# Title of the Work

**ACE GAURD**

# Dairy Number

27971/2021-CO/L

# Type of Work

Literary

# Language of Work

English

# Submitted by

**Shivam Pandit, Shruti Dantala, Rutuja Umap, Shwetambari Borade**

Shah & Anchor Kutchhi Engineering College

Applicant and Author

**Shah & Anchor Kutchhi Engineering College**

Applicant

# Preface

This work which is a Literary work on the report for the project Ace Guard. This paper includes the implementation of our project Ace Guard, the software used for making the project and the usage. This work set forth the use of AES algorithm for encryption & decryption of Text/Image in the project. Through this work we aim to elucidate our project and AES encryption.

# Index

**Abstract--**

Once the confidentiality of information is to be maintained over the network. SMS being Encryption is of great importance one of the major means of data exchange among the mobile users. Security of SMS is one of the major issue that must be handled during data transmission. So, by using Android technology an application have been developed by us which permits the sender to encode the messages before they are sent over the network. For the encryption and decryption process we have used Advanced Encryption Standard (AES) as the cryptographic algorithm. The application allows the user to input the key and the message which has to be encrypted and hence generate encrypted message which can be decrypted by the receiver. The encrypted text so developed by app is also resistant to Brute Force attack as we have used AES.

## 1. Introduction

With the technological development and era of digitization, nowadays. exchange of messages, thoughts or information are done by using various message sending applications. Security of data plays an important part in wireless communication system. This communication involves exchange of data between a sender and a receiver, where both the end users seek the security of their shared information. AES or Advanced Encryption Standard also known as Rijndael is a symmetric block cipher used to encrypt or decrypt sensitive data to protect classified information.

It is considered one of the most safest technic to encrypt data as Brute-forcing it will take a enormous amount of time. We created this project in order to demonstrate how actually the AES encryption and decryption for text and image works.

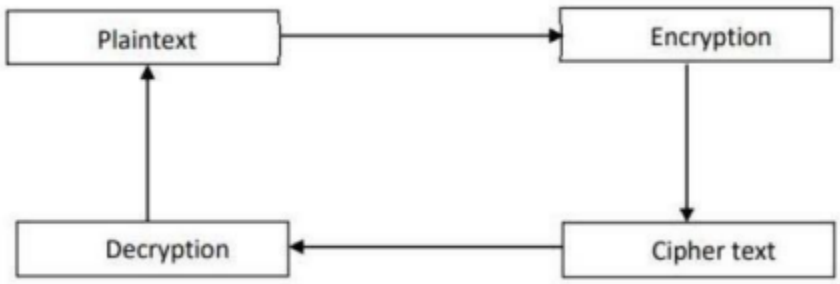
## 2. Literature survey

Analysis of cryptographic algorithm : Cryptography is usually considered as the study of secret. Where encryption is the process of converting normal text to unreadable form, decryption is the process of converting the encrypt a text to the normal text in readable form. The basic steps involved in the conventional encryption model are-
1) sending of message that is the plain text

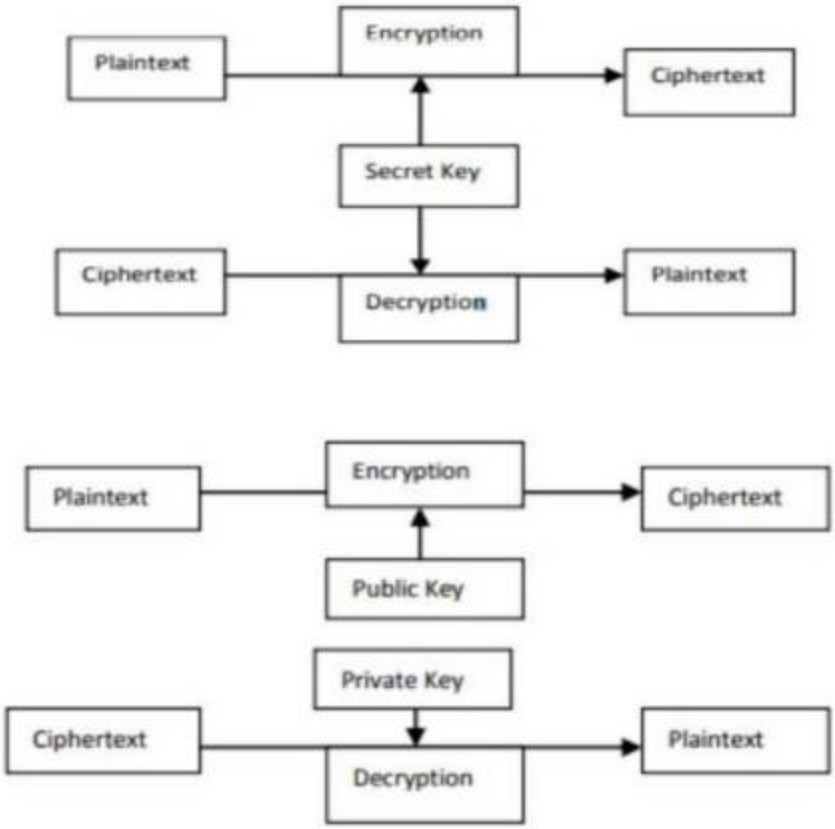
2) Converting the original message into the cipher text by using some key and algorithm

3) Transmission of the cipher text over some medium

4) The cipher text at the receiver end is then converted back to the original message using the same algorithm and key




Cryptography is mainly divided among two broad categories depending on the type of security keys used into Symmetric and a Asymmetric Encryption. While Symmetric encryption also known as private key uses single key for encryption and decryption Asymmetric encryption also known as public key encryption uses two keys separately for encryptions and cryption. While in symmetric encryption both the sender and receiver has to agree on a same secret key, in asymmetric encryption there are two keys: one public key which is known to the public and used for encryption and others private key which is known to the user and used for decryption.




Various encryption algorithms are available to perform encryption during confidential data transmission over network. Privacy is achieved by performing encryption of messages. The SMS is being on a good rise susceptible to attacks. So it has currently become important to encrypt the SMS before it has been sent. Encryption has long been used by by militaries and governments to facilitate secret communication. Encryption is currently normally utilized in protective info among several styles of civilian systems. AES need very less RAM space and it is very fast. On Pentium professional processors AES encryption needs solely eighteen clock cycles/byte corresponding to turnout of regarding 11 Mib/s for 200MHz.processor.There application provide various functionalities like plain text box. Encrypted box. Decrypted box, conversation view EI is made light weight and more importance given to the efficiency of encryption and decryption process. data can be maintained by means of cryptography. In cryptography, security is ensured by encoding the data before sending it and decoding the data after receiving it. Various cryptographic algorithms are used to ensure that privacy of data is maintained. SMS that stands for shot messager service is widely accepted as a means of information exchange, its security has become a significant concern for numerous business concern and

customers. So, there is a great requirement for an end to end SMS encryption in order to provide secure medium for communication. AES and DES are most commonly accepted and used cryptographic algorithms. While DES uses 56 bit key and hence is unprotected against brute force attack AFS is not susceptible to brute force attacks as it uses large sized keys.

## 3. Comparison of different survey papers

| SR NO. | YEAR | TECHNIQUE | PROBLEM | SECURITY SYSTEM | PROG. LANGU-AGE USED | USED ALGOR ITHM |
|---|---|---|---|---|---|---|
| 1) | 2017 | Symmetric cryptography | Less digital image and information Security on the internet | Cryptography system | JAVA | AES |
| 2) | 2015 | Application in android OS | Security breaches while the transmission occurs | Cryptography system | JAVA | NTRU |
| 3) | 2018 | Android – text to ASCII | Increase in Threats to digital data | Cryptography system | PYTHON | ECC |
| 4) | 2012 | Encryption in cloud data management | No vicinity of data for cloud user. | --- | C | RSA |
| 5) | 2020 | SMS App | apps not encrypting data by default | --- | JAVA | RC4 |
| 6) | 2020 | image steganography | Slow Encryption of LAN messages | System | --- | RSA |
| 7) | 2017 | Enigma algorithm | Improvement in security at node network and internet level | Program | JAVA | RSA |
| 8) | 2017 | --- | Large file size of data while transmitting | --- | JAVA, C, C++ | RSA, MD5 |

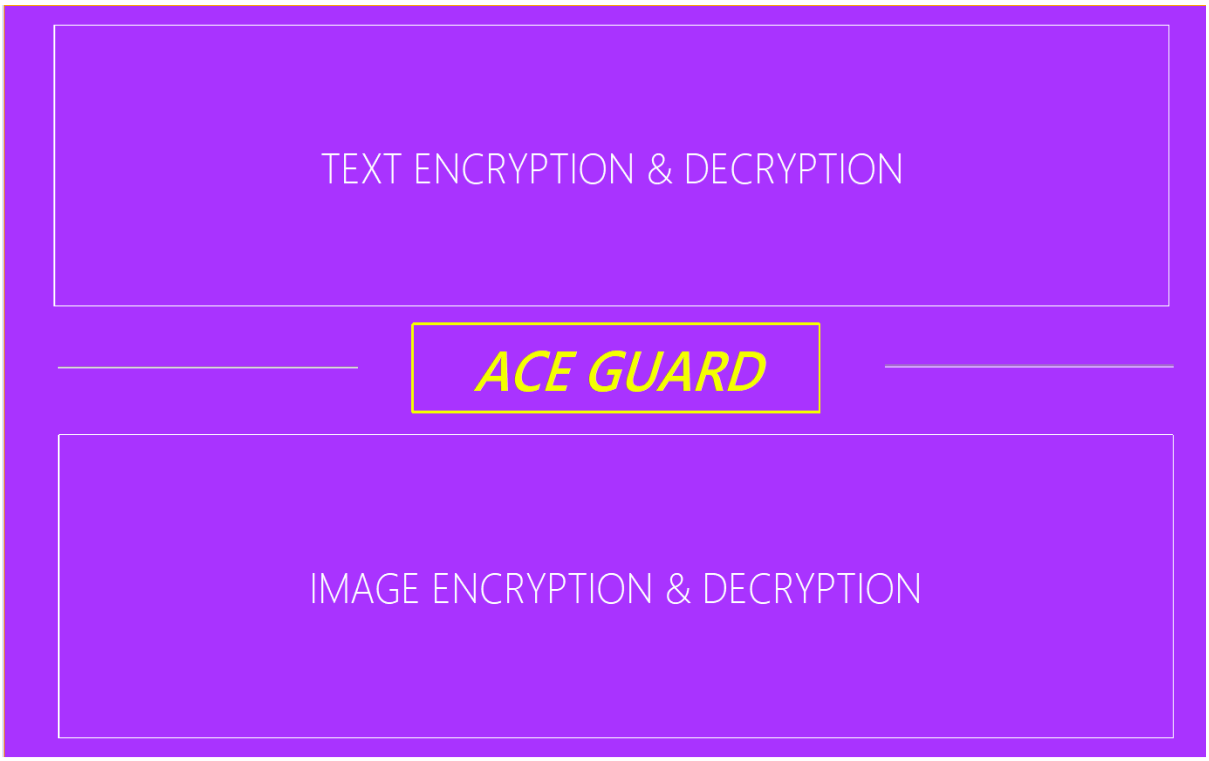
| SR NO. | YEAR | TECHNIQUE | PROBLEM | SECURITY SYSTEM | PROG. LANGU - AGE USED | USED ALGO R ITHM |
|---|---|---|---|---|---|---|
| 9) | 2020 | Hardware Implementatio n | Less efficiency When large amount of Calculation. Key management is difficult | Custom HCPU | --- | AES-RSA |
| 10) | 2017 | By changing the position of pixels | Due to data redundancy Encryption is difficult to handle on images | Magic square Method | --- | AES |
| 11) | 2014 | HTN tech | Double dummy Bridge problem | Point count system | --- | RBP |
| 12) | 2012 | Encryption and decryption | Image encryption and decryption Tech vulnerabilities | --- | JAVA | AES |
| 13) | 2019 | Cloud computing | --- | Computer program | JAVA | AES |
| 14) | 2019 | FGPA | semaphores of the algorithms relate to the proposed system. | Xilinx System | Python, C | DES |
| 15) | 2016 | Encryption and decryption | ---- | Asymmetric Cryptograph y system | JAVA | RSA |

## 4. Software used

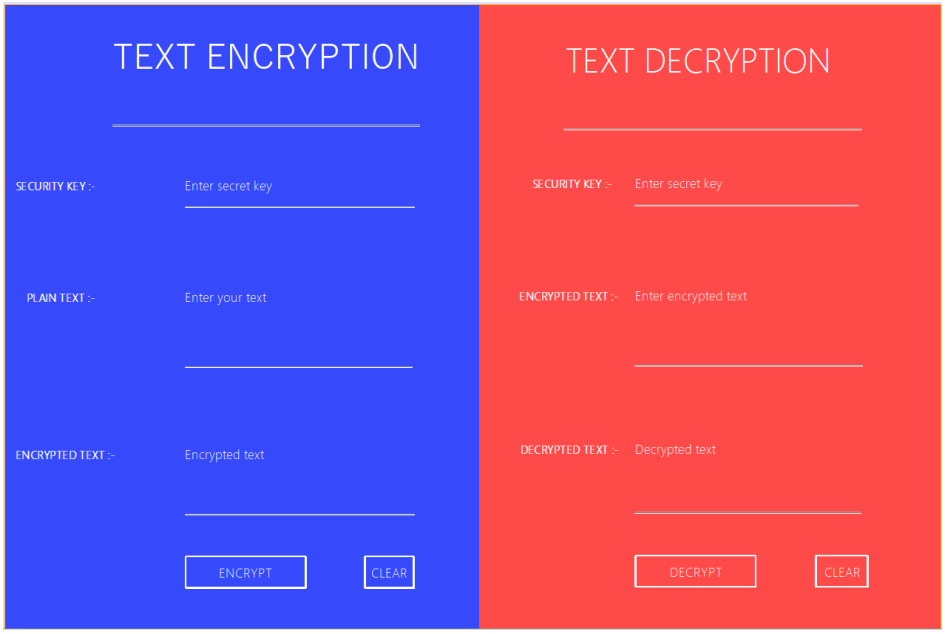
For the designing and layout of the system i.e frontend we have used JAVA Swing and JAVA for backend. We also used Apache Netbeans as IDE.

## 5. Design Details

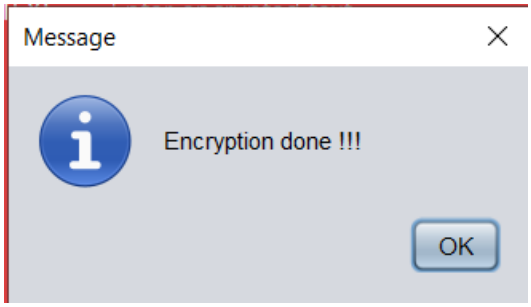
The complete outline of our project is described below

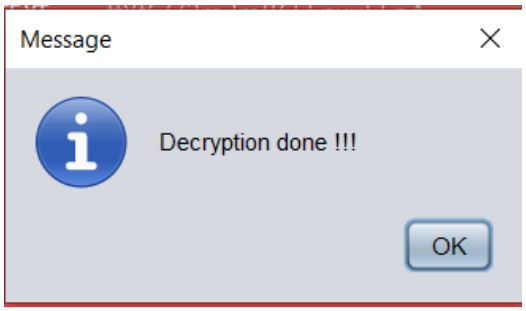


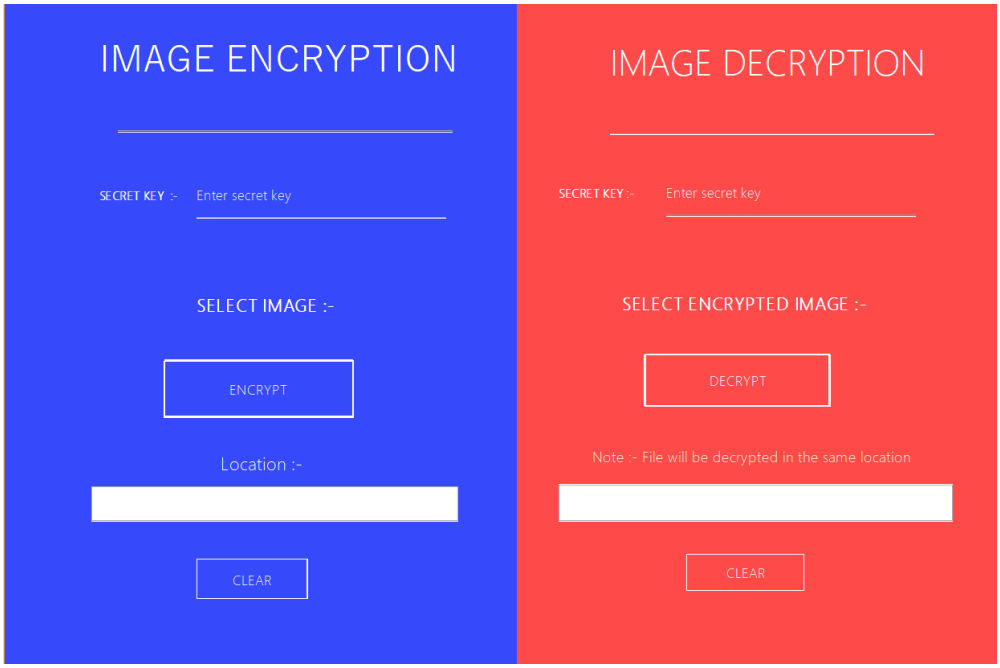

This is our main screen where the user can choose to either Encrypt or Decrypt Text or Image .




The above interface will appear once the user clicks text encryption. User have to enter the required details correctly. After the encryption/decryption is successfully done, it will pop up these below messages.



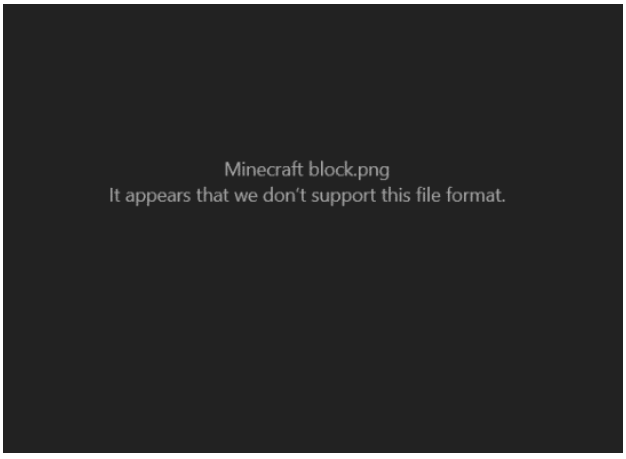






The above window will open when user clicks image encryption/decryption. The user have to put correct details and select the image and it will popup success message when done!

The below images are the demonstration of the image encryption and decryption .

(Image before encryption)




(Image after encryption)

(Image after decryption)

## 6. Future Scope:

Key distribution is also one of the major aspect that should be taken care of. As we are working with AES algorithm which is a symmetric encryption technique that is single to be used by both the sender and receiver so we also have to find ways to securely share the key. Key can be distributed in one of the following ways:

1. Physical transfer of the key from sender to receiver.

2. Key can also be delivered to sender and receiver with the help of trusted third party. 3. Key used by sender and receiver previously can be converted to new Key using Encryption.

4. Key can be provided to both users with help of KDC. 5. Diffie-Hellman method can be used for secure exchange of keys.

## 7. Conclusion:

SMS is the most common and major means of information exchange. This data can contain sensitive and vital information which needs to be protected. Which can be done using encryption. For this we have studied cryptographic algorithms. We devised that though asymmetric algorithm require 2 independent keys to encrypt and decrypt, it uses complex mathematical functions and is inefficient for small mobile devices. Hence we use symmetric algorithm for encryption. Also, among symmetric algorithms AES is the most

efficient and resistive to brute force attack. So we have designed an android application that helps the sender to encrypt the information using a key before sending it to the receiver who can decrypt the message with the same key.

## 8. References:


[1] Suchita Tayde and Asst Proff Seema Siledar, “File Encryption, Decryption Using AES Algorithm in Android Phone”, volume 5, Issue 5, May 2015, pp. 550-554.

[2] Er.Amanpreet Kaur, Er.Navpreet Singh, “SMS Encryption using NTRU Algorithm”, Vol. 3, Issue 2 (Apr.-Jun. 2015).

[3] Dimas Natanael’, Faisal’, Dewi Suryani, “Text Encryption in Android Chat Applications using Elliptical Curve Cryptography (ECC)” , (2018), 283–291.

[4] Parsi Kalpana, Asst Professor, Sudha Singaraju, “Data Security in Cloud Computing using RSA Algorithm”, Vol 1, Issue 4, September 2012, 143-145.

[5] Kaung Htet Myint, “SMS Security on Android Using RC4 Algorithm”,University of Computer Studies, Yangon, Myanmar.

[6] Faten H. Mohammed Sediq, Huda Abdalkaream Mardan and Nevart A. Minas. “Speed Up Image Encryption by Using RSA Algorithm”.2020 IEE,1302-1306.

[7] Md. Towsif Abir, Lamiya Rahman, Samit Shahnawaz Miftah, Sudipta Sarker, Md. Ibrahim Al Imran, Md. Shafiqul Islam, “Image Encryption and Decryption using Enigma Algorithm”, 2019-IEE.

[8] Altaf T. Shah, ‘’Vikramsingh R. Parihar. “QR-Code Based Messaging and File Sharing on Android Platform in View of Security”, 2017-IEE. 371-373.

[9] Lin Zhang, Bing Li, Xia Zhao, “Reconfigurable Hardware Implementation of AES-RSA Hybrid Encryption and Decryption”, 2020-IEE, 970-973.

[10] S.Sowmiya, I.Monica Tresa, A.Prabhu Chakkaravarthy, “Pixel Based Image Encryption Using Magic Square”, Department of CSE,St. Joseph’s College of Engineering.

[11] Assistant Professor, M Dharmalingam and Associate Professor, R Amalraj,“A work point count system coupled with resilient back -propagation algorithm for solving double dummy bridge problem“.Volume 3, Issue 3, May-June 2014, 189-193.

[12] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, “A Survey On Different Image Encryption and Decryption Techniques.” Vol. 4 (1) , 2013, 113 – 116.

[13] Amjad Y. Hendi, Majed O. Dwairi, Ziad A. Al-Qadi and Mohamed S. Soliman, “A Novel Simple and Highly Secure Method for Data Encryption-Decryption” Vol. 11, No. 1, April 2019 232-235.

[14] Subhi R. M. Zeebaree. Duhok Polytechnic University, Technical College of Informatics, Information Technology Department, Iraq, “DES encryption and decryption algorithm implementation based on FPGA” Vol. 18, No. 2, May 2020, pp. 774~781.

[15] M.I.Khalil Nuclear Research Center, Atomic Energy Authority, Cairo, Egypt, “Real-Time Encryption/Decryption of Audio Signal” February 2016, 2, 25-31.