EFFICIENCY ANALYSIS OF SYMMETRIC ALGORITHMS FOR MOBILE SECURITY AND COULD COMPUTING.

K RAMYA MADHAVI (ASST. PROF), G.USHASRI(ASST. PROF), P. AMBA BHAVANI(ASST. PROF), A MANASA(ASST. PROF)

Department of Information Technology, MVSR Engineering College,Nadergul,Hyderabad

Abstract: Data is important to everyone, may it be personal or an organization's data, storing and securing it has become a great challenge for the present world. Even protection through encryption of data through standard algorithms poses a risk for being compromised to third parties or unauthorized personnel. Though the data may be encrypted, new age hackers somehow find a way to breach into the security using advanced tools and tactics. Very few apps on Android have a safeguard feature to provide cryptographic security to the files present in the system. The project aims at storing and securing personal data using cryptographic algorithms. The main goal is to develop an Android Application that takes in the user's data and then secures it by encrypting it. Data may be of the format such as images, text, pictures etc. The application encrypts the data using an encryption algorithm and then can retrieve back the data using the appropriate decryption algorithms. Data which is encrypted can also be shared by uploading it to an Online Database for having global availability so that the encrypted file can be accessed anywhere in the world that too only by its rightful owner. This main feature and the whole application itself serve a serious purpose to those who are looking forward to secure their data on-the-go.

Keywords: AES, Triple DES, Blowfish, Cryptography,

Introduction

With the development of rapidly growing technological market and new trends in technology and gadgets, the measures to obtain or gain access to these technologies illegally or by wrong means are also growing in par. There is a dire need to have a system that can prevent these types of intentional breaches in the technological sector. In today's world where a person cannot be seen without his/her cell phone or smart phone in hand, hackers target these smart phone users in order to extract or obtain information or data without the users knowledge/consent or can even trick the user into giving his/her data or personal/private info.

Encryption Algorithms

1. **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.

2. **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.

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

4. **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.

5. **AES**: AES was developed by two scientists Joan and VincentRijmen in 2000. It is fast, compact, and has a very simple mathematical structure .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.

Symmetric Algorithms

Few of the popular symmetric key encryption algorithms are DES, TRIPLE DES, AES, and Blowfish. These Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA 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. A comparative analysis of three algorithms, DES, AES and RSA considering certain parameters such as computation time, memory usages and output byte was made. 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. A comparison was made between four most commonly used Symmetric key algorithms: DES, 3DES, AES and Blowfish 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.

Proposed System

Our aim is to build an application for smart phone users wherein one can secure his/her data by encrypting/decrypting it. Data may be of the format such as images, text, videos etc. The application encrypts the data using encryption algorithms and then can retrieve back the data using the appropriate decryption algorithms. Data which is encrypted can also be shared by uploading it to an Online Database for having global availability so that the encrypted file can be accessed anywhere in the world that too only by its rightful owner. This main feature and the whole application itself serve a serious purpose to those who are looking forward to secure their data on-the-go. The way a user can secure his/her data is by choosing a file from their phone storage for which they need protection for and then by giving an appropriate password to that chosen data file for being encrypted by a 3-way secure encryption process which then returns an encrypted file which cannot be accessed by anyone else in the world except by the user who has encrypted it. The file which has been encrypted can be decrypted in order to obtain back the original data file and the encrypted file is decrypted successfully only when the correct password is given to it.

The basic **key features** of this application is listed below

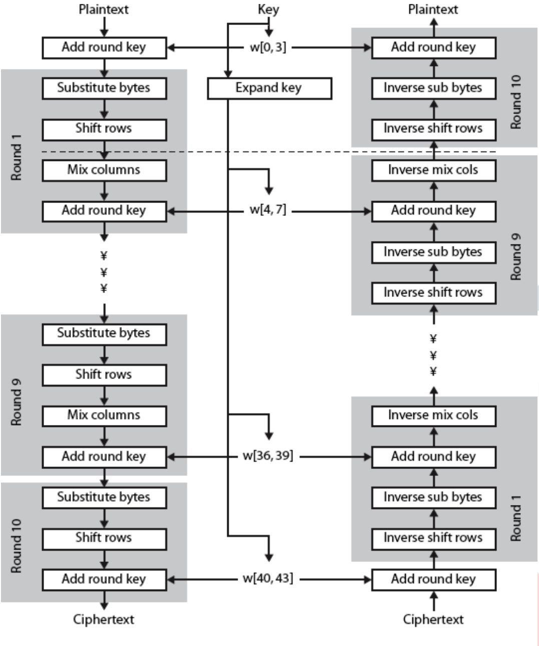
1. Encryption through 3-way encryption process
2. Decryption only when given password is correct
3. Uploading to Online Database
4. Thorough security towards phone’s data storage
5. Transfer files seamlessly without the fear of being compromised by third parties.

Encryption Process of AES:

- AES deals with fixed size block of 128 bits or 16 bytes in length which is represented in 4x4 matrixes of bytes known as state array, which is modified at each round of encryption and decryption.
- The key provided as input is depicted as a square matrix of bytes and is then expanded into an array of forty-four 32-bit words, w[i]. Four distinct words (32bits * 4 = 128 bits) serve as round key in each round of the encryption and decryption.
- Based on the length of secret key used (128, 192,256) for the encryption, the number of rounds i.e., N (10, 12, 14) in the cipher will differ accordingly. The single round of AES encryption process is shown in Fig. 4.
- First N-1 round in the AES cipher structure consists of the four basic transformations that encrypt the plain text of 128 bits in length of which one performs permutation and three perform substitution. The transformations are as follows:
  - AddRoundKey: It is a simple bitwise XOR operation of the current state array with a portion of the expanded key.
  - Substitution bytes: It uses an S-box to perform a byte-by-byte substitution of the state array.
  - ShiftRows: It is a simple permutation.
  - MixColumns: It consists of substitution operation that makes use of arithmetic over GF (28).
- The final Nth round contains only three transformations, and there is an initial single transformation i.e., AddRoundKey before the first round, which can be considered as round 0.
- The cipher begins and ends with an AddRoundKey transformation because only the AddRoundKey makes use of the key. The other three transformations together provide confusion, diffusion, and nonlinearity, but no security since they don‟t use the key.
- Each transformation in a round takes one or more 4x4 matrices or state array as an input and produces a 4x4 matrix as output. The output of the final Nth round will produce the cipher text.
- Each transformation is easily reversible. For the Substitute Byte, ShiftRows, and MixColumns stages, an inverse function is used in the decryption algorithm. For the AddRoundKey stage, the inverse is achieved by performing XOR with the same round key to the block (A XOR A XOR B = B).

Decryption Process of AES:

- The **Decryption process** in AES will use the expanded keys in the reverse order as used in the encryption. The decryption algorithm is not identical to the encryption algorithm. The order of transformations used in each round of decryption is different from that used in encryption.



(a) Encryption (b) Decryption

Fig 1: AES Encryption and Decryption Process

Triple DES (3DES) is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods. It uses either two or three 56 bit keys in the sequence Encrypt-Decrypt- Encrypt (EDE). Initially, three different keys are used for the encryption algorithm to generate cipher text on plain text message, t.

$C(t) = E_{k1}(D_{k2}(E_{k3}(t)))$……. (1)

Where C(t) is cipher text produced from plain text t,

E_{k1} is the encryption method using key k1

D_{k2} is the decryption method using key k2

E_{k3} is the encryption method using key k3

Another option is to use two different keys for the encryption algorithm which reduces the memory requirement of keys in TDES.

$$C(t) = E_{k1}(D_{k2}(E_{k3}(t)))\ldots\ldots. \quad (2)$$

3DES algorithm with three keys requires 2^168 possible combinations and with two keys requires 2^112 combinations. It is practically not possible to try such a huge combination so 3DES is a strongest encryption algorithm. The only disadvantage of this algorithm is that sometimes it can be too time consuming.

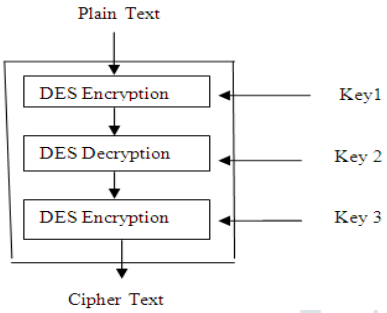


Fig2: Encryption and Decryption in 3DES

Operation of Blowfish:

Blowfish encrypts 64-bit block cipher with variable length key. It contains two parts

- **Sub key Generation**: This process converts the key up to 448 bits long to sub keys to totaling 4168 bits.
- **Data Encryption**: This process involves the iteration of a simple function 16 times. Each round contains a key dependent permutation and key- and data dependent substitution.

Blowfish suits the applications where the key remain constant for a long time (e.g. communication link encryption) but not where the key changes frequently (e.g. packet switching).

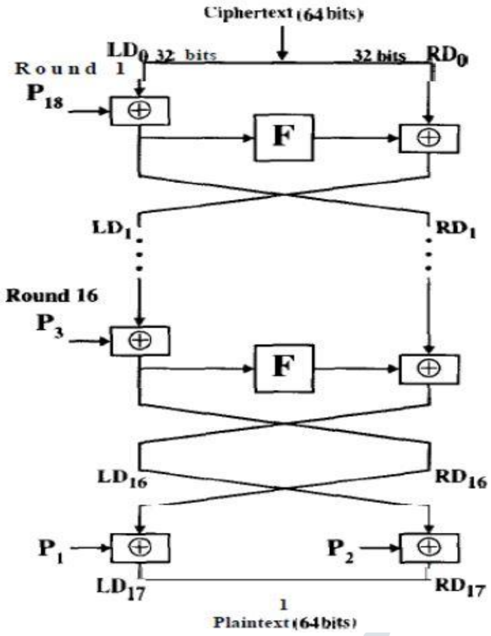
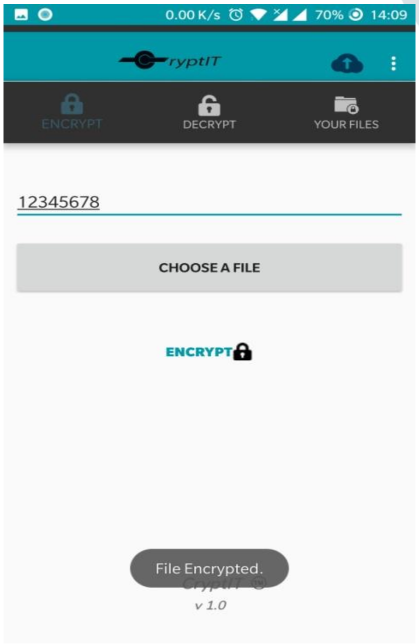


Fig 3: Blowfish Encryption

The entire operation of the underlying Application is to successfully encrypt and decrypt the file which is given to it as input. The main technique by which the whole application proves as a useful tool for securing one’s data purposes, is by **random shuffling** between the implemented algorithms in a **specific order** which is crucial for the decryption process as the order in which the file was encrypted is necessary to be known by the decryption process for implementing the decryption algorithm successfully.

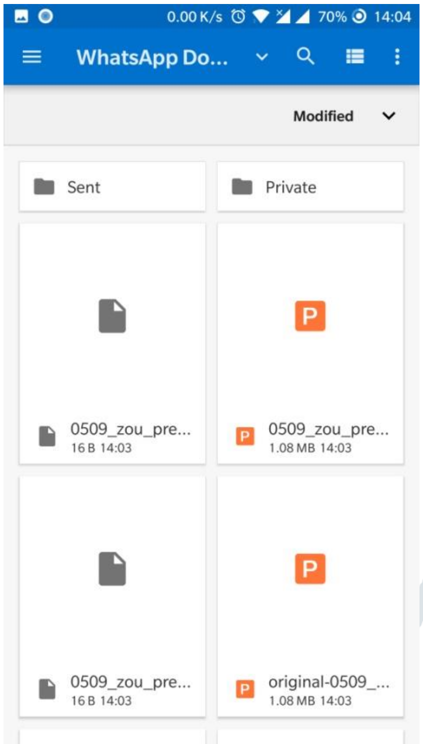
Results

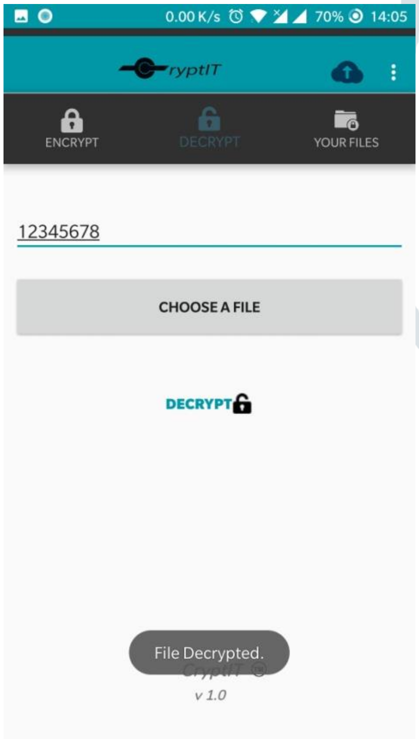


12345678

File Encrypted.

Fig4: Choosing a file to encrypt





12345678

File Decrypted.

Fig5: File is decrypted

Conclusion

The features exhibited by this application provide a user with exceptional performance with reference to securing his/her Phone's data or information in the form of files. This application will prove to be one of the most sophisticated software in the Smartphone era which will enable a user to seamlessly transfer their files from one place to another without the fear of the data being compromised by hackers or third parties while providing global availability towards their encrypted files.

This project shows successful encryption of files such as images, text, pdfs etc encryption as well as their decryption. The user experiences faster file encryption and decryption than traditional software and shows that the AES, Blowfish, and DES encryption and decryption algorithm when run in unison provide faster performance 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 developing a stronger encryption algorithm with high speed and less memory usage.

Future Scope

With the rapid pace at which technology and gadgets are increasing in the modern world, this application will serve a serious purpose to those who are looking to secure their data on-the-go and also several improvements to the current application such as addition of cloud services, extra security protection through fingerprint and biometrics, increase in the capabilities of the firebase, etc can be implemented in the upcoming versions of the current application.

This Application can also be integrated with several other features to enhance the overall stability and effectiveness of the current system and in the future can also see the addition of more and more encryption algorithms to choose from. That is, the users can choose the type of protection they need for specific files.

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.