PSYCHOLOGY AND EDUCATION (2021) 58(4): 2424-2428
Article Received: 08th October, 2020; Article Revised: 15th February, 2021; Article Accepted: 20th March, 2021

Data Security Using Cryptography & Steganography

Apoorv Jain [1], Ritesh Aggrawal[2], Akshat Kumar[3], Dr B Balamurugan[4]
[1,2,3,4]Galgotias University , Greater Noida
[1]apoorv127@gmail.com , [2]goyalsunita55@gmail.com , [3]akshatkumar0204@gmail.com ,
[4]bbalamurugan@galgotiasuniversity.edu.in

ABSTRACT

Steganography and cryptography are two ways from which we can hide data from third party users. There are numerous cryptography strategies accessible (DES, AES, Blowfish); among them AES is quite possibly the most remarkable procedure. In Steganography we have different methods to conceal the message. In this task we are building up a framework where we build up another procedure in which Cryptography and Steganography are utilized as coordinated parts to give greater security. It is a client server based image steganography in which if a user wants to hide text inside an image , the user first establishes connection between client and server via OTP generated to successfully connect. Then the user can embed that text file in the image . If a user wants to extract the text file then dembed the embed image

Keywords
Cryptography, Steganography, Encryption, Decryption, Embedded, De-embedded, AES, DES and Blowfish

Article Received: 10 August 2020, Revised: 25 October 2020, Accepted: 18 November 2020

Introduction

[1] **Cryptography** is the preparation and examination of systems for secure correspondence. It is ordinarily insinuated as "examination of secret". It is for the most part used in various fields nowadays, for instance, data mystery, data uprightness and approval. Flow cryptography exists at the intersection purpose of the controls of math, computer programming and electrical planning. Area where cryptography consolidate cards i.e Debit or Credit Card, PC credentials, and online business.
During WWI the Germans used a special kind of crypto device known as the **ENIGMA** which almost won the war for them until a turnaround occurred when the then famous maths
professor **Alan Turing** of U.S. (Inventor of the famous Turing Machine) helped the U.S. military force to break the encrypted codes used by the Germans secretly without the knowledge of the Germans & helped U.S. to win the war eventually. It also plays an important role in piracy of digital media.

Algorithms

1. Data Encryption Standard

DES is a calculation that takes a fixed-length line of plaintext bits and changes it through a progression of convoluted activities into another ciphertext bitstring of a similar length. It was created in the mid 1970s at IBM and dependent on a prior plan by Horst Fiestel, the calculation was submitted to the National authority of principles (NBS) following the office's encouragement to propose a possibility for the security of delicate, unclassified electronic govt. Information. The term of IBM engaged with figure configuration are Fiestel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas and Bryant Tuckerman. DES is currently viewed as uncertain for some applications due to it's extremely short key-size for example 56-cycle. In jan,1999 distributed.net and the electronic outskirts establishment teamed up to openly break a DES key in 22 hrs and 15 minutes. Continuously, it was supplanted by the further developed triple DES, AES and Blowfish.

2. Advanced Encryption Standard

[2] AES additionally referred to as Rijndael, is a detail for the encryption of electronic information set up by the NIST in 2001. It is a successor of Data Encryption Standard (DES) and is stronger and faster than DES. It is a symmetric key symmetric block cipher. It was grown at first by two Belgian researchers Joan Daeman and Vincent Rijmmen. AES depends on a plan guideline known as a replacement Permutation organization, mix of both replacement and stage, and is quick in both programming and equipment. In contrast to DES, it utilizes a square size of 128 pieces, and a vital size i.e. 256, 192 or 128 pieces. It works on a segment of 4x4 request lattice of bytes.

The number of cycles of repetition is as follows:

- For 128-bit requires 10 cycles of repetition.
- For 192-bit requires 10 cycles of repetition.
- For 256-bit requires 10 cycles of repetition.

For every round involves four stages i.e. Key Expansions, Rounds, Initial Round and Final Round.

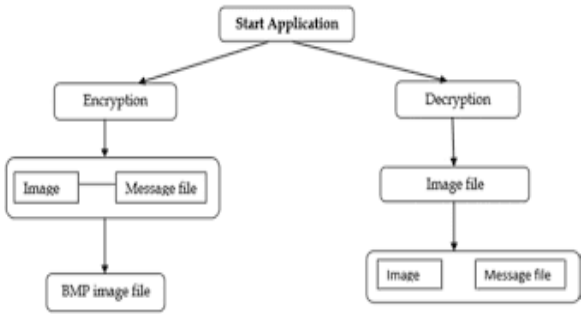
3. Blowfish

Blowfish provides a good encryption rate in software & it's better as compared to DES but one of the three AES is still considered the best. It was designed by Schneier as an alternative to DES. It has a 64-bit block size and a variable key length from 32 upto 448 pieces. The most energizing element of this calculation is the utilization of s-boxes and an exceptionally mind boggling key timetable. Every one of

the three are acceptable in their own specific manners yet the most secure out of the three is AES.

4. Steganography

[3] Steganography includes concealing data so it creates the impression that no data is covered up by any stretch of the imagination. On the off chance that an individual or people sees the item that the data is covered up within the person will have no clue about that there is any concealed data, along these lines the individual won't endeavor to unscramble the data. What steganography basically does is abuse human insight, human faculties are not prepared to search for documents that have data within them, albeit this product is accessible that can do what is called Steganography. The most well-known utilization of steganography is to conceal a document inside another record.



Proposed System

In this project, the algorithms used for cryptography are DES, AES and Blowfish. The main function of these algorithms are to convert plain text using symmetric key into cipher text and vice versa using same symmetric key.
In Steganography, it is a client server based in which if a user wants to hide text inside an image , the user first establishes connection between client and server via OTP generated to successfully connect. Then the user can embed that text file in the image. If a user wants to extract the text file then dembed the embed image when receiver enter same OTP again.

Literature Survey

[4] "DES, AES and Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis."
This Research paper describes the performance analysis of the 3 algorithms DES, AES & Blowfish in symmetric key cryptography. This paper was submitted by **Jawahar Thakur & Nagesh Kumar** in the international journal of emerging technology & advanced technology. (volume 1,issue 2,dec.2011).

Objective

The goal of the paper is to give an exhibition examination between symmetric key cryptography calculations: DES, AES and Blowfish. The investigation has been directed by running a few encryption settings to handle various sizes of information squares to assess the calculation's speed for encryption and unscrambling.

Methodology

A. Simulation and Settings

The recreation utilizes the given classes in java climate to reenact the presentation of DES, AES and Blowfish. The usage utilizes oversaw coverings for DES, AES and Blowfish accessible in java.crypto and java.security that wraps unmanaged executions accessible in JCE and JCA. The Cipher class gives the usefulness of a cryptographic code utilized for encryption and unscrambling. It shapes the center of the JCE system.
The assessment is intended to assess the outcomes by utilizing block figures. Consequently, the heap information is isolated into more modest square size according to calculation settings.

B. System Parameters

The analyses are led utilizing an AMD Sempron processor with 2GB of RAM. The recreation program is incorporated utilizing the default settings in jdk 1.7 advancement pack for JAVA. The investigations will be played a few times to guarantee that the outcomes are steady and are legitimate to analyze the various calculations.

Conclusion

The presented recreation results exhibited that Blowfish has an ideal introduction over other customary encryption counts used. Since Blowfish has no known security frail concentration as of not long ago, this makes it a bewildering probability termed as encryption figuring. AES exhibited dreary showing results stood out from various counts since it requires truly taking care of force. In future this examination can be realized in a better test framework by considering frameworks organization than showing which estimation performs better in association.

Problem Description

- **Existing Problem**

The problem that exists is that we are not sure about the security of our data while it is transmitted online. suspicion is a very dangerous thing. Doubts like may be my data is hacked somewhere in the middle before reaching its destination, or it may get hacked. So, such doubts can creep into the minds of the sender who sends the message. So, the data sent by a user needs to get secured. For that we are proposing a solution using cryptography & steganography which when integrated can provide a solid double-layer protection to the original data. Now using such techniques we face some problems which are listed below.

- **Using DES Approach**

DES is a very good method of encrypting user's data. But, every new invention in the field of science brings its shortcomings, so is the curious case of DES. DES can encrypt the original data but the main problem which arises with such kinds of algorithms are they use a single key or a shared key for both sender & receiver, so if the key is not large enough it will get cracked by **Brute force attack**. It means trying every possible turn of the key. It means trying every possibility of the key. The key length determines the quantity of possible keys. As DES defines a key length of just 56 bits so it's very easy for someone to check all the permutations & combinations & eventually find the right key to crack the code. So, this problem needs to be seriously taken into account & every measure should be taken to solve it.

- **Single layer of Security**

Encryption algorithms although removes the shortcomings of hiding the data or encrypting the data. But, then just as we call a minister needs a 5 layer security or vip security, similarly highly secret data needs more than a single layer of security. Is it enough to just encrypt the data & hope it will never get hacked or add one more security layer if possible safely first as people say so it also applies for highly secured data also.

Proposed Solutions

The proposed solution eliminates these two drawbacks as following:

- **AES & Blowfish**

AES & BLOWFISH are two algorithms which can be used to remove our basic problem i.e. security of the data & secondly they can also be used to remove the brute force attack problem faced by DES. DES have a very short key length(56 bits), so it will be easier for a hacker to just try out all the possibilities & get the correct key. But algorithms like Advanced Encryption Standards & Blowfish don't allow an intruder to have a variable length of key sizes. AES uses variable key sizes (i.e. 192, 128, 256 bits) whereas Blowfish can vary it's key length from 32-448 bits. So, both these algorithms make it very difficult for an intruder or an Hacker to hack or crack the key.

- **Steganography**

Here, comes the solution to our second proposed problem or what we can say fondly as the 'safety first' problem. Steganography provides a double-layer security to the original message or data so that it will become almost impossible for the intruder to even think that such a file can contain highly secret data, When steganography does is that it embeds the encrypted data or the encrypted message that has been encrypted by using one of the three algorithms DES, AES & Blowfish. It embeds the encrypted data or message inside an image file which will completely hide the fact that there is even a message hidden inside the image.

No one will even think that such a thing can happen that one can hide the data inside an image. So, this can provide a very high-level of security or what we can call layered security to highly secure data that needs to be protected.
So we are providing you with a solution that almost removes both your problems because we are integrating both cryptography & steganography into one system.

Results

When the software Netbeans is used for implementation of the project is executed the following occur.

- **Welcome Page**

Fig : Welcome Page

This is the first page of our implementation which just displays stegano-crypto, the basis of our project.

- **Login Page**

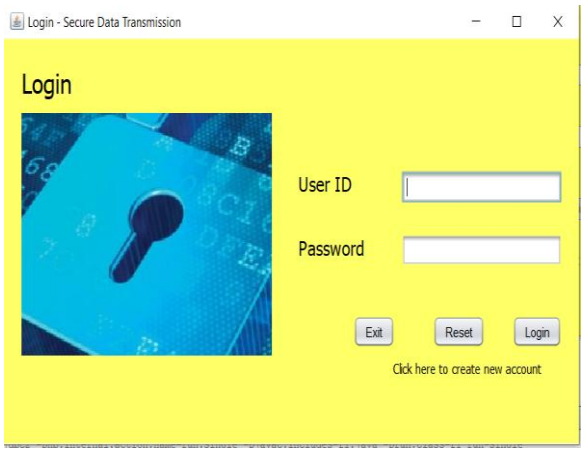


Fig : Login Page

This is the second page which shows the login page where you have to enter your User ID and Password to either login or make an account.
The user has to enter the password and the password which he has set during the time of making the project.
The user is new so there is an option for **Click here to create a new account** from which he/she has to register himself so that he/she can access this page.

The user has maintained the database of different users in the database server which in this project is Xampp Server.

- **Option Page**

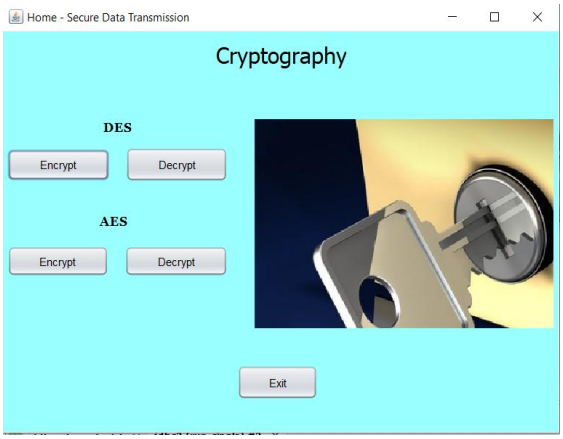


Fig : Option Page

This page appears after you login. This shows different options that are available for selection. They are Encryption, Decryption, Blowfish & Exit.

- **Encryption by DES**

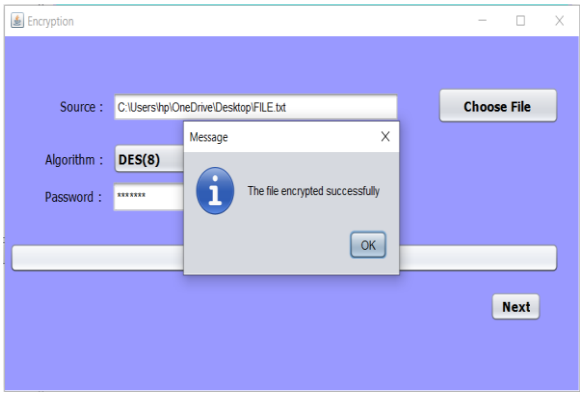


Fig : Encryption by DES

This page shows the encryption of the original message by DES algorithm.

- **Decryption by DES**

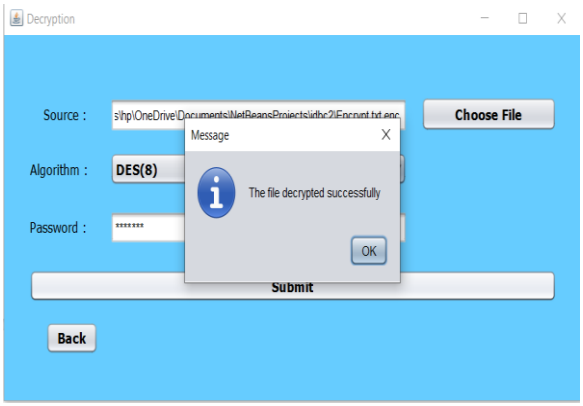


Fig : Decryption by DES

This algorithm shows the decryption of data by DES algorithm.

- **Encryption by AES**

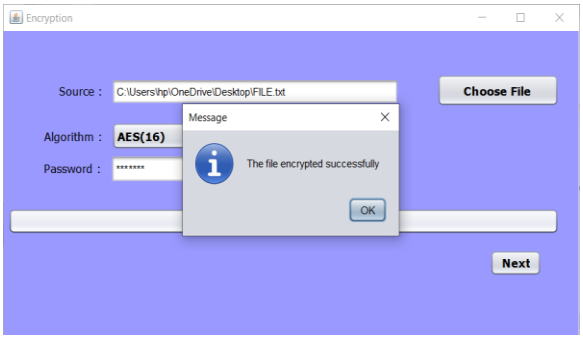


Fig : Encryption by AES

This page shows the encryption of the original message by AES algorithm.

- **Decryption by AES**

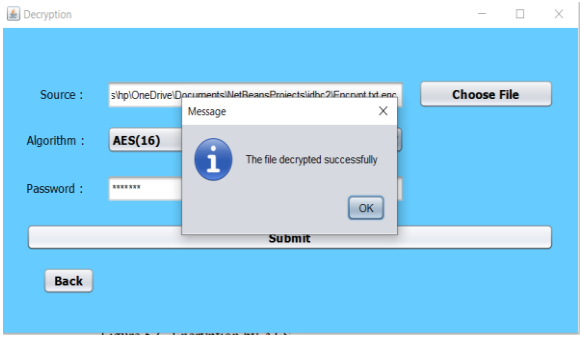


Fig : Decryption by AES

This algorithm shows the decryption of data by AES algorithm.

- **Encryption And Decryption By Blowfish**

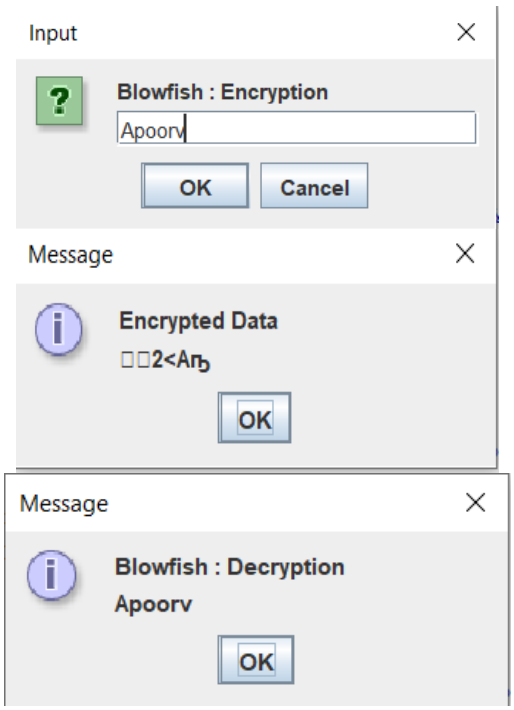


Fig : Encryption And Decryption By Blowfish

For encryption it will take an input along with a symmetric key (upto 448 bits) that input will convert into an encrypted data.
For decryption encrypted data will be converted into original data.

- **Embedding and De-embedding by Steganography**

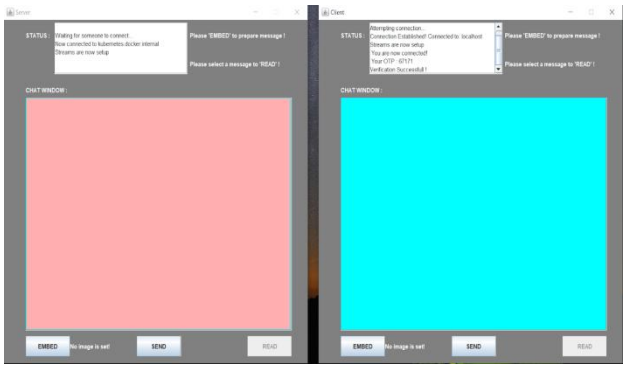


Fig: Embedding and De-embedding by Steganography

It is a client server based image steganography in which if a user wants to hide text inside an image , the user first establishes connection between client and server via OTP generated to successfully connect. Then the user can embed that text file in the image. If a user wants to extract the text file then dembed the embed image.
Embedding is a process in which we hide an encrypted text file inside an image so that it becomes almost invisible to other users that there is some data hiding inside the image. Everyone will just see that image but he will never doubt that is some text file hidden inside the image. So, in this way Embedding works.

Now, coming to the Dembedded part if the client wants to extract that text file first type an OTP then after he will extract the text file from the image.

Conclusion

So, our proposed system shows how we can protect our data or hide them by using methods of cryptography and steganography. Both of them are very useful techniques in securing data to a larger extent.
Each method or each technique have their own advantages & disadvantages but we have taken an initiative & shown that we are integrating both the methods i.e cryptography & steganography & can implement them together.
In this way we have tried to ensure the security of data by integrating both cryptography & steganography & as we all know there is always scope for improvement, so if possible we'll bring more improvements to our proposed project.

References

[1] Jawahar Thakur & Nagesh Kumar"DES, AES & Blowfish: Symmetric key cryptography, performance based analysis", International journal of emerging technology & advanced engineering, vol 1,issue 2, December 2011.

[2] Manoj gowtham.G.V1, Senthur.T2 , Sivasankaran.M3 , Vikram.M4 "AES based steganography" International Journal of Application or Innovation in Engineering & Management (IJAIEM).vol.2,issue 1,January 2013.

[3] Mr.Vikas Tyagi" Data Hiding in Image using least significant bit with cryptography" International Journal of Advanced Research in Computer Science and Software Engineering.vol.2,issue 4,April 2012.

[4] "DES, AES and Blowfish: Symmetric Key Cryptography Algorithm Simulation Based Performance Analysis."