Image Encryption and Decryption for Secure Internet

Prof. S.R.Dhavle[1] Shubhangi.P.Kale[2] Parwati.C.Kore[3] Ashwini.S.Nakod[4] Almas.S.Navidgi[5]
[1]Assistant Professor [2,3,4,5]Student
[1,2,3,4,5]BMIT, Solapur, India

Abstract— In today's era ubiquitous computing is worldwide adopted. Internet is the main root for providing a ubiquitous network for communication between different people across the world, such communications can be through a wireless channel or wired channel that helps in getting messages or confidential information exchanged between different groups of people. Data security is of utmost importance because of wireless communications on insecure network. So the concept of cryptography is emerged which is nothing but known as an art of writing a secret code and it provide diverse set of services for protecting data over network such as authentication, confidentiality, non-repudiation and integrity. Cryptography offers wide range of algorithms which can help to guard communications over an insecure network such as symmetric encryption techniques which uses one key for encryption and decryption. For a symmetric cipher security can be compromised as it uses a single key, with this an advantage comes out while using an asymmetric security technique that makes use of a pair of keys to secure communications over unsafe channels. In this paper the positive characteristics of both the techniques discussed above are taken and a hybrid approach is used to guard messages on timid wireless medium. AES which is known as symmetric algorithm is combined with ECDH algorithm that is asymmetric by nature and is an amalgam of ECC and Diffie-Hellman – anonymous key agreement protocol. Different text files are taken as input to the model with varying sizes. Encryption and decryption is performed using Advance encryption standard (AES) whereas ECDH will help in securing the communication for a session set up between client and server by generating key for AES. Also Diffie-Hellman will provide security by establishing a shared secret between client and server after successful key agreement. At last analysis of proposed model is done on the basis of different metrics like storage, encryption time, decryption time, correlation and avalanche effect. Proposed approach has been proven effective in reducing the gaps discovered in the present literature.

Key words: Image Encryption & Decryption, Secure Internet

I. Introduction

In present era the requirement of internet for wireless communication is rising day by day and thus there is a need of security to guard such communication by users on insecure wireless channel. Data sent over the communication channels is susceptible to attacks because of sensitive information it contain. To defend the data from external threat the concept of Cryptography is emerged. Cryptography is defined as "An art of writing a secret code" Methodology of writing such code is cipher and text is converted into cipher text which is commonly called Encryption whereas the reverse practice of converting a cipher text into normal text is known as Decryption. Cryptography can be categorized as classical and modern, classical cryptography techniques were used to foil eavesdropping and message interception problems whereas the modern cryptography techniques are more secure and used for high speed communications. Modern cryptography techniques are more secure than the classical ones and are widely used such as DES, 3DES, AES, ECC, ECDH, RSA etc. Figure 1 represents the terminology of encryption and decryption process.

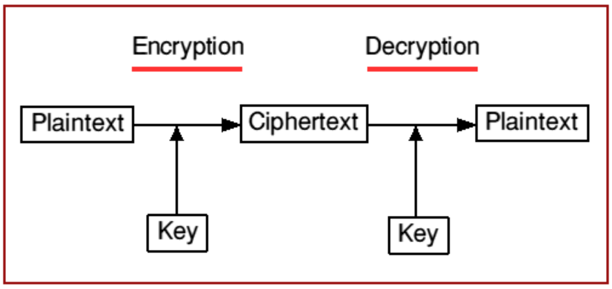


Figure 1. Encryption/Decryption Terminology

- Plain Text: Original text which user uses for the communication purpose is termed as plain Text. For example bob sends "how are you" to Alice here the plain text is "how are you".
- Cipher Text: Plain text is transformed into a message (cipher text) which cannot be interpret by third party out of communication.
- Example: "bye" is converted into "#@a%". Encryption: Encryption is a procedure of transforming the plain text into the cipher text which is in non-readable form.
- Decryption: Decryption is a procedure of transforming the encrypted text back into the plain text. Cryptography must ensure four basic data protection requirements which are authentication, privacy, integrity and non – repudiation. We can define these requirements as:
- Authentication -Where we have to verify user's identity involved in communication.
- Privacy - To ensure no third person can intercept the message.
- Integrity - Ensures that original message and received are identical i.e. no alteration of data. Non-repudiation- Here we need to verify the sender's identity.

II. Work Carried Out

- Key Selection: The sender and receiver agree upon a 128 bit key. This key is used for encryption and decryption of images. It is a symmetric key encryption technique, so they must share this key in a secure manner. The key is represented as blocks k[0],k[1]...k[15]. Where each block 8bits is long (8*16=128 bits).
- Generation of Multiple keys: The sender and receiver can now independently generate the keys required for the process using the above explained Modified AES Key Expansion technique. This is a one time process; these expanded keys can be used for future communications any number of times till they change their initial key value.

- Encryption: Encryption is done in spans, where we process 16 pixels in each span. For both its Cipher and Inverse Cipher, the AES algorithm uses a round function that is composed of four different, byte oriented transformations: SubBytes, ShiftRows, MixClumns and AddRoundKey.
- Decryption: The decryption process is similar as encryption, but we use Inverse SubByte Transformation.

III. IMPLEMENTATION DETAIL WITH PROCEDURE, CODING SAMPLE, OUTPUT:

A. Encryption algorithm:

The implementation of the AES-128 encryption and decryption algorithm with the help of MATLAB software is done. In which the input is an image and the key in hexadecimal format and the output is the same as that of input image. For encryption process first, dividing image and making it 4*4 byte state i.e. matrix format. Calculate the number of rounds based on the key Size and expand the key using our key schedule. And there are (n-1) rounds performed which are substitute byte, shift rows, mix columns and add round key. The final round “n” does not consist of mix column in the iteration.

B. Decryption algorithm:

The AES decryption process is the revers process that of the encryption process. The above figure shows flow of the AES decryption algorithm. Which consist of cipher text as the input, the key is same for decryption process which for encryption. In case of decryption the inverse substitute byte, inverse shift rows and the inverse mix columns are to be implemented. While the add round key remains the same

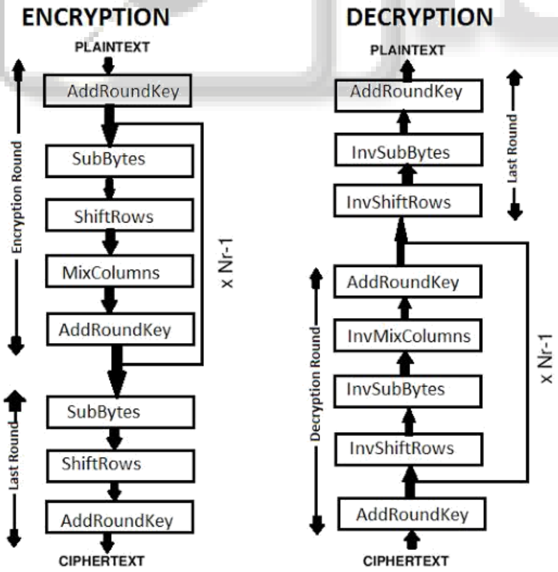
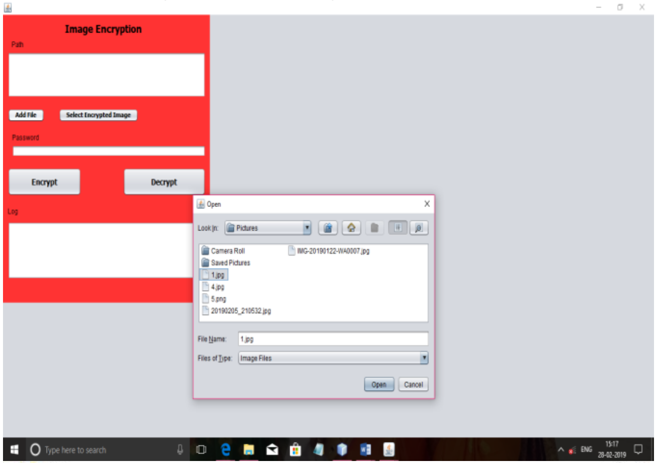
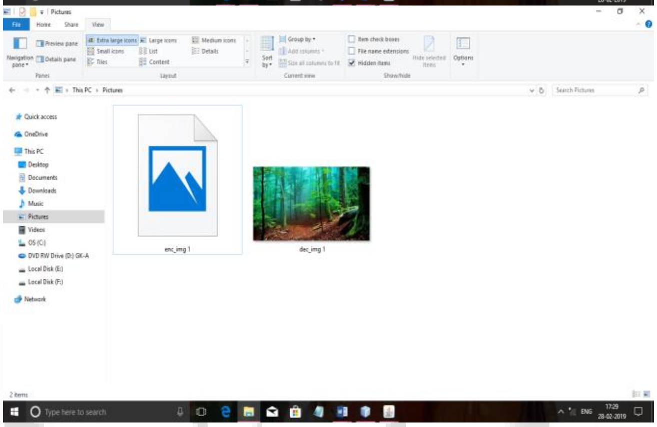


Fig: Algorithm image encryption and decryption

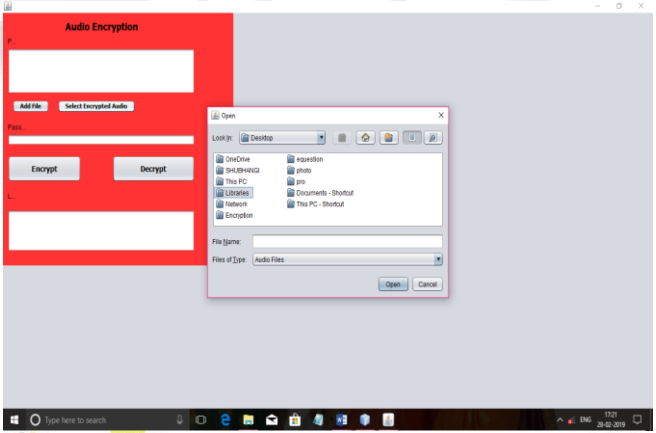
C. Snapshots and Output:

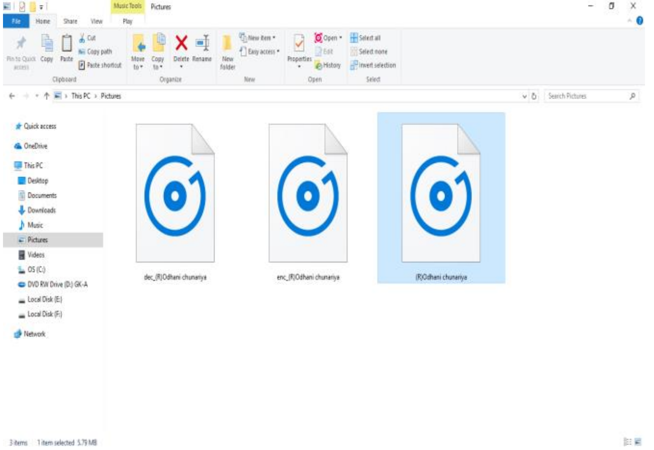
1) Image encryption and decryption:



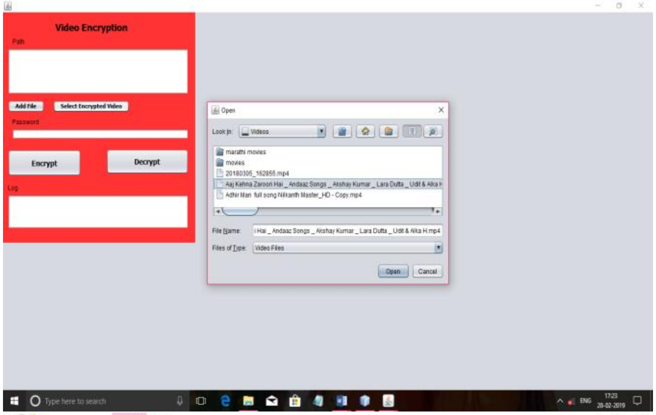


2) Audio encryption and decryption:





3) *Video encryption and decryption:*

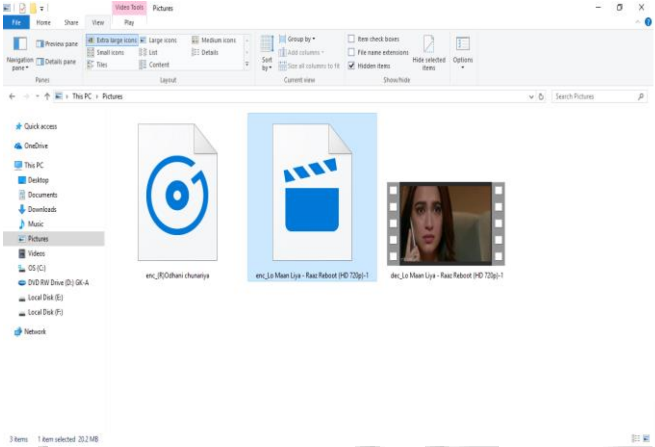


Look in: Videos

- marathi movies
- movies
- 20180305_162855.mp4
- Aaj Kehna Zaroori Hai _ Andaaz Songs _ Akshay Kumar _ Lara Dutta _ Udit & Alka H
- Adhir Man full song Nilkanth Master_HD - Copy.mp4

File Name: i Hai _ Andaaz Songs _ Akshay Kumar _ Lara Dutta _ Udit & Alka H.mp4

Files of Type: Video Files



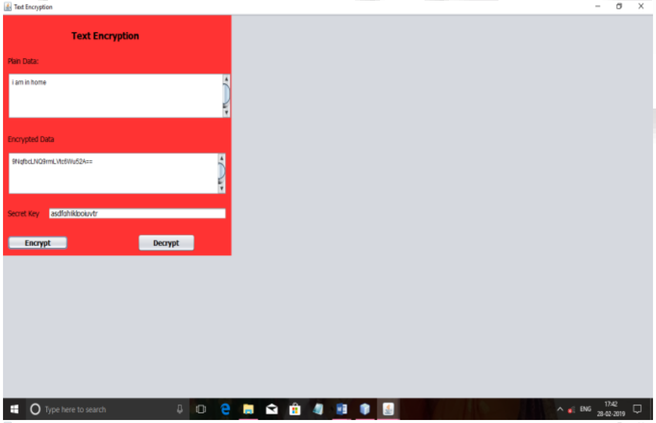
enc_(R)Odhani chunariya

enc_Lo Maan Liya - Raaz Reboot (HD 720p)-1

dec_Lo Maan Liya - Raaz Reboot (HD 720p)-1

3 items 1 item selected 20.2 MB

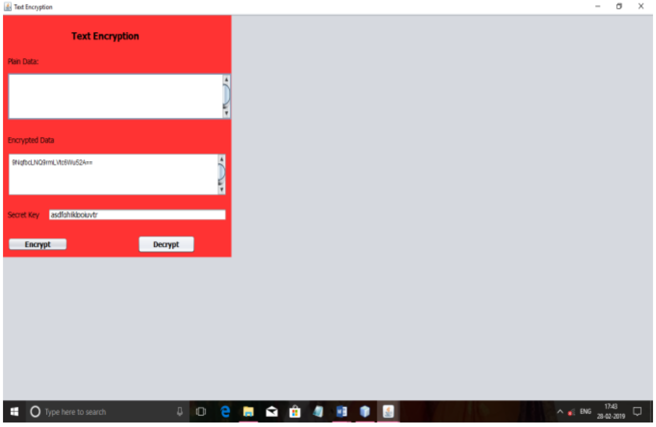
4) *Text encryption and decryption:*



Plain Data: i am in home

Encrypted Data: 9NqfbcLNQ9rmLVfc6WuS2A==

Secret Key: asdfohiklboiuvtr



Plain Data:

Encrypted Data: 9NqfbcLNQ9rmLVfc6WuS2A==

Secret Key: asdfohiklboiuvtr

IV. RESULT

The original input image given to the algorithm is of JPG. The unreadable image is the encrypted image and by applying the decryption algorithm the original image is obtained in JPG format. In this paper, For Encryption and the decryption the same key is used. The key is in hexadecimal form and length of key is 16bit.

V. SCOPE AND OBJECTIVES

To create a tool that can be used to hide data inside image. The tool should be easy to use, and should use a graphical user interface.

The tool should work cross platform. The tool should effectively hide a message using an image degradation approach, and should be able to retrieve this message afterwards. The tool should take into account the original content, to theoretically more effectively hide the message. The technique should fail under the category of secret key steganography where without the key the hidden message cannot be retrieved. The tool should be able to encrypt the message before embedding it.

The idea of this project is to develop and Image encryption and decryption the project scope based on Netbeans IDE8.2 Java, 2D^{TM} API. All of the scope help as below:

1) Net beans IDE8.2
   This application enable to edit any java code that is relevant for the project.
2) Java 2D^{TM} API
   This API is imported to the source code and enable action such as reading/loading, drawing, creating and Writing/saving an image.

VI. PROPOSED WORK

In Proposed model AES and ECDH are used for text file encryption. Input text fissle is transformed into encrypted form using AES algorithm with key generated by ECC and different-Hellman will help in generating a shared secret which is then combined with ECC key and uploaded to the server. After successful key agreement client would be able to decrypt. The above methodology is implemented in JAVA 8 using Eclipse an open source platform that allows a developer to create a customized development environment (IDE). The above experiment is conducted on different text files with different sizes (KB), evaluation is done on the basis of different parameters like correlation, Avalanche effect, storage, encryption time and decryption time. Given below Figure 3 illustrate the complete process of AESECDH Encryption and Decryption.

VII. Architecture

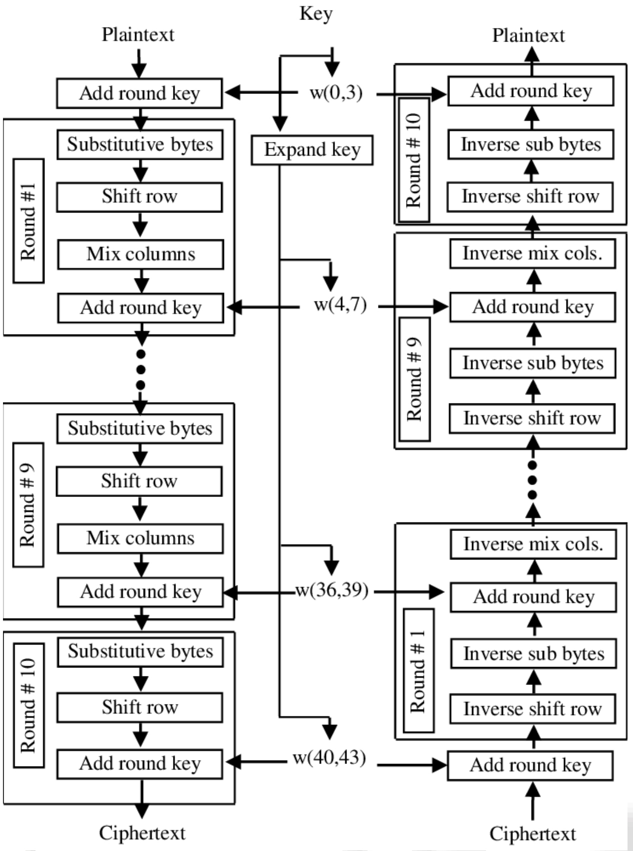


Fig: Architecture of encryption and decryption

Above figure 1 shows architecture of proposed system which consist of following three components:

AES is announced as a federal information Processing standard by NIST (National institutes of standards and technology) in 2001. AES is recurrently used encryption technique due to its high security, efficiency and simplicity. It uses the same key for both encryption and decryption process and known as symmetric block cipher. It uses three block ciphers AES-192, AES-128, AES-256. There are different rounds of processing according to the block size such as 10 rounds for 128- bit key, 12 rounds for 192-bit key and 14 rounds for 256-bit key. Different steps for encrypting data with AES are given below:

- Key Expansion- Rinjndael's Key Schedule is used to calculate the round key using the cipher key.
- Initial Round- Add round key: Bitwise XOR operation is used to combine each byte of the state with the derived round key.

A. Different Rounds of Processing

- Sub Bytes: every Byte is replaced with another using the lookup table, a non linear kind of substitution.
- Shift rows: This is called transposition step where each row will by cyclically shifted to number of times required.
- Mix columns: four Bytes of each column are combined in a state matrix.

Final Round,
Sub Bytes
Shift Rows
Add Round Key

So, the final round will not have mixing of columns. During Decryption the processing rounds will be same but the only difference is Inverse of every processing round will be executed. If in encryption we have sub bytes then in decryption it will be Inverse sub bytes. Similarly for shift rows and mix columns in encryption there will be Inverse shift rows and inverse mix columns for decryption.

VIII. Conclusion

Data security is to safeguard the information which is getting exchanged between two parties communicating over an insecure network. Cryptography provides wide range of algorithms to protect such communications so that information can be transmitted securely over the wireless medium and provide authentication, data integrity, privacy and non-repudiation. This paper propose a hybrid model combining the characteristics of AES algorithm which is a symmetric technique and ECDH which is widely known as asymmetric technique to guard the communication from external threat. Different text files of different sizes are taken as input; the key for encryption is generated with the help of elliptic curve cryptography while encryption and decryption is performed with the help of Advanced Encryption Standard (AES).

Acknowledgement

We would like to thank our guide Prof.S.R.Dhavale, Assistant Professor at Dept. of CSE, BMIT Solapur, for his guidance and support. We also thanks full to our project co-coordinator Prof.Dodmise.U.S for her valuable support. We will forever remain grateful for the constant support and guidance extended by guide as well as project coordinator, for the completion of paper.

References

[1] Java Cryptography Architecture Standard Algorithm Name Documentation for JDK 8:

[2] https://docs.oracle.com/javase/8/docs/technotes/guides/security/StandardNames.html

[3] Java Cryptography Architecture (JCA) Reference:

[4] https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html

[5] RFC 2898 : Password-Based Cryptography Specification version 2.0

[6] About AES – Advanced Encryption Standard, Copyright 2007 Svante Seleborg Axantum Software AB.

[7] Cryptography And Network Security: Principles And Practices, 4Th Ed.