ASIAN COLLEGE OF HIGHER STUDIES

(Affiliated to Tribhuvan University)

Dhobidhara, Kathmandu

Document Encryption Using AES

Final Year Project

Submitted by

Arogya Thapa Magar

(cs170810)

Sahil Ramjali
(cs170838)

Saken Rai

(cs170839)

Bachelor in Computer Science and Information Technology

Tribhuvan University

5th June 2021

Contents

1. Introduction

Cryptography is used to protect data and information. Among different information of the user, we are creating an android app to protect the document in this project using a cryptographic algorithm.

We are using Advanced Encryption Standard (AES) as it is a symmetric-key algorithm, where the same key is used for both encrypting and decrypting the data. It takes 128-bit plain text gives a 128-bit cipher key. Document and secret key are taken as input for the encryption and are stored in an encrypted format. That file can only be accessed after decrypting using the same key from this app.

Our objective is to develop a secure format of the document using the algorithms of cryptography (i.e AES)

2. Problem Definition

The number of android users is increasing day by day which also increases the rate of vulnerabilities of their data. [For more than a decade, the number of vulnerabilities reported in the National Vulnerability Database (NVD) was fairly stable, varying annually between 4,000 and 8,000 reported issues and for the most part decreasing or increasing by only 10% to 20% and in only one case, by half in any given year (2019). More security vulnerabilities were disclosed in 2020 (18,103) than in any other year to date at an average rate of 50 CVEs per day. 57% of vulnerabilities in 2020 were classified as being 'critical' or 'high severity.] [1]

This increase in vulnerabilities creates the risk of leaking the private information of the users. In order to protect their documents, it is a necessity to develop a method to keep their files safe. In order to decipher the data and information, a correct encryption scheme must be used. Document encryption is one of the efficient methods to doing so as it helps us to maintain a private and confidential manner. So, this application provides a method to convert files into a secure format.

3. Objectives:

- To maintain privacy of the document.
- To maintain authenticity and integrity of the document.

4. Research Methodology

4.1 Related work

Different types of cryptographic algorithms are being used in the different computer fields for securing data and information in the system. AES algorithm is also one of the algorithms that are used in the different computer fields for the protection of data and information. AES algorithms are widely used in networking, file transferring and communication, etc. to make data confidentiality and integrity. Some research journals and works done by others using the AES algorithm are given below.

Journal published on Procedia Computer Science on the project called A comprehensive Evaluation of Cryptographic Algorithms: DES,3DES, AES, RSA and Blowfish published by Priyadarshini Patil, Prashant Narayankar, Narayan D.G and Meena S.M [2] they used AES algorithm along with another algorithm for experiment and results show that evaluating DES, 3DES, AES, Blowfish and RSA algorithms based on parameter Avalanche effect AES scores highest; we can conclude that AES can be used in applications where confidentiality and integrity are of the highest priority. Results show that if cryptographic strength is a major factor in the application, AES is the best-suited algorithm.

Likewise in a Research paper published on International Journal of Advanced Research in computer science and software engineering on the topic called File Encryption, Decryption using AES Algorithm in Android Phone published by Suchita Tayde and Seema Siledar [3] They perform encryption and decryption of file and image using AES algorithm where they found faster encryption and decryption of file and image. This shows that the AES encryption and decryption algorithm run faster in android phone. It gives better security of mobile from unauthorized access.

Similarly, a Journal published in the International Journal of Computer Applications on the topic called SMS Encryption using AES Algorithm on android by Rohan Rayarikar, Sanket Upadhyay and Priyanka Pimpale they [4] make an application for an end to end secure transmission of SMS using AES algorithm. The application is developed on the Android platform.

Also in Journal published in the International Journal of Computer Science and Engineering on the topic called A Modified AES Based Algorithm for Image Encryption by M. Zeghid, M. Machhout, L. Khriji and R. Tourki where they [5] use A5/1 Key Stream Generator and W7 Key Stream Generator along with AES algorithm for image encryption in result improvement of the security of the AES algorithm.

5. Proposed System

Our project is about encrypting a document with the key provided by the user into a cipher document. Our project takes the document and the key from the user and creates a cipher document using that key, and the same key can decipher the document.

We are using AES (Advance Encryption Standard) algorithm for our project to encrypt the document. Among all the formats that are supported in android, we are mainly focused on encrypting the format of the document.

The approach is described below:

For encryption

- Takes a document and secret key from a user.
- Encrypts the document by passing it through AES algorithm.
- Returns the encrypted document to the user.

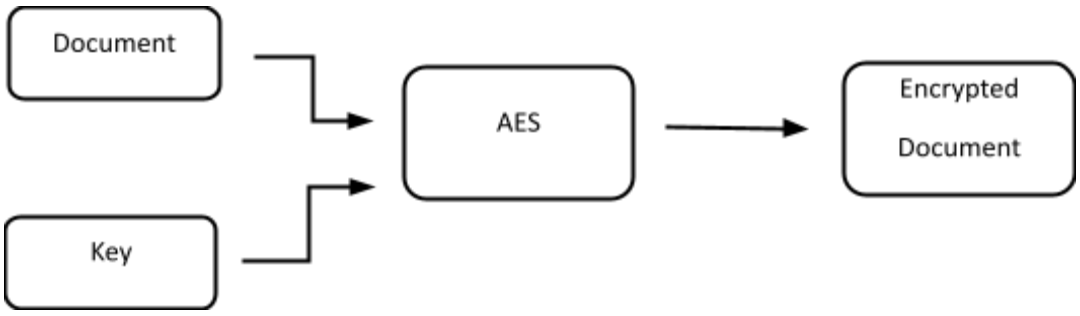

Fig.5.1: -Encryption

For decryption:

- Select the decrypt document and enter key that has been used for encryption.
- Press decrypt document.
- Result must be document is decrypted to its original form.

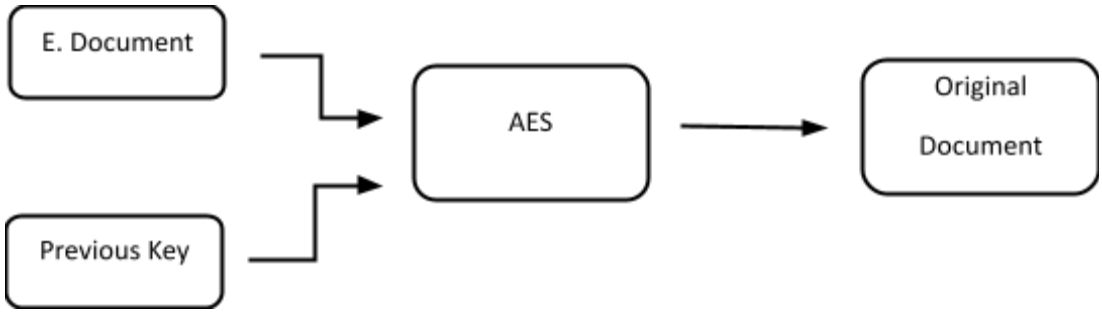

Fig 5.2: -Decryption

5.1 Feasibility Study

5.1.1 Technical feasibility

There is an AES algorithm to implement which is deliberately faster. So, this project is technically feasible.

5.1.2 Economic feasibility

All the resources that are needed to develop the project are available with us, so no further expenses are required. So, the project is economic feasible.

5.1.3 Schedule feasibility

We have enough time and proper schedule to develop the project, so it is schedule feasible.

5.2 Implementation

The tools and languages we are going to use are as follows:

- Primary coding language: Java
- Algorithm: Advanced Encryption Standard
- Design Tools: Photoshop
- IDE/Code Editor/App templates: Android Studio

5.3 Testing

Once the development of our project is completed, as we are using AES algorithm the testing will be done on following ways:

- Encryption and Decryption using same key. (Should be True)
- Encryption and Decryption using different key. (Should be False)

5.4 Evaluation

We evaluate following workings after testing:

- Does the system encrypt the document?
- Does the system generate the same output as input before encryption and after decryption?
- Does the key used for encryption can be used for decryption to give the same output as input?
- Is UI user friendly?

6. Working Schedule

6.1 Work Distribution

Task	Sahil	Saken	Arogya
Study and Analysis	✓	✓	✓
Coding and Design	✓	✓	✓
Implementation		✓	✓
Testing		✓	
Documentation	✓		✓
Review	✓	✓	✓
Presentation	✓		

Topic/Week	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th	11th
Study and Analysis											
Coding and Design											

Implementation											
Testing											
Documentation											
Review											
Presentation											

7. References

[1] R. Lemos, "TechBeacon," [Online]. Available: https://techbeacon.com/security/state-vulnerability-reports-what-cve-surge-means. [Accessed 01 06 2021].

[2] P. P. P. N. N. D. and M. S. , "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Computer Science,* no. 1 jan 2016, pp. 617-624, 2016.

[3] S. Tayde and S. Siledar, "File Encryption, Decryption Using AES Algorithm in Android Phone," *International Journel of Advanced Research in computer science and software engineering,* no. 5 may 2015, 2015.

[4] R. Rayarikar, S. Upadhyay and P. Pimpale, "SMS Encryption using AES Algorithm on Android," *International Journal of Computer Applications,* no. 2012 July, pp. 12-17, 2012.

[5] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, "A Modified AES Based Algorithm for Image Encryption," *International Journal of Computer Science and Engineering,* vol. 1, pp. 70-75, 2007.