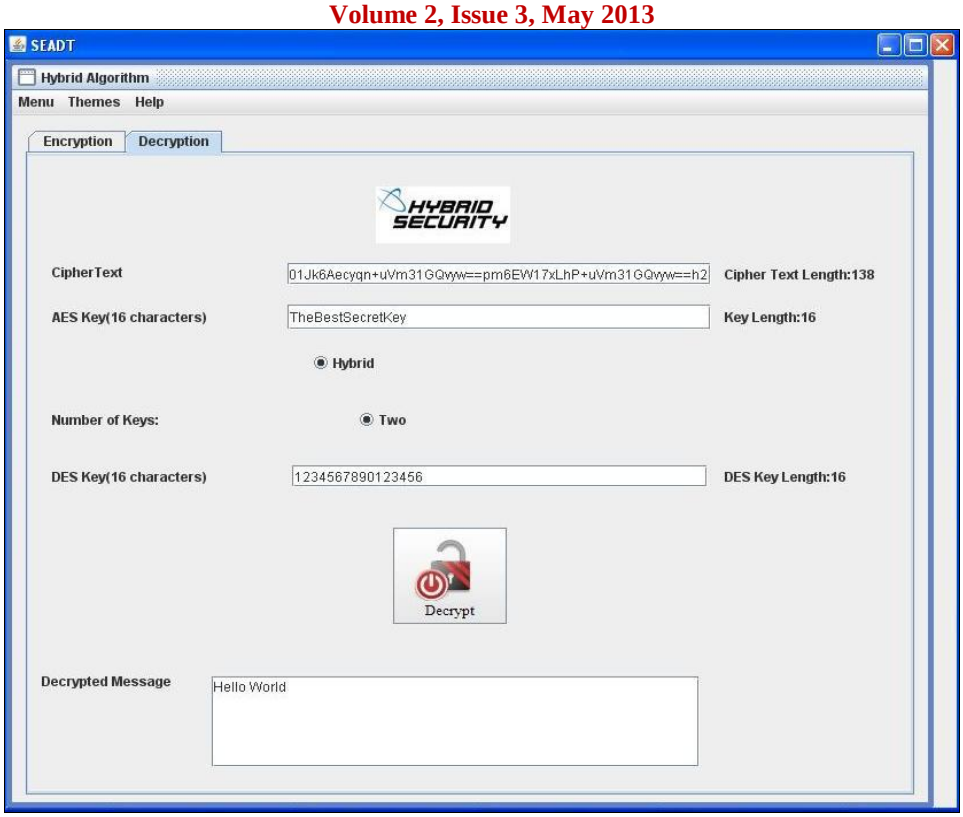

Fig 10: Message Decryption using Hybrid Algorithm

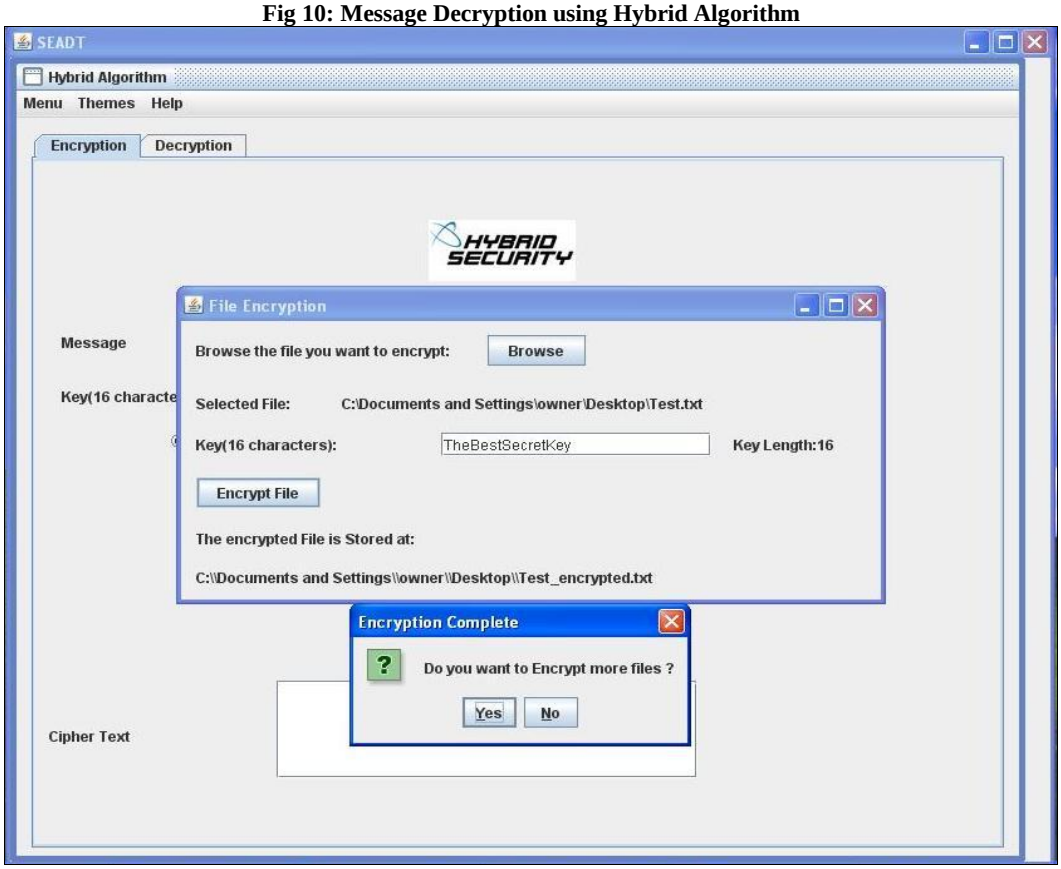

Fig 11: File Encryption using Hybrid Algorithm

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

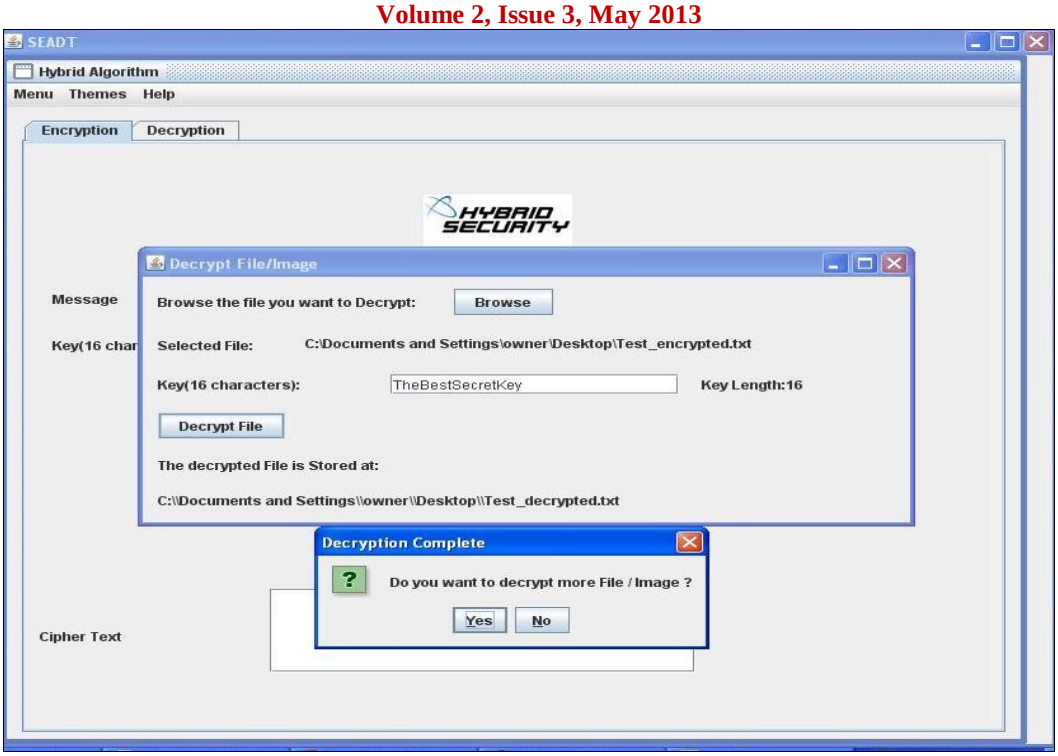

Fig 12: File Decryption using Hybrid Algorithm

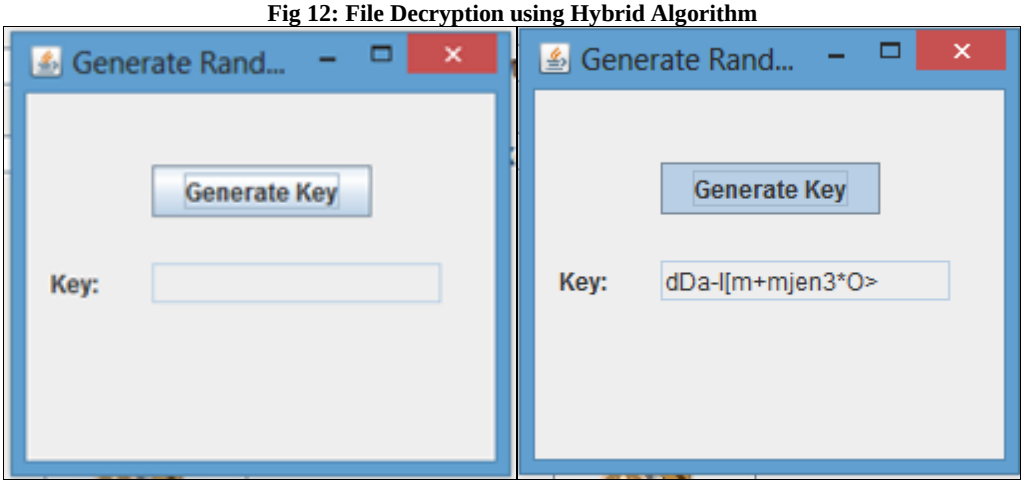

Fig 13: Random Key Generation Window

V. CONCLUSION

Thus the paper uses combined concept of AES and DES to obtain a hybrid model which can be used for encrypting various kinds of data. Nowadays it is very important to design strong encryption algorithms as the power of computers is growing day by day. Thus the hybrid model gives a better non linearity to the plain AES and as it is merged with DES, there is better diffusion. Hence the possibility of an algebraic attack on the hybrid model is reduced. Hybrid mode involves more computations as computations as compared to AES or DES alone hence; we can say that the encryption time for the hybrid model is much greater than the times for AES or DES alone. Thus it can be inferred that the hybrid model will take longer time to be broken by cryptanalysis

REFERENCES

[1] Vikas Kaul, S K Narayankhedkar, S Achrekar, S Agrawal, P Goyal, "Security Enhancement Algorithms for Data Transmission for Next Generation Networks", International Journal of Computer Application (IJCA).

[2] William Stallings:" Cryptography and network Security: Principles and Practices".

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 3, May 2013

[3] Advance Encryption Standard, [Online], Available: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[4] J.Orlin Grabbe:"The DES Algorithm Illustrated", [Online], Available: http://orlingrabbe.com/des.htm.

[5] Data Encryption Standard, [Online], Available: http://en.wikipedia.org/wiki/Data_Encryption_Standard.

[6] Deven N. Shah:"Information Security: Principles and Practice".

[7] U.S. Department of Commerce, National Institute Of Standards and Technology:"Advance Encryption Standard (AES)".

AUTHOR BIOGRAPHY

Jigar Chauhan pursuing B.E in INFORMATION TECHNOLOGY, Vidyalankar Institute of Technology, Mumbai University, was part of the group that has participated in a OPUS'13, A National level Project Exhibition and participated in X-ZIBIT 2013, A State Level Project Exhibition titled "SECURITY ENHANCEMENT OF DATA TRANSMISSION FOR NEXT GENERATION NETWORKS".

Neekhil Dedhia pursuing B.E in INFORMATION TECHNOLOGY, Vidyalankar Institute of Technology, Mumbai University, was part of the group that has participated in a OPUS'13, A National level Project Exhibition and participated in X-ZIBIT 2013, A State Level Project Exhibition titled "SECURITY ENHANCEMENT OF DATA TRANSMISSION FOR NEXT GENERATION NETWORKS".

Bhagyashri Kulkarni pursuing B.E in INFORMATION TECHNOLOGY, Vidyalankar Institute of Technology, Mumbai University, was part of the group that has participated in a OPUS'13, A National level Project Exhibition and participated in X-ZIBIT 2013, A State Level Project Exhibition titled "SECURITY ENHANCEMENT OF DATA TRANSMISSION FOR NEXT GENERATION NETWORKS".