JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

STUDY OF CRYPTOGRAPHY ALGORITHMS AND THERE IMPLEMENTATAION

[1]VEDANT SINGH, [2]SHUBHAM BHASIN, [3]ER.ANJANI KUMAR

[1]STUDENT, [2]STUDENT, [3]ASSISTANT PROFESSOR
[1]DEPARTMENT OF INFORMATION TECHNOLOGY,
[1]SHRI RAMSWAROOP MEMORIAL COLLEGE OF ENGINEERING AND MANAGEMENT(SRMCEM), LUCKNOW,UP, INDIA

Abstract : In Today's Technology-driven world, there is assertion of high data dependency. Data serves as a vital characteristics for accomplishment of standard goals for any existing entity. The growth of data dependency had caused an outcome of large data being produced and transferred. Digital media serves an essential role in distribution of data. With increasing data dependency, there is a higher possibility of severe data attacks and threats. This proclaims for establishment of data privacy and security issues, which needs to be resolved for protecting sensitive information. Protecting digital documents from manipulation, duplication, modification had become the need of an hour. To enhance data with security features, cryptography algorithms are implemented. This research paper consists of study of implementing cryptography algorithms for providing data security, integrity and confidentiality. Implementation of DES, AES algorithms at single platform and creating a secure environment for transmission of data have been a challenging model for researches.

***IndexTerms* – Data Encryption Standard, Advanced Encryption Standard, 3-DES, Encryption, Decryption**

I. INTRODUCTION

Cryptography is a mechanism of enriching our information with security features from unauthorized access. The general concept of cryptography states that information vanishes out from the sight of attackers during the time of information being transferred or stored. Extraction and conversion of data of any form such as text, image, video, audio, etc into an encrypted form (i.e unreadable and mysterious) during the time of transfer or retrieval is called Crucifixion.
With the ideology of cryptography, a secured environment is created for sharing, transfer and retrieval of information.
The objectives of Cryptography focuses on extant of providing data security, integrity, confidentiality and authentication.
In today's modern world, cryptography is no longer restricted to secure, preserve military information. Rather, it has broaden it's extent for maintaining security policy for any business venture or organization. The organization needs to have a secured environment for communication regarding assets, liabilities, etc. Thus, for establishment of successful business organization cryptography serves as an important attribute. Cryptography defines security policy set up of an organization leading to establishment of secured network for information security, electronic financial transaction, accessibility to resources, etc.
Ideology of cryptography is stated as-
Text or original data to be shared is termed as plain text. This plain text along with secret key is passed through mechanism of cryptography algorithms with embedment of secret key. A cipher text or data is produced as an output which can be shared across any network(i.e secured and unsecured). The cipher text can be decrypted only by the authorized user by unwrapping it with secret key.

Cryptography is an important trait for establishment of secure communication between two entities. There are several cryptography algorithms which can be implemented to enhance information with security features. In this paper, we will be focusing on methodology of following algorithms:

- Data Encryption Standard (DES)
- 3 DES
- Advanced Encryption Standard (AES)

Along with the study of these algorithms, this paper incorporates the encryption of text format data using DES, AES and encryption of image using AES inside an Android framework. The accomplishment of these modules creates a single platform with multiple functionalities. Thus, enriching security policy for any business ventures or organization.

II. Literature Review

This section focuses on the ideology and concept of block cipher which can also be referred to as fundamental entity of cryptography algorithms. The concept of block cipher can be stated as symmetric key which operating on pre-defined or fixed length group of bits, referred as blocks, with constant change. The general perspective of block cipher can be understood as:

It takes a 128 bit plain text and produces an output of 128 bit cipher text. Thus, embracing our text with security and privacy features. The same methodology is implemented while decrypting text data i.e. 128 bit cipher text is passed as input and output of p 128 bit plain text data is produced.

Most popular and applied design of block cipher is Data Encryption Standard Algorithm (DES). The introduction of DES algorithm in the world saw a outburst of conflicting opinions regarding the due to small range of key length and other limitations it inhibited.

DES provoked people to learn more about the outreach of block cipher and it's extent of being measured as security mechanism.

Describing about the current scenario, DES is considered to be unsafe for many applications as it's security had been preached by attackers several times. This makes it difficult for people to trust over this algorithm. There are certain possibilities due to which the DES algorithm failed. Some of them include: 56 bit key length was too small, no support for file with large data capacity. Several studies have embraced the theoretical weakness existing in the cipher. The advanced version of this algorithm i.e. 3-DES inhibits heavy security support for securing data. In past few years, the Advanced encryption Standard (AES) had overcome the extremities of DES.

III. METHODOLOGY

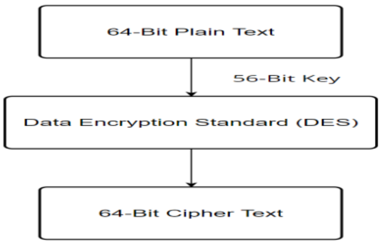
Elaborating further the concept of cryptography, in this paper we will discuss about the entire working of DES, AES algorithms.

To sustain sensitive information from unauthorized sources, it is essential to implement these algorithms for protecting our information. The detailed description and ideology of the above mentioned algorithms are as follows:

- Data Encryption Standard (DES) – The algorithm follows the basic fundamental of Feistel type cipher with substitution – permutation mechanism. DES algorithms comes under the category of symmetric block cipher recognized by National Institute of Standard and Technology (NIST). The approach of the algorithm can be understood as:

  DES accepts an input of 64 bit plain text along with 56 bit key and produces an output of 64 bit block. The plain text corporates to manage to shift the bits around the key. A single parity bit individually from each block gets removed from the key by subjecting the key to it's permutation. A 16 round feistel system is utilized convergence of 56-bit key into 16 number of 48-bit sub keys, individually assigned one for each cycle. For decryption, same algorithm is used but the order of sub keys is reversed. The blocks formed are 32 bits each, resulting complete block size of 64 bits.

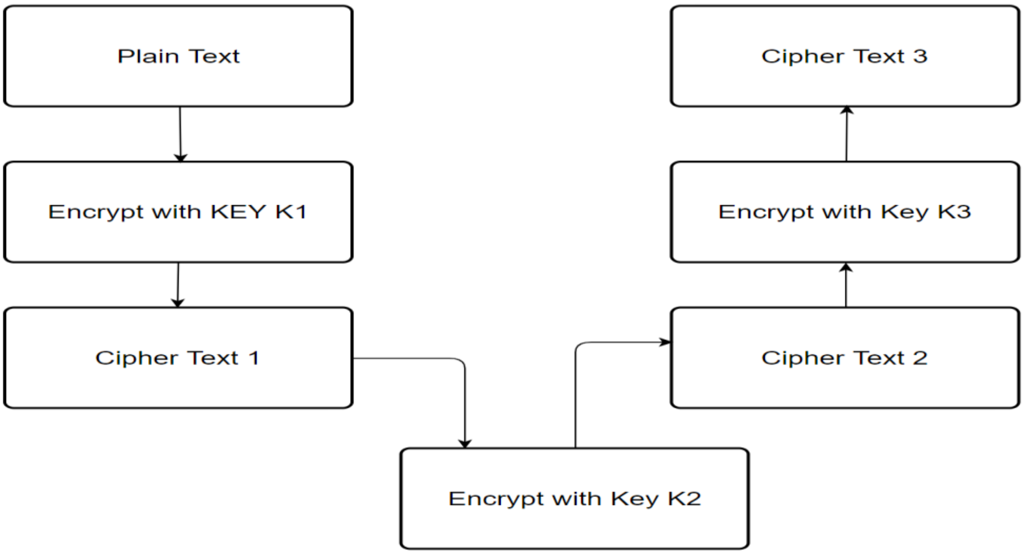
  In our model we have utilized DES algorithm for encrypting text format data.



Fundamental Diagram of DES

- Triple DES-We have not implemented this algorithm in our module, but to understand the concept of advanced security procedure, it is essential to acknowledge the perspective of 3 DES. It was designed to address the issues and challenges that were encountered in DES. In simple terms, 3 DES extends the key size capacity of DES by applying the algorithm 3 times repeatedly with 3 individual keys. Therefore, the total length of key after implementing 3 DES is 168 bits which deploys the fear of brute force attack being encountered. In today's Internet era, 3 DES is present in implemented in number of internet protocols protecting our information and data.

JETIR



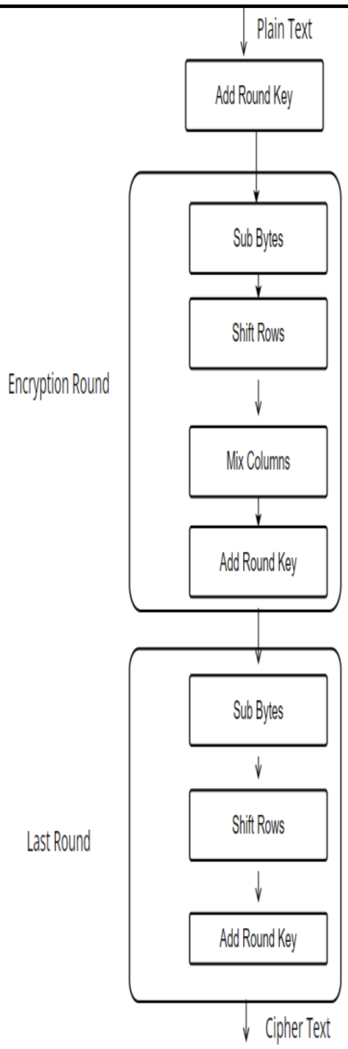
Fundamental Methodology OF 3DES

- Advanced Encryption Standard (AES) – With DES algorithm being easily obsolete by attacks, there was an immediate need to replace it with some standard algorithm for information privacy and protection. Therefore, NIST organized an event for developing a replacement of DES. As an outcome, Rjindael algorithm was introduced to the world which later on become Advanced Encryption Standard Algorithm. The AES algorithm depends on stating two ideologies i.e. speed and security. The approach of the algorithm can be described as:
AES algorithm defines data block of consisting of 128 bits distributed in 10, 12 and 14 rounds depending upon the size of the key. AES is an iterative approach which is composed of different rounds depending on the size of the key expansion. Each round consists of following four steps:

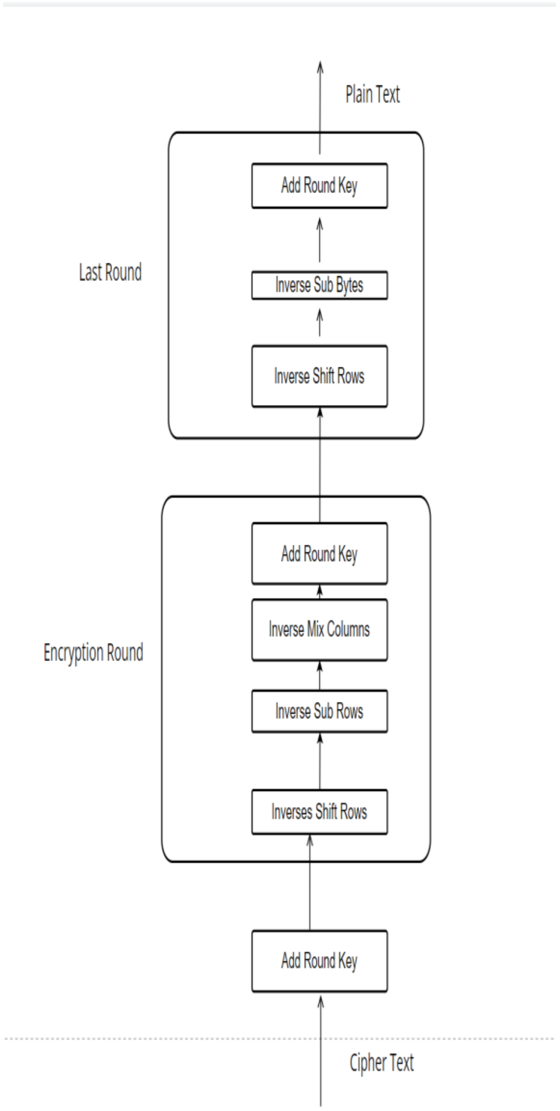
  Shift Rows : This is defined as a row-wise step that leads to a circular shift on the last 3 rows of the state.
  Sub Bytes: A process that enhances a non-linear substitution step by changing each byte with another value from the substitution box.
  Mix Columns: It is defined as a linear transformation which is obtained as a matrix product from four bytes of a column
  Add Round Key: This process is stated to implement the XOR operation on output obtained from the previous steps in combination with round key which generates the cipher key.

  The above steps are followed while encrypting information using AES algorithm. For decrypting the information ,the above steps are followed in an reverse manner i.e. Inverse Shift Rows, Inverse Substitute bytes, Add round key, Inverse mix columns. According to recent studies and analytics survey, there is a proclamation which states that the military intelligence could attacks equivalent to 90 bits. Since AES is entitled with 128 bits or 256 bits, making it difficult for any organization to attack on it. Based on recent study and evidences found, it has been observed that AES does not have any weakness except the exhaustive search approach which is brute force method. Therefore, AES provides efficient performance against several attacks surpassing the pitfalls of other obsolete algorithms.

  In the project mentioned, the implementation of AES algorithm is done for encrypting text data and image data file.



AES Encryption



AES Decryption

Performing comparative Analysis of DES, 3-DES AND AES:

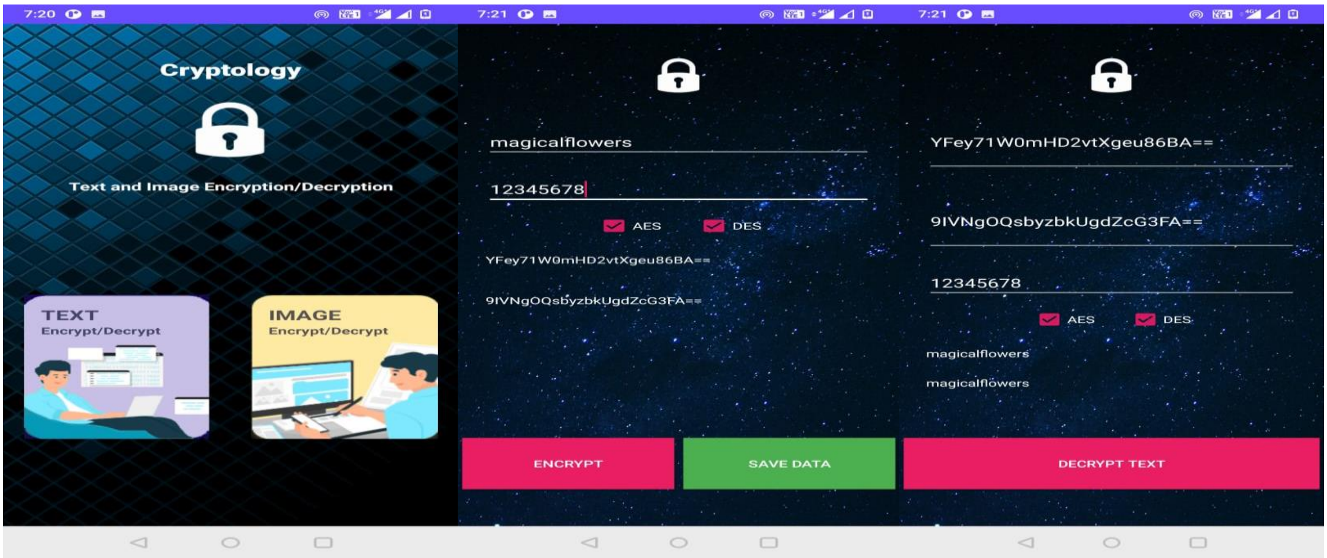
DES(Data Encryption Standard)	3-DES(Triple DES)	AES(Advanced Encryption Standard)
It was Developed in 1977 and is considered as the oldest crypto structure.	It was developed in 1978 to address the challenges faced by DES.	It was developed in 2000 to process data with speed.
Fixed block size of 64 bits.	Block size is fixed i.e. 64 bits, but the implementation of key is done thrice.	Varying block size can be created with capacity equal to 128 ,192 or 256 bits.
The length of the key is 56 bits i.e. 8 parity bits.	Total sum of 3 Keys with each having individual capacity of 64 bits equals to 168 bits.	It is similar to as block size with value as 128, 192 or 256 bits.
Proven obsolete against brute force.	Efficient for security purpose but consists of pit holes.	It is recognized as secured.
It is exhaustive and vulnerable towards linear, differential crypto methodology.	It can be attacked using brute force mechanism by implementation of differential analysis.	Designed in a way to sustain vulnerable attacks caused due to differential, linear and square attacks.

IV. IMPLEMENTATION

Depicting the out structure of our project model, we will be implementing DES, AES algorithms inside over android application to make it secure. We would be implementing the DES algorithm for encrypting text data format and AES for encrypting text, image format. This enables our project module to be multifunctional. The project is designed in such a way with user friendly technical as well as non-technical through which they can manage to maintain their information security and privacy.

V. RESULT

This section deals only with application working and its precision. As the model we have created encrypts data with precision of 70% to 80% (because we have implemented DES also, which can be breached). Also, there is a limitation while designing the DES module which states that the secret key must be of minimum 8 characters to encrypt the text data file. But in other module, where we have implemented AES, it provides efficient security performance(approx. 99%) without any restriction or limitation. Therefore, we can perform encryption over text data and image file with accuracy. Hence, the model serves as single platform with multiple functionality.



magicalflowers

12345678

☑ AES ☑ DES

YFey71W0mHD2vtXgeu86BA==

9IVNgOQsbyzbkUgdZcG3FA==

YFey71W0mHD2vtXgeu86BA==

9IVNgOQsbyzbkUgdZcG3FA==

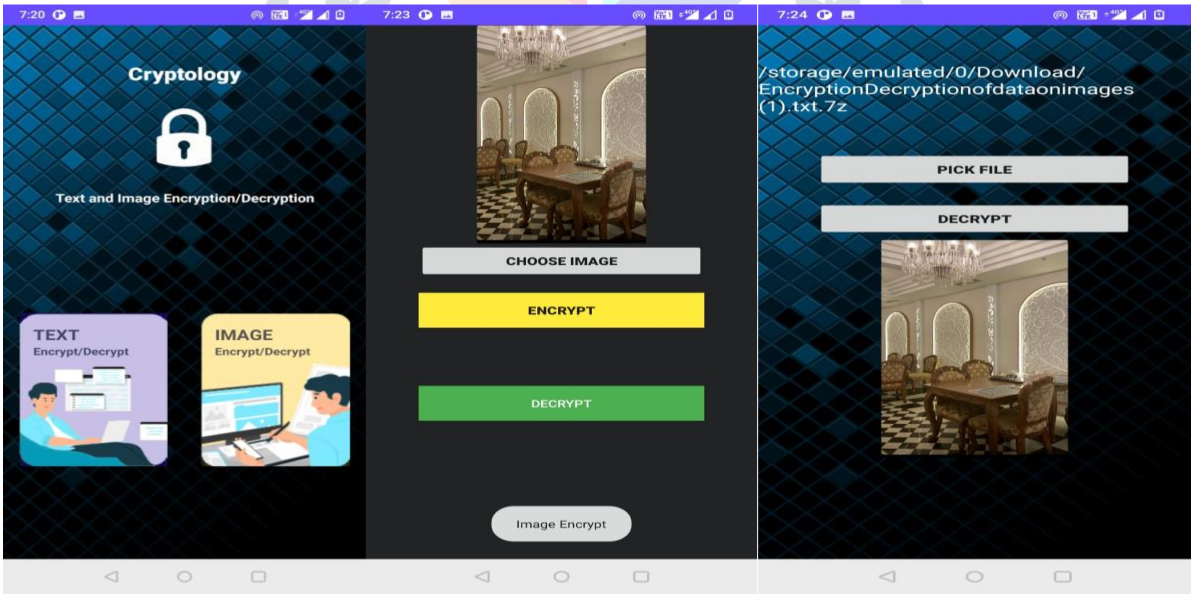
12345678

☑ AES ☑ DES

magicalflowers

magicalflowers

Text Encryption/Decryption using DES and AES



/storage/emulated/0/Download/EncryptionDecryptionofdataonimages(1).txt.7z

Image Encryption/Decryption using AES

VI. CONCLUSION

The ideology or principle behind performing this project was to enhance the practical approach of cryptography algorithms. There is a vast detailed study of cryptography algorithm present persisting of theoretical knowledge. There is a less study and research analysis done on the practical implementation of these algorithms. Our primary objective was to enhance our knowledge with theoretical explanation of these cryptography algorithms and perform detailed study regarding it. Further, the secondary objective focused on establishing practical implementation of our knowledge. We had successfully implemented the DES, AES algorithms in our application for encrypting our text and image format data. The efficient performance of these algorithms leads to powerful and effective performance of our application. Although the DES had been obsolete, but the combination of DES with AES at a single platform still provides high efficiency and accuracy for securing our information.

REFERENCES

- Data Encryption Standard. FIPS PUB 46, Appendix A, Federal Information Processing Standards Publication, January 15, 1977, US Department of Commerce, National Bureau of Standards.
- Samiul Islam “Comparative Analysis of AES algorithm and implementation of AES in Arduino” 20.12.2015.
- F.M. Haschka, “ Design and implementation of cross-platforms application for internet and mobile based interventions,” bachelor, Ulm university, 2019.
- V.R. Joan Daemen. AES proposal: Rijndael, version 2, AES Submission, 1999.
- Joan Daemen, Steve Brog and Vincent Rijmen.” The design of Rijndael: AES The Advanced Encryption Standard ,” Springer, 2002.
- Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid,” Symmetric Algorithm Survey: A comparative Analysis ” May 2,2014.
- A. Kahate, Cryptography and Network Security. Tata McGraw-Hill Education,2013.
- C. Paar and J. Pezl, Understanding cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.
- M. Sharma and R.B. Garg, “ DES: The Oldest Symmetric Block Key Encryption Algorithm,” no. November 1976, pp. 53-58,2016

JETIR