International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362
IJARST

SECURE DATA TRANSMISSION FOR CRYPTOGRAPHY USING STANDARD FORMAT

ARULKUMAR M
Assistant Professor, Department of Electronics and Communication Engineering
Government College of Engineering, Bargur, Krishnagiri-635104
Mail id: arul03@gmail.com

Abstract - Network security and cryptography (encryption & decryption) is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. In this paper we also studied cryptography along with its principles. Cryptographic systems with ciphers are described. The cryptographic models and algorithms are outlined.

Keywords: Network Security, Authentication; Cryptography; Encryption; Decryption;

1. Introduction

Since this information happen to more significance and secrecy like managing account information, military information, delicate data like medical records, and multimedia data, for example image, sound, or video. This requires a need of satisfactory and successful cryptographic algorithm to secure these sorts of information transmissions from an unauthorized user revealing. Then again, the pace of the innovation and the improvements in the field of computational processing speed in our lives is turning out to be quicker and speedier. These improvements facilitate the threats and attacks on the information or data to uncover its secrecy progressively and load the enormous test of fulfill the undertaking of securing the communications. Best approach of security assurance is Encryption. For changing input image into another image, encryption system used many techniques. So that changed image is difficult to understand by other unauthorized person and to maintain the secret of images between clients. Another advantages of encryption technique is can’t access the image information without decryption key. Main application of image encryption is multimedia frame work. Here we are using established cryptographic algorithm that is Data Encryption Standard (DES). DES was a generally utilized cryptosystem for securing the characterized information transmissions. DES is a symmetric key cryptosystem that is nothing but for both encryption process and decryption process, using same secret key. Many algorithm keeps DES as their core design for cryptographic design. By upgrading DES's security, other algorithm' security, for example, Triple-DES and IDEA will be improved. In this project, a capable change is proposed to bring the legacy DES to live by strengthening its security.

2. Cryptosystem

security service of cryptography

Cryptography is art of making a cryptosystem is shown in Figure.1, equipped for giving data security. Cryptography manages the genuine securing of advanced information. It refers to the outline of systems in view of mathematical algorithms that give major data security

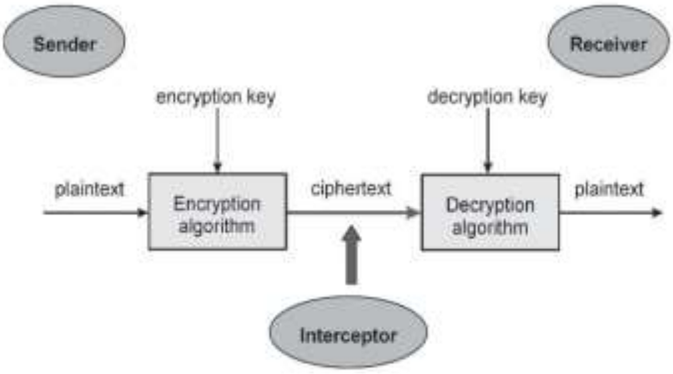


Figure.1 Cryptography

security services of cryptography

Authentication- Identity of the receiver and sender should be verified in communication system, before sending as well as receiving the information in system.

Secrecy or confidentiality- In the secured system, this is a task of the system to how best security which people maintain. Authorized users are capable to understand and access the data in the system.

Integrity- Assurance of the transmitted data has to be free for any alternation between sender and receiver in communication.

Non repudiation- guarantees the package security, element can't decline the responsibility for past activity. This is nothing but information sender and receiver certification

.

3. Image Encryption

Image encryption is necessary for future multimedia Internet applications. Password codes to identify individual users will likely be replaced with biometric images of fingerprints. However, such information will likely be sent over a network. When such images are sent over a network, an eavesdropper may duplicate or reroute the information. By encrypting these images, the content still has some degree of added security. Furthermore, by encrypting non-critical images as well, an eavesdropper is less likely to be able to distinguish between important and non-important information. Image encryption can also be used to protect privacy. An example for image encryption to protect privacy is in medical imaging applications. Recently, in order to reduce the cost and to improve the service, electronic forms of medical records have been sent over networks from the laboratories to medical centres or to doctors' offices. According to the law, medical records, which include many images, should not be disclosed to any unauthorized persons. Medical images, therefore, should be encrypted before they are sent over networks. Moreover, image encryption can be used to protect intellectual properties. One of concerns of the entertainment industry is that movies and videos in digital format are vulnerable to unauthorized access, theft, and replication. Entertainment industry has lost billion dollars due to the illegal copies. Recently, new technologies have been developed which allows multimedia can be delivered to millions of household very quickly. Entertainment industry will utilize Internet and satellites for multimedia distributions. The threat of unauthorized access during transmission over networks and the threat of illegal copy increase significantly. Image encryption, therefore, can be used to minimize these problems. Although encryption is sufficient to protect digital images and videos in some civil applications, this issues have taken into consideration when advanced encryption algorithms are specially designed for sensitive digital images and videos, for their special features are very different from texts.

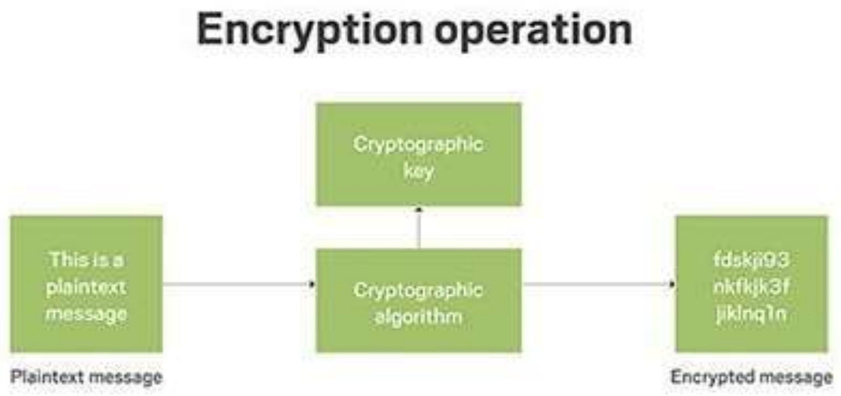


Figure.2 Encryption

As show in Fig.2, the first output is sampled from the stream of binary bits, which are packetized. The second output is the encrypted signal. This is due to Applying the Encryption Technique .The third output is sampled directly from the input file. We compare the encrypted signal with the original image sample in the results. We explain the implementation of technique of the encryption and decryption implementation in the following sections.

4. Encryption Standard

The implementation structure of DES is Fiestel cipher. In Fiestel structure as 16 rounds of steps are used.64 bit block size is used for DES structure .It has 64 bit key length, but DES utilizes only 56 bit key. Remaining 8 bits is used later but not used for encryption. Considering the method, Encryption process includes two inputs to the function of encryption. That in plain text is an input and key. In encryption process of DES used 64 bit plain text and 56 bit length key three steps of plain text processing are shown in the left side of the above figure.2. First step is initial permutation, 64-bit blocks input plain text is rearranges the bits. That is considered as permuted input, which means arranged bits. This step followed by 16 rounds of operation continusly. These 16 rounds process involves the permutation, substitution function, Last 16th round considered as output. So this last round had 64 bits. The key and function of output data is of 64 bits. Swapping the right and left side output halves. Swapped data is called as pre output, last step includes inverse permutation process of pre output that is called as reverse operation of initial permutation that is final permutation it has 64 bit length output. 56 bit key is produced in the right side of the figure, this key is passed in permutation block for encryption .Key can written as by name sub key Ki ,it is a combination of permutation and left circular shift. Same permutation function is used but produced sub keys are different because shift of the key bits are repeated.

DES algorithm

As already mentioned DES is symmetric key block cipher algorithm. Currently this algorithm use identical secret key for both encryption process and decryption process. General algorithm design 64 bit plaintext used as input. The algorithm transforms input into series of block which is 64 bit cipher text.16 rounds of encryption process is handled for every plaintext block. Decryption process is done in reverse manner of encryption method, by introducing sulky ki introduced by main key k where i=1………16

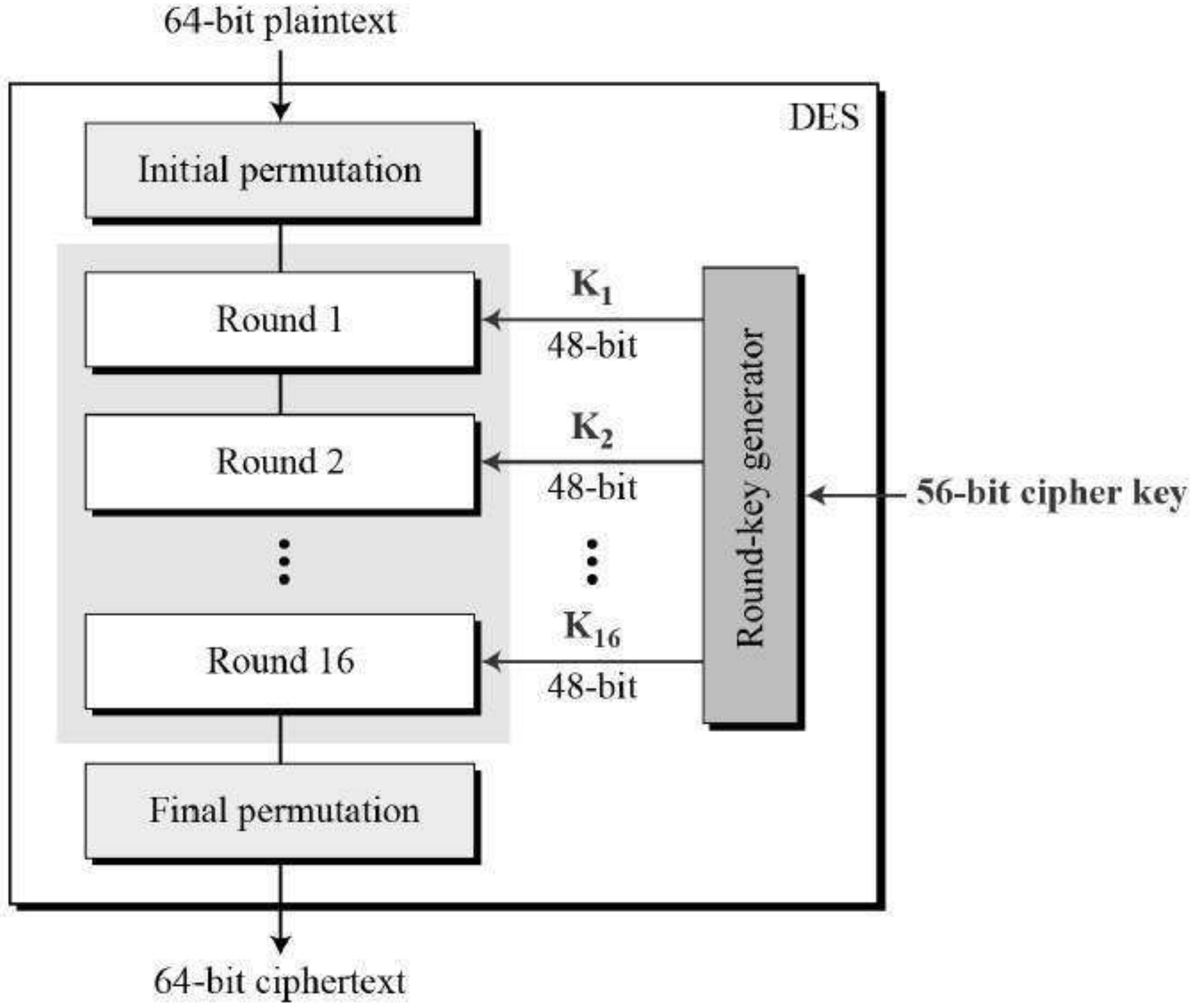


Figure. 3 plain text to cipertext

single DES round operation

As shown in figure 3, DES algorithm structure three phase of operation is considered for plain text. Input data undergone initial permutation in first phase of operation. In second phase produced permuted output that is rearranged. IP blocks split into two parts named R0, L0.Performs substitution and permutation process by function f and sub key Ki. Function f XOR ed with 32 bit right half data. Final phase is swapping between left and right half of system algorithm. This procedure repeated for next 15 round it considering the below equations. Li = Ri-1 R i= Li-1⊕f (Ri-1, k i). R16 and L16 swapped again after the 16th round process. Reverse operation of initial permutation is called final permutation, to get cipher text. Finally we got output of 64- bit data same as input data.

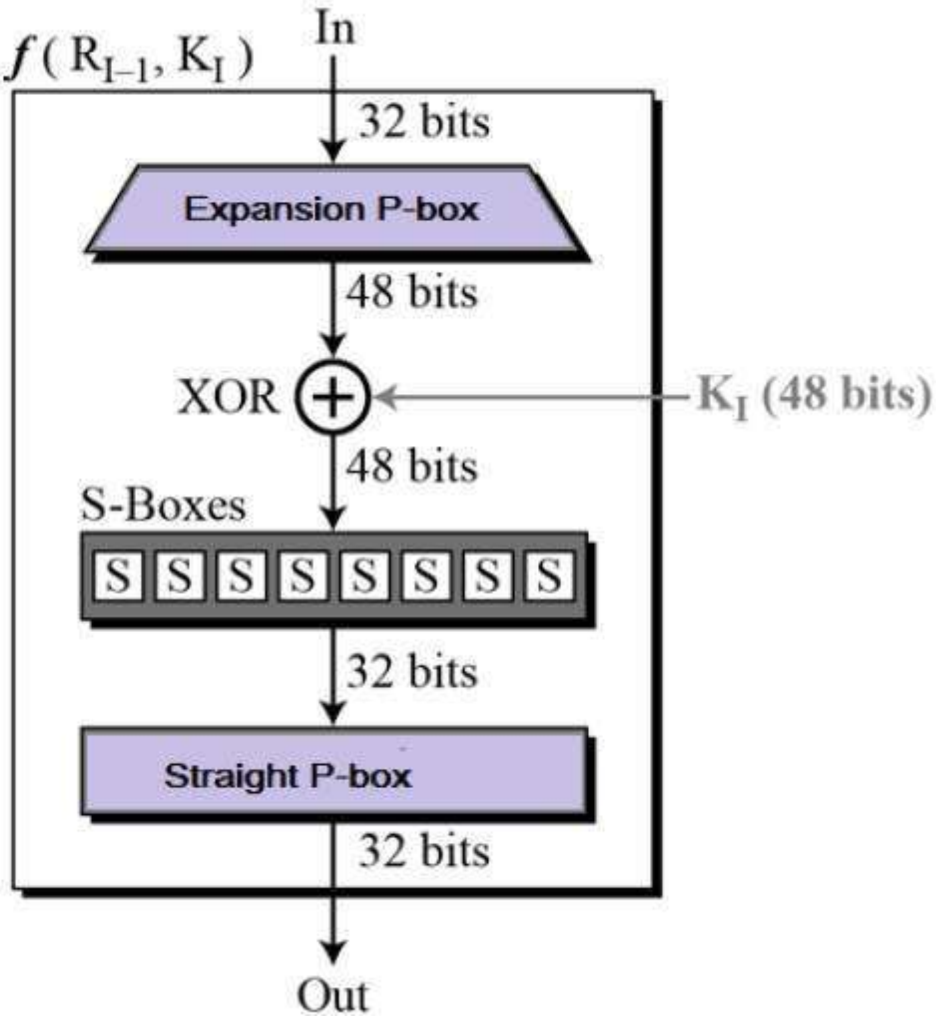


Figure. 4 Block diagram

5. Technique Encryption of Image

Binaries Image:

It will extract three channels from input image (color image) and converts the values of it to binary values. The binary values are stored in one multidimensional array as Data Here we have to generate total three arrays which represent three different channels of image i.e. red channel, green channel and blue channel.

LSB of RGB:

In this process we will consider input image for key generation and converts the value of its pixel in binary. After converting in binary; Least Significant Bit (LSB) will considered from each pixel**.**

Key Generation:

A cryptographic key is information generated to encrypt and decrypt the message. At the receiver side the exact reverse is done to getting original image. We will generate keys for encryption/decryption process. In this process consider input image which have to encrypt. For key generation channels (red or green or blue) will be extracted from the selected image. In key generation process three keys are generated from the color image i.e. one key will generated from red channel one key will generated from green and similarly one key will generated from blue channel. After that binary value of each pixel is calculated and these values are stored in one array. After generation of binary array each pixel is scanned and LSB of each pixel is calculated and new array of these LSB value is generated. Finally, to generate key each bits of LSB array is scanned and neighbor pixels having absolute difference one will be stored in one array.

Encryption:

After that three different keys will be generated using the image after that using key arrays and arrays of binary value encrypted images are generated. To encrypt the image XOR operation is performed on keys and three different channels of image as shown . In encryption process red channel of input image will be encrypted using the key generated from the red channel of color image which is used for key generation and similarly green channel and blue channels are encrypted with the key generated from the respective channel.

Decryption:

The decryption process is the exact same process as Encryption. For Decryption generating Key by using cipher image hence we don't need to save key which is generated at time of encryption and is efficient as security purpose. After that XOR operation is performed on array of keys and array of cipher images and array of original channel is calculated. This operation is performed on all red, green and blue channels and value of all channels is calculated. After that from the value of all three channels original image is extracted. This process of decryption done on receiver side as describe in Picture

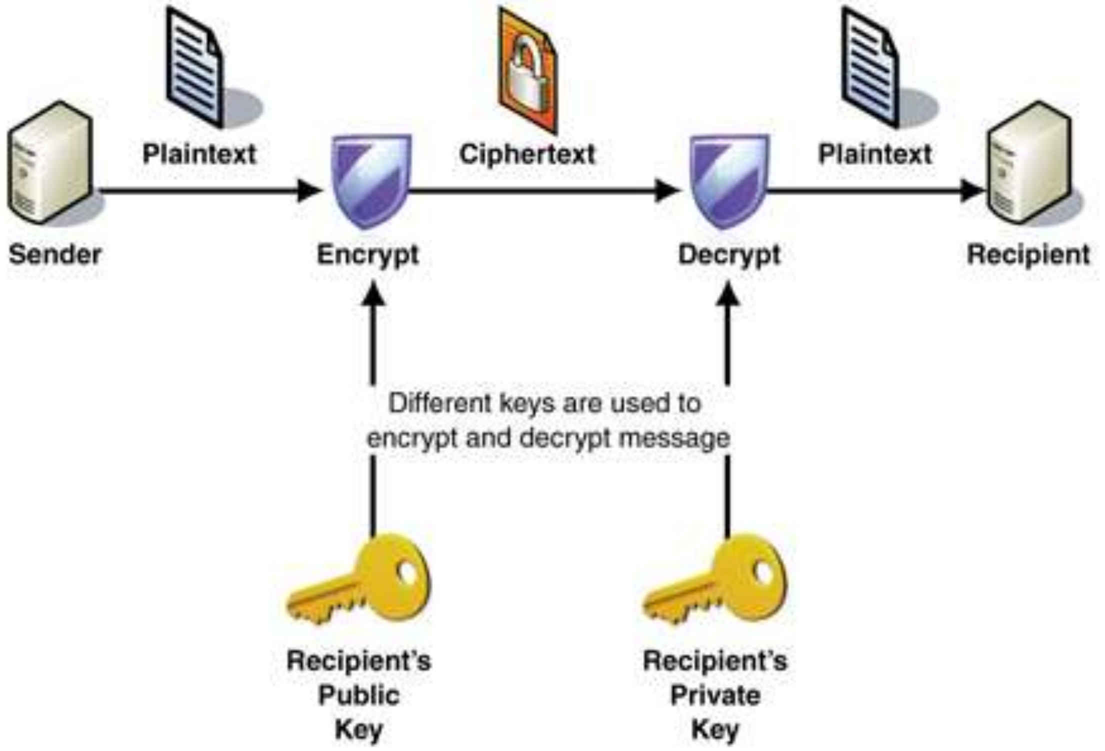


Figure. 5 Encryption & Decryption Process

Software Specification

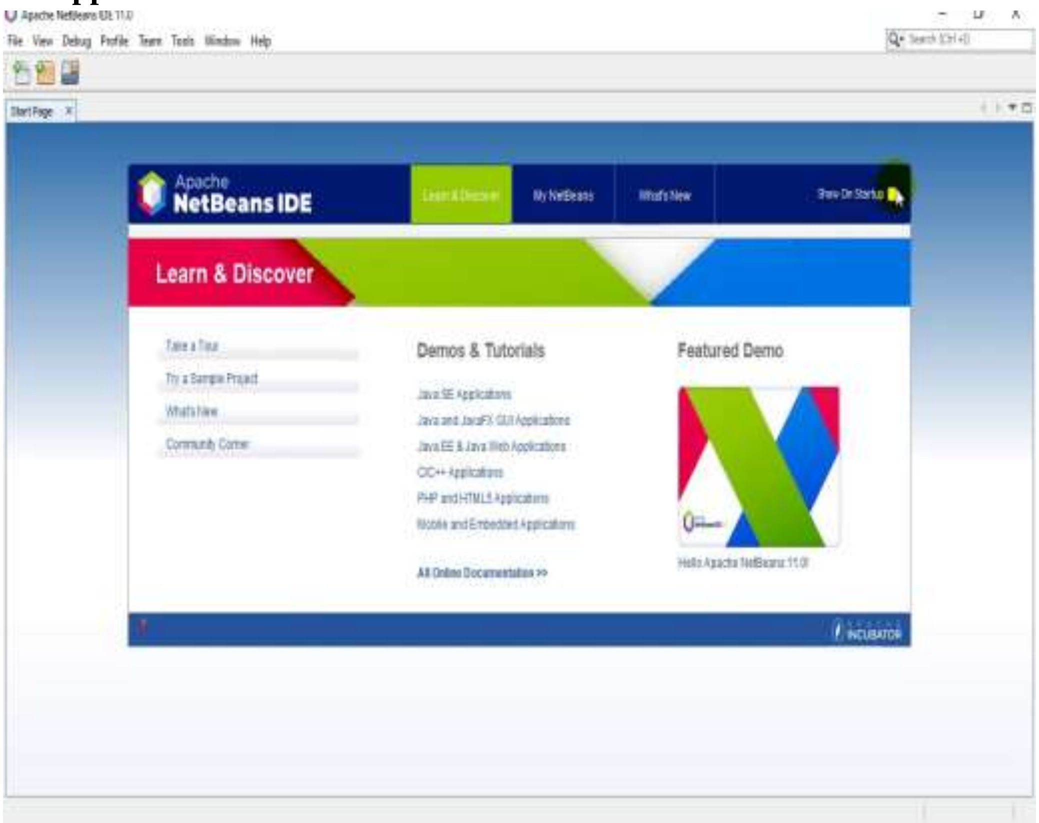
NetBeans IDE 8.0.2 Information:

NetBeans IDE 8.0.2 provides out-of-the-box code analyzers and editors for working with the latest Java 8 technologies--Java SE 8, Java SE Embedded 8, and Java ME Embedded 8. The IDE also has a range of new enhancements that further improve its support for Maven and Java EE with PrimeFaces; new tools for HTML5, in particular for AngularJS; and improvements to PHP and C/C++ support.

NetBeans IDE 8.0.2 is available in English, Brazilian Portuguese, Japanese, Russian, and Simplified Chinese.

The latest available download is NetBeans IDE 8.0.2, which is an update to NetBeans IDE 8.0 and contains:

- **Bug fixes in the installer for OS X 10.9.5 and 10.10**
- **Bug fixes included in** Patches 1, 1.1, 2 for NetBeans IDE 8.0 **and** Patches 1.1, 2 for NetBeans IDE 8.0.1
- **GlassFish 4.1 and Tomcat 8.0.15 bundled with the IDE**
- **Support for WildFly Server and WebLogic Server 12.1.3**
- **Added support for RequireJS**
- **Grunt tasks available in the popup menu for web projects**
- **Support for debugging JavaScript files with Karma**
- **Node.JS and Bower modules can be installed directly within the IDE**
- **Improved Git support**



6. RESULTS:

ORIGNAL IMAGE: (BEFORE ENCRYPTING)

Mobile Ad Hoc Network
www.educba.com

ENCRYPTED IMAGE: (AFTER ENCRYPTION)

The image part with relationship ID rId18 was not found in the file.

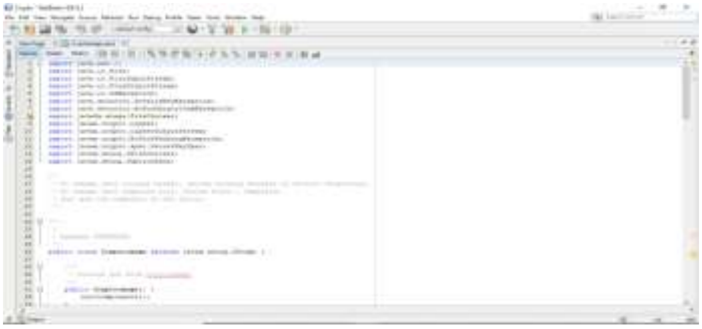
DECRYPTED IMAGE: (AFTER DECRYPTION)

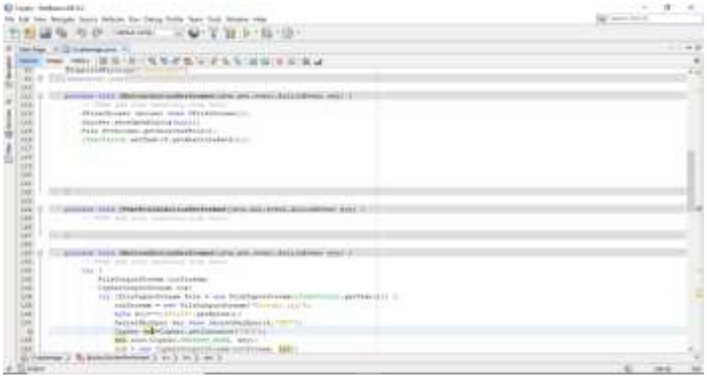
Mobile Ad Hoc Network
www.educba.com

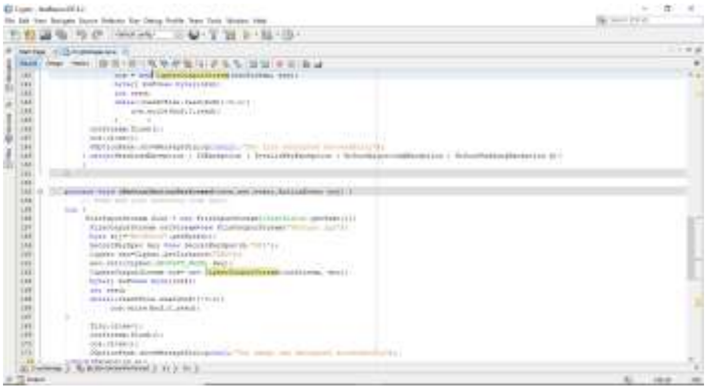
7. CONCLUSION

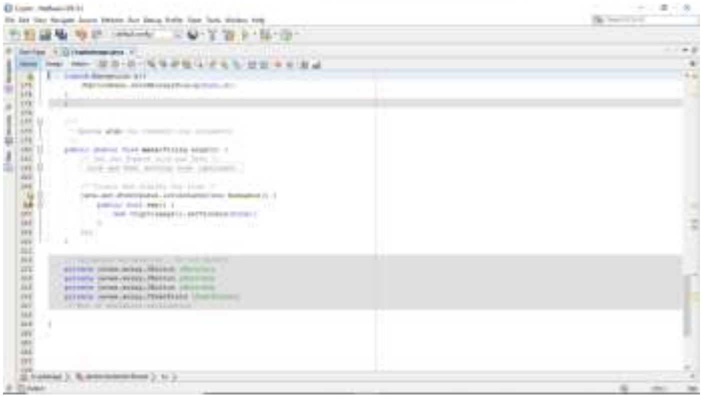
Colour image encryption and decryption is done by using DES algorithm, by providing required security for image between two authorized users or clients. In our project DES guarantee the unbreakable security for colour image. In the project image encryption is done using DES algorithm, Experimental consequences of proposed DES algorithm is very motivating? The implementation approach shows the encrypted and decrypted image and also historical analysis is done with enhanced techniques. Future work of our project is based on enhancing T-DES security level by implementing DES technique, by repeating three times of DES key to generate three sets of key for TDES algorithm for make T-DES algorithm more secure. Another future plan is of applying this proposed DES method for encrypting the video file to providing secure transmission in communication channels.

APPENDIX









REFERENCS

1 Shakshuki, et al. “EAACK - A Secure Intrusion Detection System for MANETs”, IEEE Trans.,2013, Vol. 60, No. 3, pp.1089-1098. https://doi.org/10.1109/TIE.2012.2196010

2 Prabu, K. and Subramani, A. “Energy efficient routing in MANET through edge node selection using ESPR algorithm”, Int. J. Mobile Network Design and Innovation, 2014, Vol. 5, No. 3, pp.166–175. https://doi.org/10.1504/IJMNDI.2014.065747

3 Thamizhmaran, R. Santosh Kumar Mahto, and V. Sanjesh Kumar Tripathi, "Performance Analysis of Secure Routing Protocols in MANET," International Journal of Advanced Research in Computer and Communication Engineering, vol. 1, no. 9, pp. 651-654, November 2012.

4 Venkanna and Leela Velusamy, “TEA-CBRP: Distributed cluster head election in MANET by using AHP”, peer-to-peer Network Application, Vol. 9, 2016, pp. 159-170. https://doi.org/10.1007/s12083-014-0320-0

5 K.Thamizhmaran., M. Anitha and Alamelunachippan “Performance Analysis of On-demand Routing Protocol for MANET Using EA3ACK Algorithm”, International Journal of Mobile Network Design and Innovation, Vol. 7, No. 2, pp. 88-100, 2017. https://doi.org/10.1504/IJMNDI.2017.085743

6 K. Thamizhmaran, M. Anitha and Alamelunachippan “Reduced End-To-End Delay for Manets using SHSP-EA3ACK Algorithm”, I-Manager Journal on Communication Engineering and Systems, Vol. 7, No. 3, pp. 9-15, 2018. https://doi.org/10.26634/jcs.7.3.14309

7 Thamizhmaran Krishnamoorthy, Akshaya Devi Arivazhagan, "Energy Efficient Routing Protocol with Ad hoc On-demand Distance Vector for MANET", IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) 2015.

8 Akshaya Devi Arivazhagan, et.al “Co-operative analysis of Proactive and Reactive Protocols Using Dijkstra's Algorithm” IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) 2015.

9 Vennila, K., and K. Thamizhmaran. 2017. Implementation of multilevel thresholding on image using firefly algorithm. International Journal of Advanced Research in Computer Science 8 (3):373–78

10 Akshayadevi Arivazhagan, et.al (2015) “Performance Comparison of on Demand Routing Protocols under Back whole For MANET”, Advance Research in Computer science and software Engineering, Vol. 5, No. 3, pp. 407 – 411.

11 K. Thamizhmaran (2016) “Performance Evaluation of EA3ACK in different topology’s Using EAACK for MANET, I - Manager Journal of information technology , Vol. 5, No. 4, pp. 5-10.

12 K.Thamizhmaran, M.Anitha and Alamelunachippan (2017) “Comparison and Parameter Adjustment of Topology Based (S-EA3ACK) for MANETs”, International Journal of Control Theory and Application, Vol. 10, No. 30, pp. 423-436.