Research Journal of Computer and Information Technology Sciences _____ISSN 2320 – 6527
Vol. **6(3),** 1-7, April **(2018)** *Res. J. Computer and IT Sci.*

Implementation of DNA cryptosystem using Hybrid approach

Manoj Kumar Pandey
Swami Shri Swaroopanad Saraswati Mahavidyalaya, Hudco, Bhilai, CG, India
manojpnd88@gmail.com

Available online at: www.isca.in
Received 28th June 2017, revised 17th March 2018, accepted 18th April 2018

Abstract

Data security is one of the important aspects of network security so we need encryption algorithm to increase data security like DNA Cryptography. This paper mainly focuses on implementation of the DNA cryptosystem with the use of AES and keys management using RSA algorithm and also verification of data at other side. The system has been implemented in java using NETBEANS IDE 8.2.

Keywords: Data security, AES, RSA, DNA cryptography, data verification.

Introduction

Cryptography is a field of study about the secret text. Encryption means converting plain text into cipher text and decryption is just reverse process of encryption means converting Cipher text into plain text[1]. Cryptography means converting plain text into secret codes. Sensitive information is being encoded using cryptography[2]. Information security has rich set of encryption algorithm. They can categorize in private key encryption and public key encryption, in private key encryption only one common key is used whereas in public key encryption public and private key is used[3]. Public key is known publicly, used to encrypt data whereas private key is only known to the authorized user and cipher text can only be decrypted using private key. An application that enables both encryption and decryption is called cryptosystem. The size of key used for encryption specifies the level of security. For example if key size is 512 and 1024 bits respectively then 1024 bits key is more secure than 512 bits keys[4]. The size of the key space is propositional to the time taken to crack the cipher text by the intruders[2]. Key management is one of the important aspects of cryptosystem, the more efficiently we manage those key, and more security will be provided to the system. DNA cryptography is a new area of cryptography research which derived from the biology[5]. This paper holds implementation of DNA cryptosystem using AES and managements of keys using RSA algorithm.

DNA Encryption Algorithm

DNA cryptography is a modern technology and has been derived from biotech field. DNA cryptography can play a vitalrole in the field of network security. In DNA cryptography we substitute following values for the binary numbers and a chain of DNA is generated which is more secure and reliable. In DNA cryptography mixture of mathematical and biological concepts are used to get the encrypted data in the form DNA sequences. The benefit of this scheme is that it makes difficult to read and guess about data (plain text)[6].

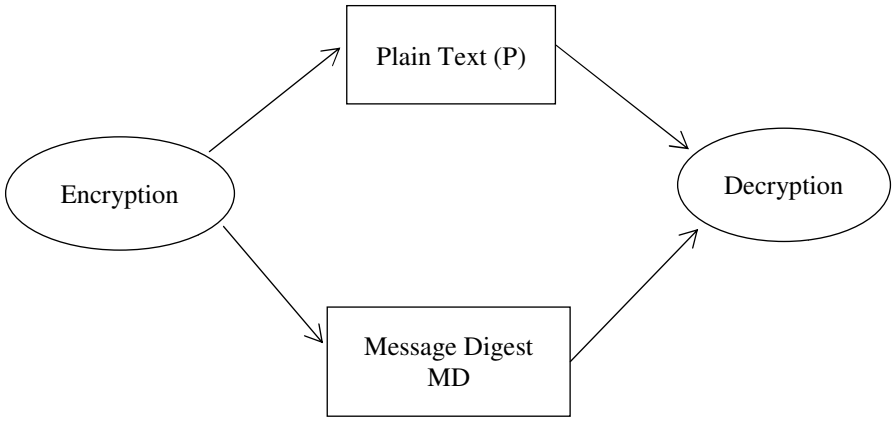

Figure-1: Encryption and decryption process.

Problem Identification

In this era it is very important to keep messages secure and now a days many technologies has been developed to protect messages from intruders, and along with that modern system and technologies have also been developed to crack the messages being sent over the networks so there is a need of powerful techniques that can provide higher level of security and reliability. DNA cryptography can be used to achieve higher level of security and reliability.

Problem Solution

The solution of the problem is to use an algorithm which is complex and reliable too. Here we have used AES using 128 bit for implementing DNA cryptosystem. In order to ensure the integrity of the message concept of hashing is also used using SHA-256 algorithm. One of the main problems encountered during the implementation is to maintain different keys. The keys should be kept in such a way that it should not be accessible to any unauthorized user while communication otherwise it could reveal the secret.

There are two ways to manage the keys such as: i. Using a separate database, which can only be accessed by authorized user? ii. Using RSA in order to manage keys while communication (RSA Key Exchange)[7,8].

The implementation of system using first way requires enough security so that only authorized user can access keys. The implementation of system using second way is more appropriate and does not requires much overhead to get the task done. This paper contains the implementation using the second way and the steps are as follows: i. Keys K1 will be encrypted using RSA algorithm (1024 bit key) to obtain CK1 using public key PK1. ii. Private Key will be sent to the receiver so that keys CK1 can be decrypted using the private key to get original keyK1 in order to decrypt the cipher text, which has been sent to the receiver, to get plain text.

Working of Proposed System

This section of the paper contains the working of the proposed system at the side of sender and the receiver too. Appropriate diagram has also been used wherever required so that working can easily understand by the readers.

At the sender side: i. A plain text will be given by the user as input in the first phase where AES encryption will be performed using 128 bit key, to get cipher text C1. ii. Cipher text C1 received from the first phase will be converted into binary text B where each converted value is composed of 8 bits. (add extra bits in order to make it of 8 bits). iii. Now covert binary text into corresponding DNA base pair (amino acid group) to get DNA encrypted text[5]. iv. Apart from that a hash function H (SHA-256) will be put on the original plain text to obtain the message digest MD1, which will be sent to the other side. v. Keys K1 will be encrypted using RSA algorithm to obtain CK1 using public key PK1. vi. DNA encrypted text, encrypted keys CK1 and message digest MD1 will be written in a registration entry file and likewise private key will be stored in a another file, which will be sent to the receiver for decrypting at the other end.

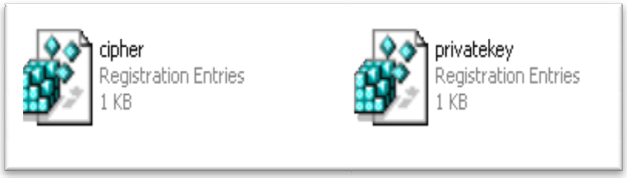

Figure-2: File structure.

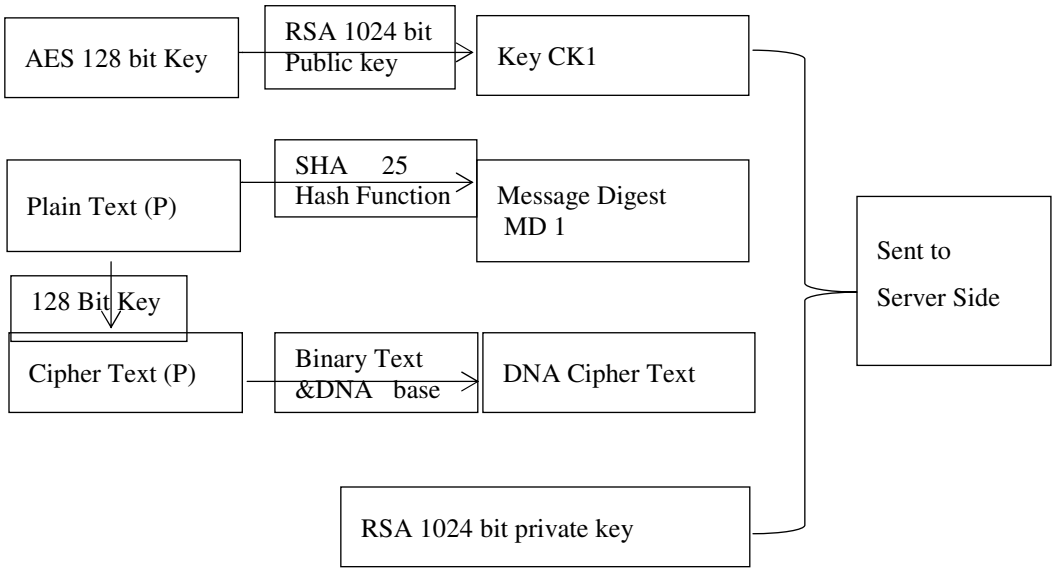

Figure-3: Working of the proposed system.

At the receiver side: i. At the receiver side the DNA cipher text C1, keys CK1, private 1024 bit RSA key and Message Digest MD1 will be read from the registration file and decryption will be performed on Keys Ck1,using private key to get Keys K1. ii. After obtaining key K1 we apply amino acid group base to get binary text where each value is composed of 8 bits. iii. In obtained binary text we apply reverse method to get original decrypted text message (cipher text). iv. Now we apply AES 128 bit decryption process using key K1 to get original plain text. v. Now a hash function H (SHA-256) will be put on the obtained plain text P to obtain the message digest MD2, which will be compare with the message Digest MD1. vi. If both MD1 and MD2 matches then we can say that original message has not been altered otherwise the original message has been altered with.

Implementation of the System

This section of the paper contains the implementation of the system step by step. Appropriate diagram has been used wherever required. Working of system at the side of the sender and receiver has been explained using the diagram. i. Figure 4 depicts that a plain text P will be passed to the AES encryption phase using 128 bit keys to get cipher text C. ii. Cipher text C would be converted into binary text. iii. Binary text is converted into DNA base pair i.e. DNA encrypted text.

Table-1: DNA digital coding.

Coding DNA Nucleotide	Decimal	Binary
T	3	11
G	2	10
C	1	01
A	0	00

The Figure-5 depicts that a message digest can be generated using SHA-256 algorithm (hash function) by applying it on the plain text to get Message Digest MD1, which will be sent to the other end along with the encrypted key.

Figure-6 depicts the decryption process which is just reverse of the encryption process mentioned in Figure-4.

The Figure-7 shows the comparisons of message digest will be performed at the receiver side in order to check the integrity of message being sent.

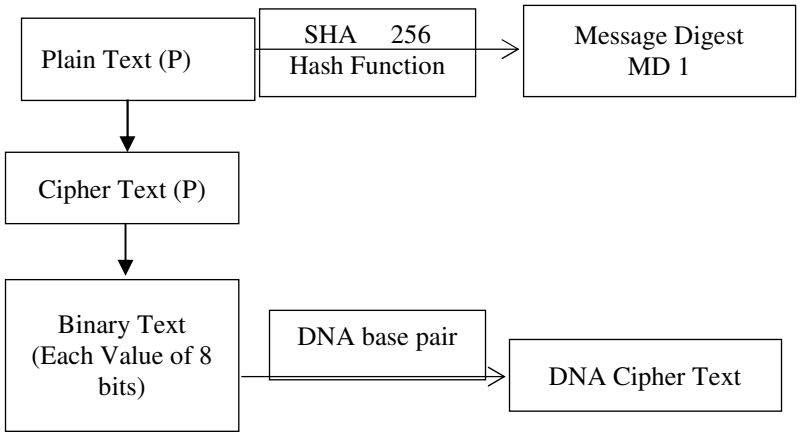

Figure-4: Working of the system at sender side.

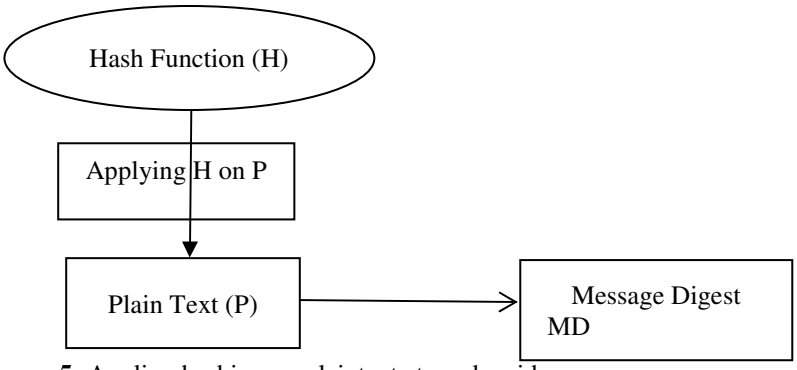

Figure-5: Appling hashing on plaintext at sender side.

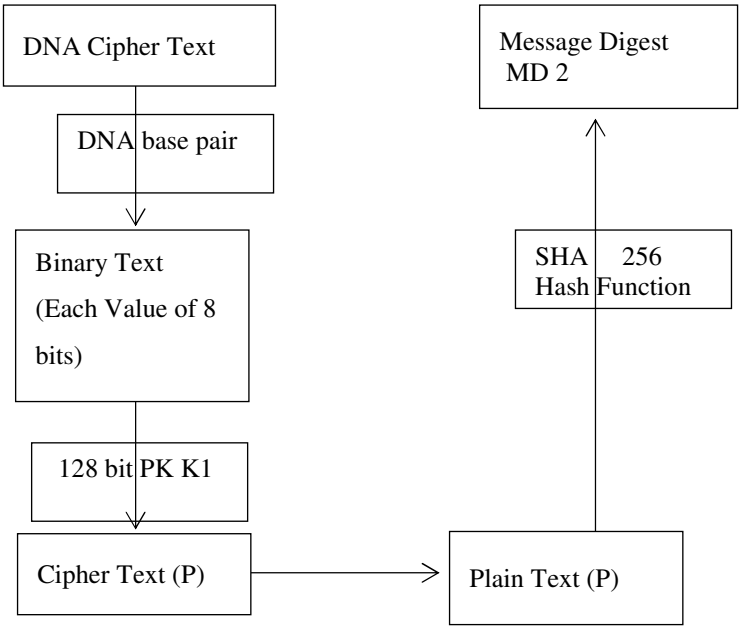

Figure-6: Working of the system at other side.

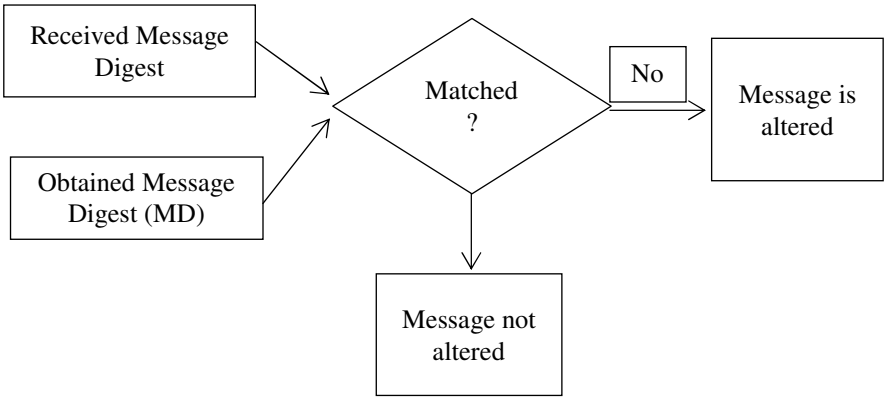

Figure-7: Verifying decrypted message at receiver side.

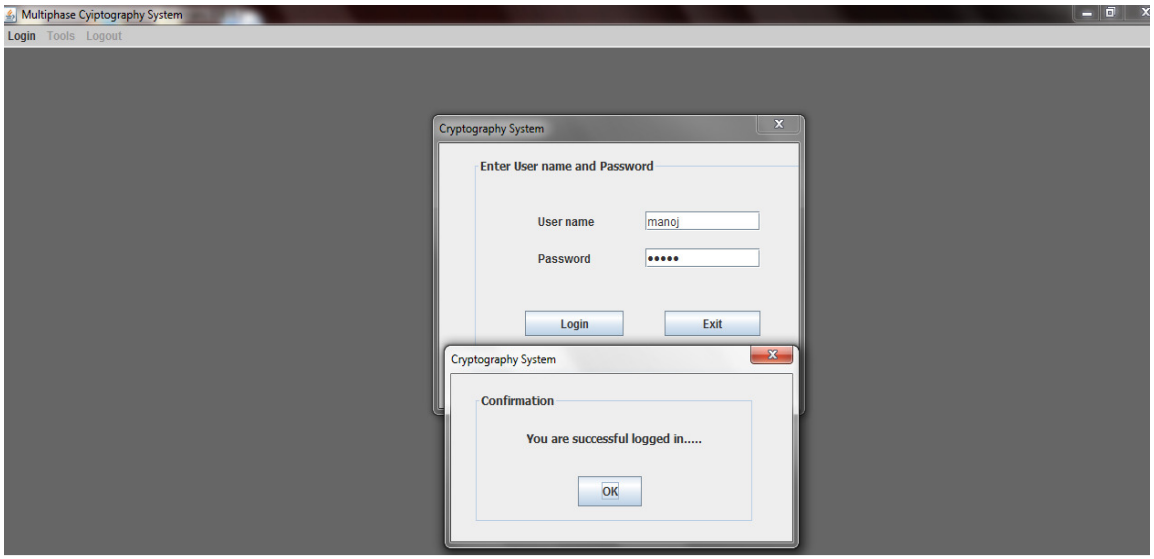

Figure-8: Login page.

In Figure-9 is encryption page where DNA encryption of any given text is performed and time taken for encryption is calculated each time. In this page message digest MD1 and encrypted key K1 (using RSA 1024 bit public key is stored) and from this page we save DNA cipher text, MD1 and encrypted keys into registry file.

In Figure-10 is Decryption page in which we have to read Cipher text and RSA private key written on registry entry file and then DNA Decryption of cipher text is performed and any type of alteration in original message is checked each time using message digest and also time taken for decryption is calculated each time.

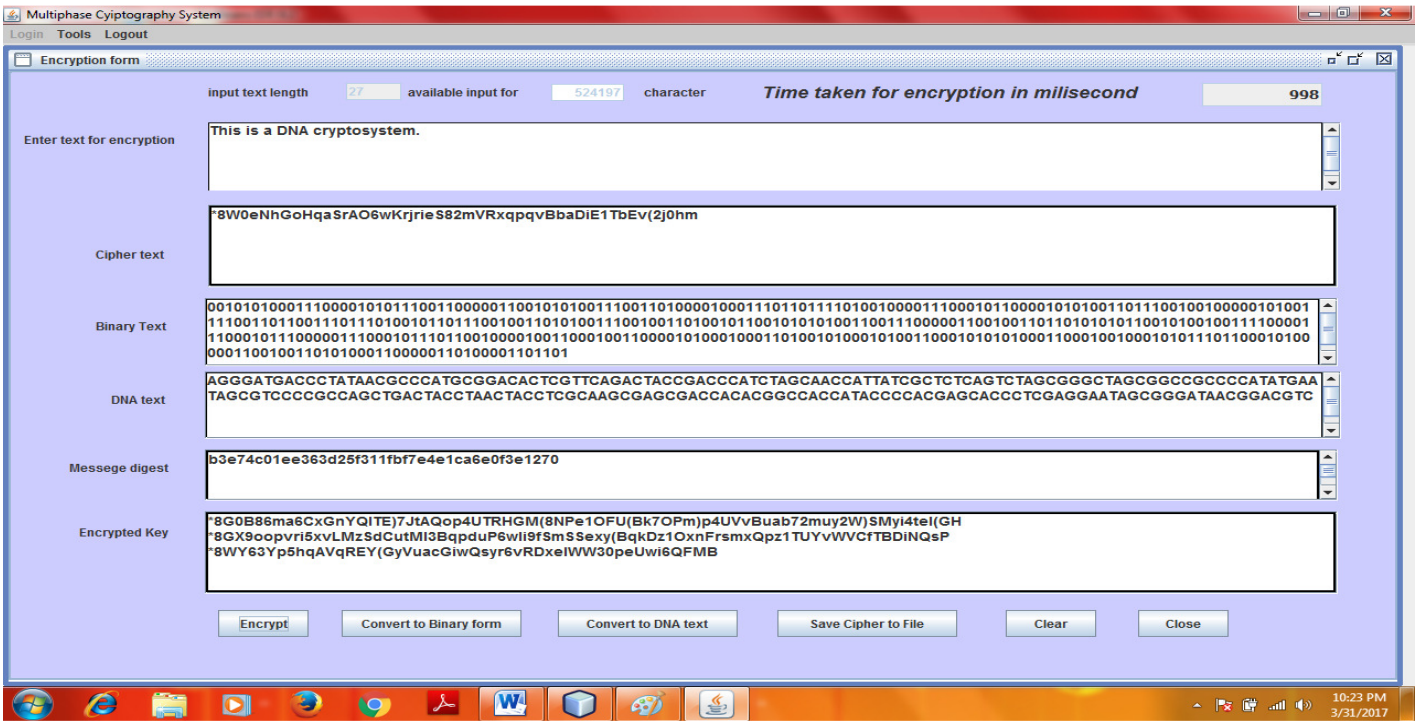

Figure-9: Encryption page.

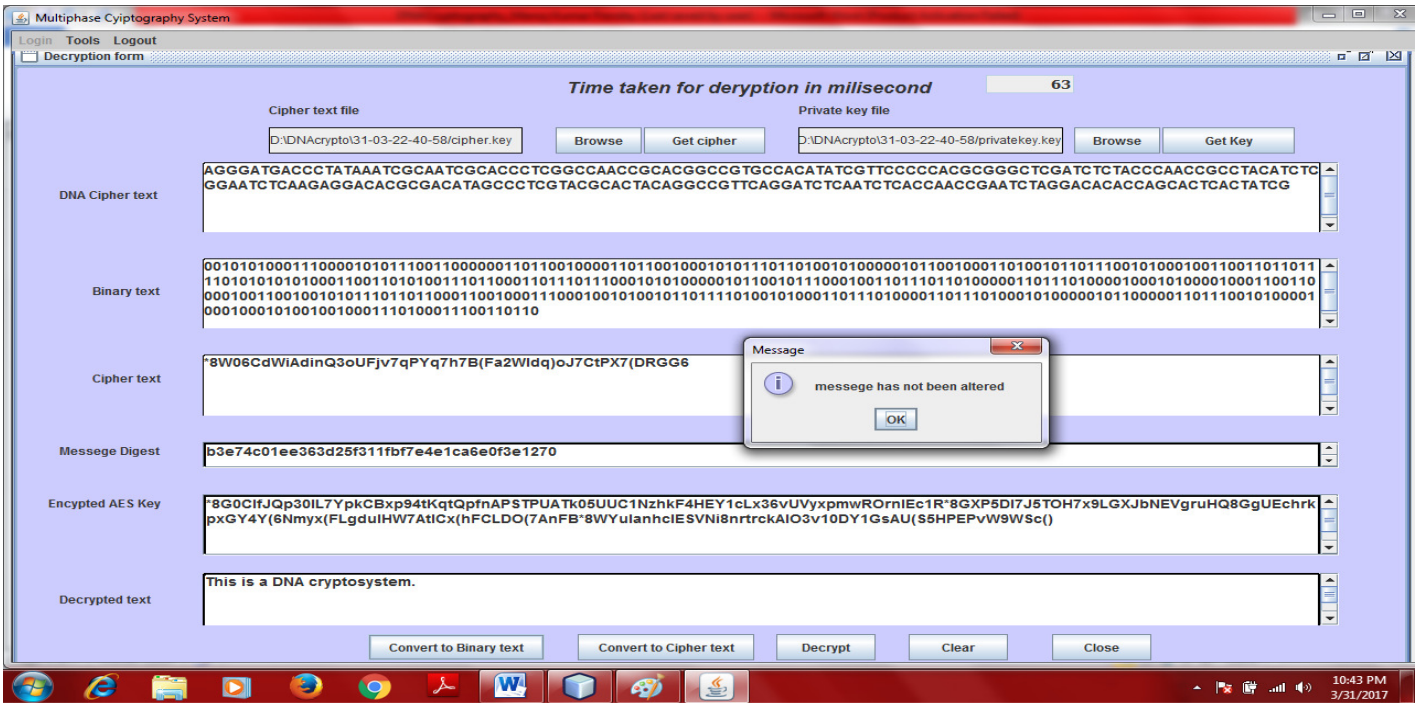

Figure-10: Decryption page where message is not altered.

In Figure-11 is Decryption page in which we can verify whether message has been altered or not if there is any alteration in between we will get message like above diagram.

Comparisons

We have compared encryption and decryption time for various Size of text file i.e. 1KB, 2KB,3KB,4KB and 5KB and results are shown in following given chart. In the following chart the encryption time is much higher than of decryption time it can be because of RSA key encryption takes lot of time during encryption.

Conclusion

Data security is one of the prime aspect of network security it includes mechanism to prevent unauthorized access of data while communication. The implementation of DNA encryption is a step ahead to the network security. DNA encryption is a fusion of cryptography with DNA based molecular. It plays an important role in the modern cryptography.

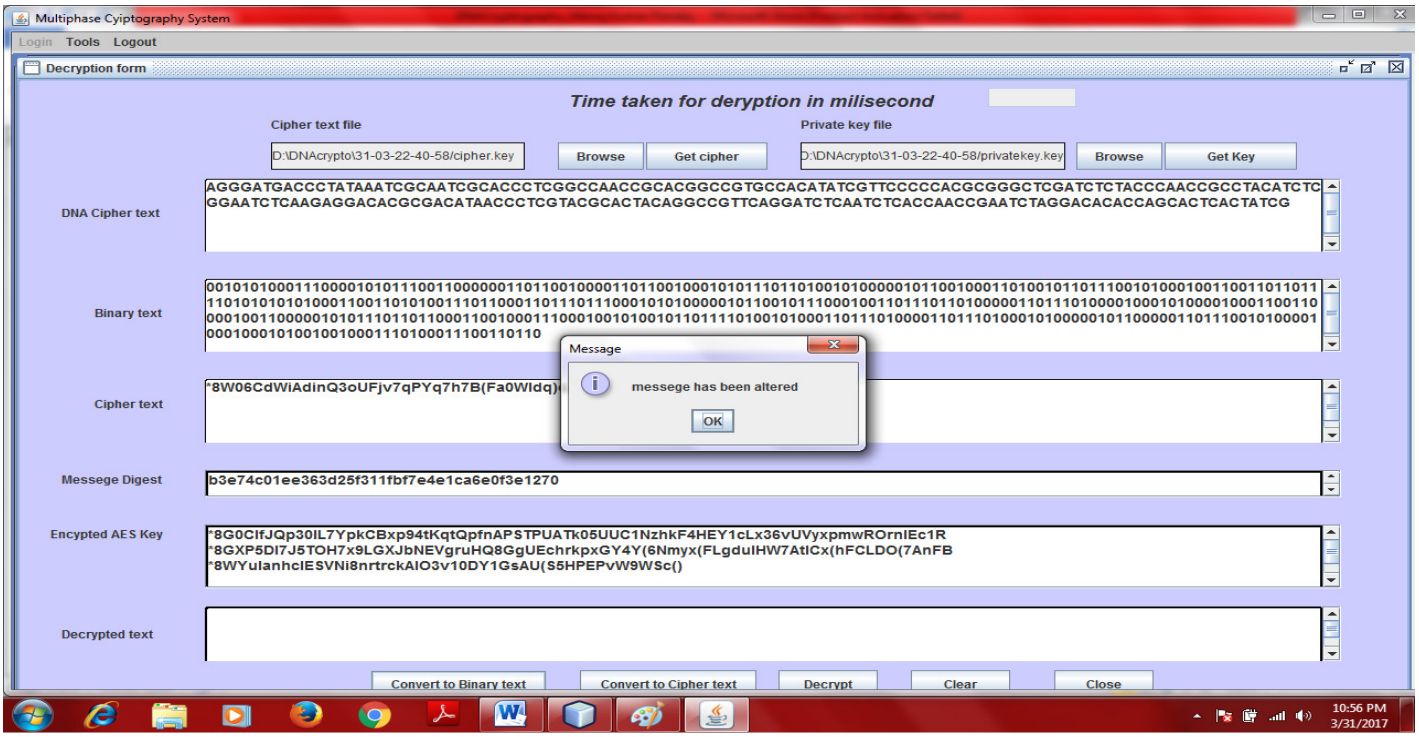

Figure-11: Decryption page where message is altered.

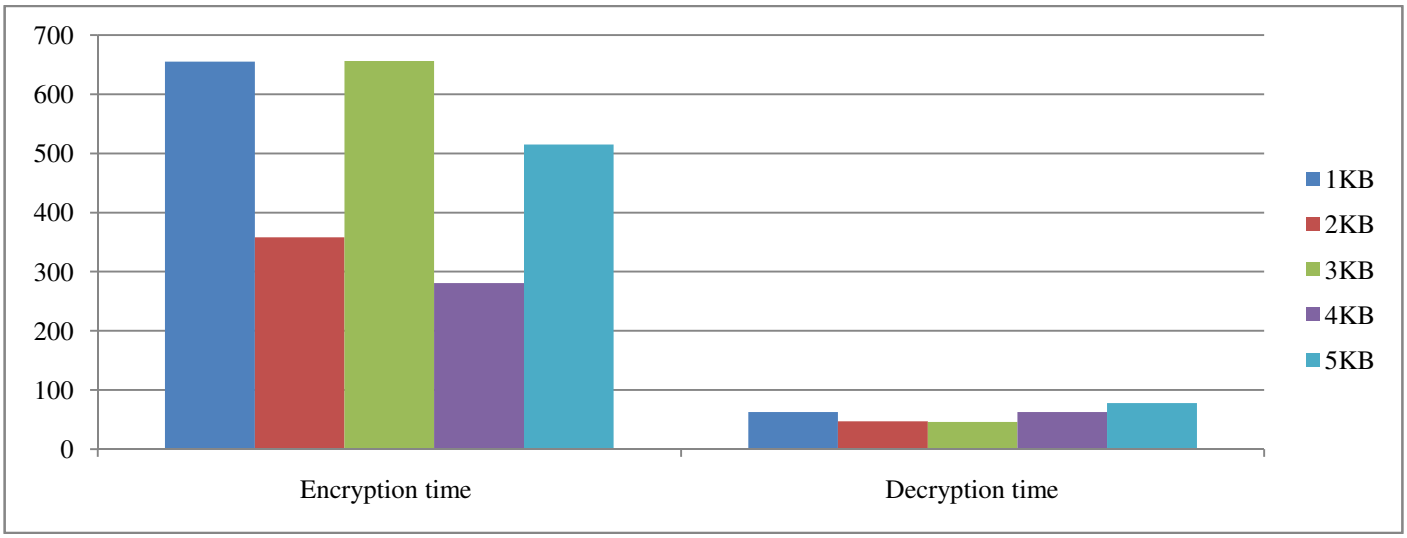

Figure-12: comparisons of encryption and decryption time of various texts file having different size.

References

1. Thakur J. and Kumar N. (2011). DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis. *International journal of emerging technology and advanced engineering*, 1(2), 6-12.

2. Soni S., Agrawal H. and Sharma M. (2012). Analysis and comparison between AES and DES Cryptographic Algorithm. *International Journal of Engineering and Innovative Technology*, 2(6), 362-365.

3. Kumar Yogesh, Munjal Rajiv and Sharma Harsh (2011). Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures. *International Journal of Computer Science and Management Studies*, 11(3), 60-63.

4. Posch K.C. and Posch R. (1995). Designing a new encryption method for optimum parallel performance. *Algorithms and Architectures for Parallel Processing*, 1995. ICAPP 95. IEEE First ICA/sup 3/PP., IEEE First International Conference, IEEE, 2, 849-854.

5. Pant V. and Kumar A. (2016). DNA Cryptography an New Approach to Secure Cloud Data. *International Journal of Scientific & Engineering Research*, 7(6), 890-895.

6. Javheri S. and Kulkarni R. (2014). Secure Data Communication Using DNA based Cryptography in Mobile Adhoc Network. *International Journal of Science and Research (IJSR)*, 3(9), 1504-1508.

7. Microsoft (2017). Secret Key Exchange. http://technet.microsoft.com/en-us/library/cc962035.aspx. 12/04/2017

8. Mokhtarnameh R., Muthuvelu N., Ho S.B. and Chai I. (2010). A Comparison Study on Key Exchange-Authentication protocol. *International Journal of Computer Applications*, 7(5), 5-11.