Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

File Encryption, Decryption Using AES Algorithm in Android Phone

Suchita Tayde*, Asst. Prof. Seema Siledar
Department of Computer Science & Engineering;
MIT Aurangabad, Maharashtra, India

Abstract— Nowadays smart gadgets including smart phones and tablets are gaining huge popularity. Comparing with conventional computer, smart phone is easily carried out and provides much computer functionality, such as processing, communication, data storage as well as many computers services such as web browser, video or audio player, video call, GPS, wireless network. However, smart phone have to come long way in terms of security. Encryption is used for security of information in data storage and transmission process. Various encryption algorithms like DES, 3DES, Blowfish, RSA and others are available to secure the data. In DES, key size is too small. In 3DES, key size is increase but the process is slower than other methods. We have used Advanced Encryption Standard algorithm to overcome above problems. AES algorithm is not only for security but also for great speed. It can be implemented on various platforms especially in small devices like mobile phone. Everyday data is shared, transmitted, stored for many purpose like banking, production, research and development. Hence, we need security for information. Encryption can provide security. This application allows user to run this application on android platform to encrypt the file before it is transmitted over the network. It is used for all type of file encryption such as text, docx, pdf and image encryption. AES algorithm is used for encryption and decryption.

Keywords— Smart handheld devices, AES, Encryption, and Decryption.

I. INTRODUCTION

Today mobile phones are most important and habitual thing for each human being. Due to increasing use of smart phone, tablet, computer, growth of internet, multimedia technology in our society digital image and information security is the most critical problem. Criminal or thief is an unknown person who reads and changes the information while transmission occurs. So to protect such sensitive data has become demand of the day. Encryption is one of the technique uses to protect the sensitive data from the unauthorized person.

There are two types of encryption algorithm Symmetric keys encryption and Asymmetric keys encryption.

In Symmetric keys encryption or secret key encryption, only one key is used to encrypt and decrypt data. Key should be distributed before transmission between entities. Keys play important role [8]. Various symmetric key encryption algorithms are DES, 3DES, AES, and Blowfish.

In Asymmetric key encryption or public key encryption, two keys are used; private and public keys. Public key is used for encryption and private key is used for decryption. Because user tends to use two keys public this is known to public and private who is known to user.(E.g. RSA and Digital Signatures)[8].There is no need for distributing them prior to transmission [3].

II. LITERATURE SURVEY

In this various encryption technique are used by different papers are discussed.

Agrawal et al. [3] present detailed study of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than asymmetric encryption algorithms. Security of Symmetric key encryption is superior to Asymmetric key encryption. It was concluded that the supremacy of Blowfish algorithm over DES, AES and Triple DES on the basis of key size and security. The F function of Blowfish algorithm provides a high level of security to encrypt the 64 bit plaintext data.

Seth et al. [4] made a comparative analysis of three algorithms, DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte. It was concluded that RSA consumes longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm. Based on the text files used and the experimental result it was concluded that DES consume least encryption time and AES has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm.

Mandal et al. [6] made the comparison between four most commonly used Symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison has been made on the basis of parameters: round block size, key size, encryption/decryption time, and CPU process time in the form of throughput and power consumption. It was concluded

that blowfish is better than other algorithms. Also AES has advantage over the other 3DES and DES in terms of throughput and decryption time. 3DES has least performance among all mentioned algorithms.

Marwaha et al. [7] discussed three algorithms DES, 3DES and RSA. DES and 3DES are symmetric key cryptographic algorithms and RSA is an asymmetric key cryptographic algorithm. Algorithms have been analyzed on their ability to secure data, time taken to encrypt data and throughput the algorithm requires. Performance of different algorithms was different according to the inputs. It was concluded that confidentiality and scalability provided by 3DES over DES and RSA is much higher and makes it suitable even through DES consumes less power memory and time to encrypt and decrypt the data but on security from DES can be easily broken by brute force technique as compared to 3DES and RSA, making it the last secure algorithm.

Abdul et al. [8] discussed six most common encryption algorithms such as AES (Rijndael), DES, 3DES, RC2, BLOWFISH and RC6. These algorithms were compared and performance was evaluated. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. It was concluded that there is no significant difference when the results are displayed either in Hexadecimal Base encoding or in Base 64 encoding. Secondly in the case of changing packet size, it was concluded that BLOWFISH has better performance than other common encryption algorithms used, followed by RC6. Also in the case of changing data type such as image instead of text, it was found that RC2, RC6 and BLOWFISH has disadvantage over other algorithms in terms of time consumption. Also, it was found that 3DES still has low performance compared to algorithm DES. Finally in the case of changing key size, it can be seen that higher key size leads to clear change in the battery and time consumption.

Apoorva et al. [9] compared most common symmetric cryptography algorithms: AES, TWOFISH, CAST-256 and BLOWFISH. The comparison took into consideration the behavior and performance of algorithms when different data loads were used. The comparison was made on the basis of these parameters: speed, block size, and key size. It was concluded that blowfish is superior to other algorithm as it takes less time. Although when the data size was very small this difference was not clearly visible. But for file having size greater than 100 KB, it was very clearly visible.

III. ENCRYPTION ALGORITHMS

A. DES: DES (Data Encryption Standard) was designed by IBM in 1977.The algorithm encrypts a 64 bits plaintext block using 56 bit key and 16 cycle of each 48 bit sub keys are formed by permuting 56 bit key. Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher.

B. 3DES: 3DESis a modified version of the DES algorithm that improves the security power of the DES by applying the algorithm three times in succession with three different keys. Encryption method is same as original DES but applied 3 time to increase the encryption level so the process was too slow than other methods [1].

C. Blowfish: Blowfish uses 64-bits block size, and a variable key size ranges from 32-bits to 448-bits.It is a 16 round fiestel cipher that uses the large key size. Since the key size is larger it is complex to break the code in the blowfish algorithm [2]. Moreover it is vulnerable to all the attacks except the weak key class attack

D. RSA: RSA is widely used Public-Key algorithm. RSA firstly described in 1977. The RSA Algorithm is public key cryptography and it ensures that whilst an encryption key is publicly revealed, it does not reveal the corresponding decryption key.

E. AES: AES was developed by two scientists Joan and VincentRijmen in 2000. It is fast, compact, and has a very simple mathematical structure [3].AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits, or 256 bits; called AES-128, AES-192, and AES-256, respectively. AES-128 uses 10 rounds, AES-192 uses 12 rounds, and AES-256 uses 14 rounds. AES performs the following functions: 1. SubBytes () 2. ShiftRows () 3. MixColumns () 4. AddRoundKey ().

1. Substitute bytes – The sub byte step replace each state data byte with an entry in fix lookup table.
2. Shift rows – The shift rows step rotates the four bytes of state data in each row in state data matrix.
3. Mix column – The mix columns step performs a transformation on the four bytes of state data in each column in state data matrix.
4. Add round key – The add round key step is a transformation that combines the current state data block and the round key corresponding to specific round using XORed function.

IV. METHODOLOGY

1. SYSTEM ARCHITECTURE

Symmetric key cryptography is generally used to encrypt the data having large sizes. In symmetric cryptography, there is a single key (called secret key or private key) that is used to encrypt as well as decrypt the data. The parties that need to communicate with each other must have same secret key. The system architecture is shown in Fig 1 Proposed system is performing in the following procedures: Fig1 shows the encryption and decryption process of plaintext file. Encryption takes place at sender side while decryption at receiver side. The input of encryption process is plaintext file and that of decryption process is the cipher text file. First plain text file is passed through the AES encryption algorithm which encrypts the plain text file using a key and then produce cipher text file i.e. encrypted file is transmitted. At the end of decryption the input cipher text file is passed through the AES decryption algorithm which can decrypt the cipher text file i.e. encrypted file using the same key as that of encryption finally we get the original plain text file. The result shows the encryption and time.

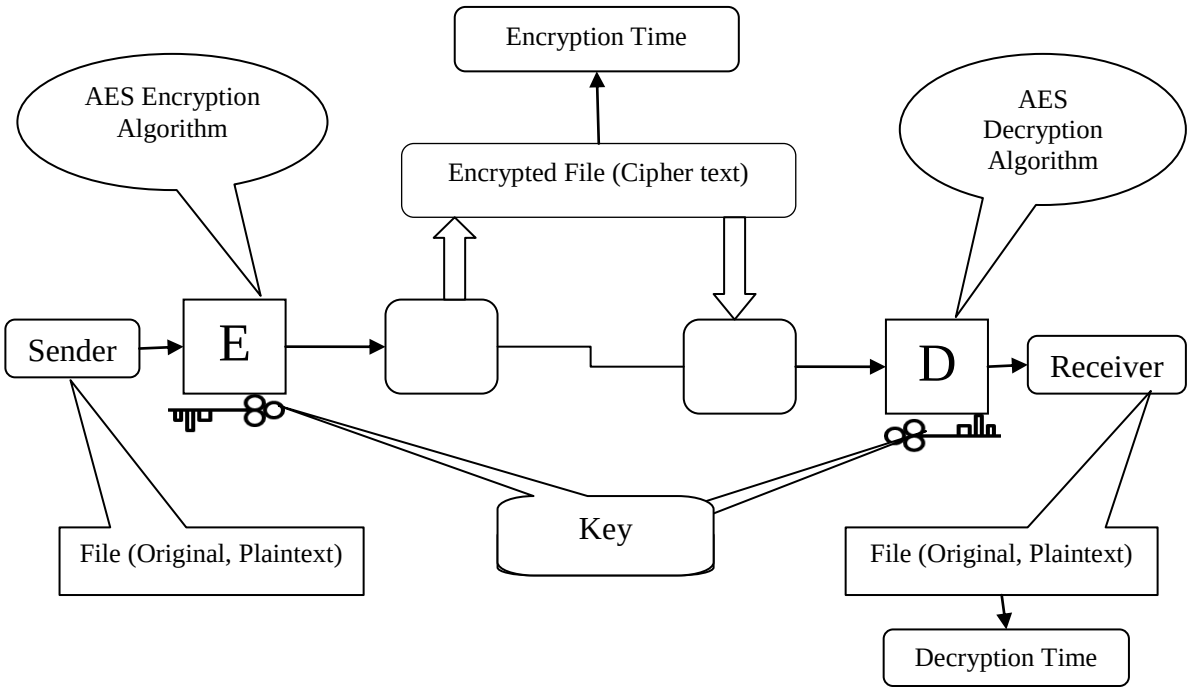

Figure 1: System Architecture

2. ALGORITHMS FOR PROPOSED SYSTEM

There are different types of terminologies used in algorithm to describe the implementation of proposed system. The flow of a system divided into two phases, one is 'Key Generation 'and second is 'To Encrypt and To Decrypt'.

a. Key Generation

The following steps are used to generate the key

1. Generate the AES key using Key Generator.
2. Initialize the key size.
3. Generate the secret key.

b. To Encrypt and To Decrypt

1. Create a Cipher by specifying the following parameters //Algorithm name - AES
2. Initialize the Cipher for Encryption.
3. Encrypt the file. // Declare /Initialize file
   //Convert the input array to bytes
   //Encrypt the byte using doFinal method
4. Calculate the encryption time.
5. Decrypt the file. //Initialize a new instance of cipher.
   //Decrypt the cipher bytes using do Final method.
6. Calculate the Decryption time.

3. PACKAGES AND CLASSES USED IN IMPLEMENTATION

The following packages and classes are used in the program:

javax.crypto.Cipher; // Used to initialize cipher for the algorithm and specify the mode which we want ENCRYPT-MODE or DECRYPT-MODE

javax.crypto.KeyGenerator; // This class provide the public API for generating symmetric key.

javax.crypto.spec.SecretKeySpec; //Key Specification for secret key also used for raw secret key that can be specified as byte.

java.security.SecureRandom; //This class is used when the pair of keys are generated to choose parameter randomly.

V. RESULTS

A. Result for File Encryption and Decryption

The original input file taken by this project is of .txt file of size 165 kb which is as follows:

Figure 2: Input original file before encryption

The cipher text file .txt file of size 235 kb as shown below:

Figure 3: Encrypted File

This file is output of encryption and input to decryption. The decrypted output file looks like original file. It is also .txt file of size 165 kb as below:

Figure 4: Decrypted File after decryption

B. Result for Image Encryption and Decryption

The original input image taken by this project is of .jpg file of size 603.3 kb which is as follows:

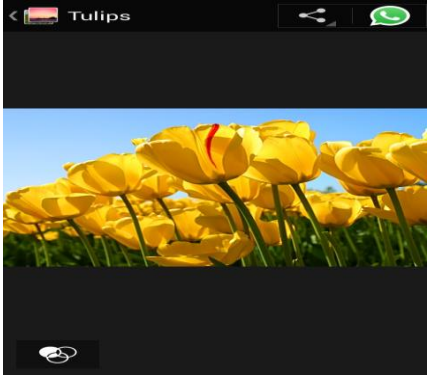

Figure 4: Input original image before encryption

The cipher text image is blank image .jpg file of size 819.1 kb as shown below:

Figure 5: Encrypted image

This image is output of encryption and input to decryption. The decrypted output image looks like original image. It is also .jpg file of size 603.3 kb as below:

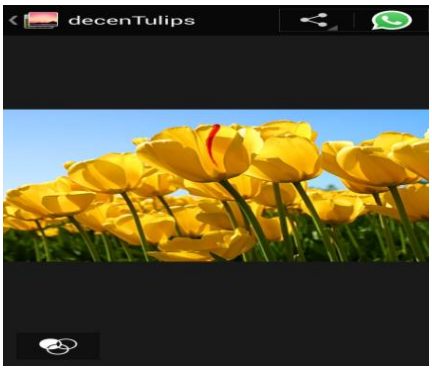

Figure 6: Decrypted image after decryption

VI. CONCLUSION

This paper shows successful implementation of file and image encryption as well as decryption. The user experiences faster file encryption and decryption. This shows that the AES encryption and decryption algorithm run faster in android phone. It gives better security of mobile from unauthorized access. This application guarantees secure end to end transfer of data without any corrupt data.In future the work may be extended by video encryption and developing a stronger encryption algorithm with high speed and less memory usage.

REFERENCES

[1] William, "Cryptography and Network Security Principles and Practice", Fifth Edition, Pearson Education, Prentice Hall, 2011

[2] Schneier B., "Applied Cryptography", John Wiley& Sons Publication, New York, 1994.

[3] Agrawal Monika, Mishra Pradeep, "A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, pp. 877-882.

[4] Seth ShashiMehrotra, Mishra Rajan, "Comparative analysis of Encryption algorithm for data communication", International Journal of Computer Science and Technology, vol. 2, Issue 2, June 2011, pp. 292-294.

[5] AlamMd Imran, Khan Mohammad Rafeek. "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 10, October 2013, pp.713-720.

[6] MandalPratap Chandra, "Superiority of Blowfish Algorithm" IJARCSSE, volume 2, Issue 9, September 2012, pp. 196-201

[7] MarwahaMohit, Bedi Rajeev, Singh Amritpal, Singh Tejinder, "Comparative Analysis of Cryptographic Algorithms", International Journal of Advanced Engineering Technology/IV/III/July-Sep, 2013/16-18.

[8] Abdul D.S, Kader H.M Abdul, Hadhoud, M.M., "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA, Volume 8, 2009, pp. 58-64.

[9] Apoorva, Kumar Yogesh, "Comparative Study of Different Symmetric Key Cryptography", IJAIEM, vol. 2, Issue 7, July 2013, pp. 204-206.

