International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Encryption using AES, RSA and Stegnography

Harini G

Dr MGR Educational and Research Institute, Maduravoyal, Chennai – 600095, Tamil Nadu, India

ABSTRACT

The image encryption based on AES, RSA Algorithm andSteganography was used for ensuring more security over Triple DES.The AES algorithm is a symmetrical block cipher algorithm that takesplain text in blocks of 128 bits and converts them to cipher text usingkeys of 128, 192, and 256 bits. Under RSA encryption, messages areencrypted with a code called a public key, which can be sharedopenly, once a message has been encrypted with the public key, it canonly be decrypted by another key, known as the private key.pyCapsulating allows you to encrypt your data (text or a file),using AES encryption and then to encode it/hide it to an PNG imageusing an steganography algorithm and also we add an RSAEncryption to secure the data.

Keywords: RSA Algorithm, AES Algorithm, Asymmetric Encryption and Stegnography

1. Introduction

pyCapsulating is an image encryption process based on AES, RSA algorithms and Steganography techniques. Advanced Encryption Standard (AES) which is adopted by the U.S. government in 2001, is now used in the Wifi security, compression tools. This algorithm has been developed by two Belgian researchers, Joan Daemen and Vincent Rijmen to replace the DES and the 3DES algorithms. The AES algorithm is easy to implement, it consumes less memory and it uses keys of 128, 192 or 256 bits. Asymmetric systems such as RSA requires the use of large numbers. This branch of cryptography has of major interest, it removes problem of transfer of the key. But it cannot grab the place of symmetric encryption algorithm because its computation time is comparatively long. For a large amount of data such as image, it is not preferable to use asymmetric encryption. The Asymmetric (public) key cryptosystem, it uses the same algorithm for encryption and decryption with a pair of keys, public and private, computationally is impossible to derive the private key from the public key.

1.1. Literature Survey

According to Sheeja.R(2020) the Triple DES image encryption project contains a major drawbacks as the main disadvantage to DES is that it is broken using brute-force search. However, using 3DES mitigates this issue at the cost of increasing execution time. DES is also vulnerable to attacks using linear cryptanalysis.

According to S. Karthik, A. Muruganandam (2014) Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System contains a drawback as the 56 bit key size is the biggest defect of DES. DES was not designed for software and hence runs relatively slowly. In a new technology it is improving a lot of possibility to break the encrypted code, so AES is preferred than DES.

1.2. Proposed System

In this project we propose a method based on AES, RSA and Steganography technique. We encrypt the image using AES with the password to make the process more secure we use RSA algorithm to generate key and encrypt image or file using Steganography technique. Presented approach is more efficient in terms of computation cost compared with schemes that use asymmetric encryption. We believe that projected approach is more secure due the strength of RSA, AES and Steganography methods.

Asymmetric encryption is inappropriate for images because the computation time is long, but it is more secure than symmetric encryption because it removes the exchange of the secret key, also it is mathematically infeasible to know the private key from the public key. The speed of symmetric encryption is better than asymmetric encryption but less secure since it requires secret key sharing. To take advantage of the speed of symmetric encryption and security of asymmetric encryption and steganographic methods. We propose an algorithm which combines AES, RSA with steganographymethod. First of all we encrypt the plaintext image or file using AES and a password is assigned for encrypting purpose. Then to make it more secure we can include RSA if desired once the dialog is chosen it generates the public and private key which is the downloaded in the desired location which is used for the further decryption purpose. The proposed approach eliminates sharing key during the encryption process.

Initially, we have encrypted the original image using a symmetric algorithm. In our case we have used advance encryption standard (AES).Then, the AES is assigned a password for encryption and then an asymmetrical RSA algorithm is generated if needed to enhance more security to the data. In propose scheme we have encrypted the plain image using AES and is enciphered by RSA asymmetric algorithm. The strength of our technique is based on the plus points of RSA and AES.

1.3. Module Description

Encryption:
In this module we have libraries which are used to embedded the process of encryption and decryption using AES algorithms with steganographic techniques and also generate RSA Keys.

pyCapsulatingCli:
In this module we import path validator to validate the path the file path for the images to be encrypted and decrypted with User Input.

pyCapsulatingGUI:
In this module we build the GUI by embedding the encryption module and pyCapsulating module which results in the encryption of the image of any file path and also with decryption process using RSA.

1.4. Workflow

The workflow of this project is going to be based on Stegnographic implementations on the text content or the file content embedded with AES algorithm and if required by the user they can access the RSA algorithm for more secured way of encrypting the data.

The user is required to choose the operation type whether it is going to be encryption or decryption and then they are supposed to choose input type either file or text And then the user is supposed to choose the image path of the file which is to encrypted and to choose the target path in which the file is going to be processed with the stegnographic implementations.

The user can also include the RSA support where the RSA algorithm is supposed to encrypt the file and generate a public key as well as a private key and the public key is shared with the other user to whom the encrypted file is transferred and then it is used in decrypting the file.

These three algorithms are embedded together and then are processed with the target file to encrypt the chosen folders and is forwarded to the other user and accessed with the public key used in the process of encrypting the file using RSA Algorithm.

REFERENCES

"Overview: Main Fundamentals for Steganography" by Zaidoon kh.AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi Journal of computing, Volume 2,Issue 3,March 2010 ISSN 2151-9617.

Advanced Steganography Algorithm using encrypted secret message, by Joyshree Nath and Asoke Nath, International Journal of Advanced Computer Science and Application (IJACSA) Vol-2 No.3, Page 19-24, March 2011.

"Image Security using Encryption based Algorithm" Ratinder Kaur, V.K. Banga International Conference on Trends in Electrical, Electronics and Power Engineering (ICTEEP 2012)July 15-16,2012 Singapore.

Cryptography: current status and future trends, by S.B. Sadkhan, in: Proceedings of IEEE International Conference on Information & Communication Technologies: From Theory to Applications, Damascus. Syria, April 19–23, 2004, pp. 417–418.