International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Cryptography Encryption and Decryption File Protection Based On Mobile Bluetooth Proximity

Muthuramalingam B[1], N.S. Akshay Bharadwaj[2]

[1]*Assistant Professor, Department of Computer Application, Sir MVIT, Karnataka, Bangalore*
[2]*Student, Department of Computer Application, Sir MVIT, Karnataka, Bangalore*

Abstract - *In recent times, high growth in the field of networking technology leads to a practice of interchanging digital data frequently. The idea is to build a system, which uses an encryption algorithm to convert a file, which has meaningful information into data that cannot be read without decrypting. Therefore, if anyone tries to access a file present in the system, which is encrypted, the person gets junk data. The only way to access such file is by using a security key. The key which is used in our system is the bluetooth MAC address of a device that is registered with the system. The security key used for the system will be the file owner's smartphone or any other device which has bluetooth in it .*

***Key Words*: AES, Bluetooth MAC, Cryptography, Decryption, Encryption.**

1. INTRODUCTION

Cryptography provides various number of security goals to ensure data privacy. The idea of encryption and AES encryption algorithm by which one can encode the data in secret code and it is not readable by hackers or unauthorized person. The idea is to build a system, which uses an encryption algorithm to convert a file, which has meaningful information into data that cannot be read without decrypting it. The only way to access such file is by using a security key. The key that is used in the system is Bluetooth MAC address of a device that is registered with the system. Encryption Data security in wireless communication plays an important role because wireless communication is always used in online transmission. There are many cryptographic techniques available and among all AES is one of the most powerful technique.

2. LITERATURE REVIEW

2.1 Purpose of Cryptography

- Authentication: Authentication mechanism helps to establish proof of identities. This process ensures that the login credentials are correctly identified.
- Confidentiality: The principle of confidentiality specifies that only the sender and the respective recipient should be able to process the contents of a message.
- Availability: The principle of availability states that resources should be available only to authorized users.
- Access Control: Access Control specifies who can access the information.

2.2 Types of Cryptography

2.2.1 Secret Key Cryptography:

In this, same key is used for both encryption and decryption, Example of such algorithms are DES, Triple DES, AES, RC5 etc.

2.2.2 Public Key Cryptography:

In this two different keys are used, one key for encryption and another key for decryption, Example of such algorithms are RSA, Elliptic Curve and etc.

2.3 Cryptography

2.3.1 Plain Text:

Any communication that is used in the human language, takes the form of plain text. It is understood by the sender and the recipient and also by anyone who gets an access to that message.

2.3.2 Cipher Text:

Cipher means a code or a secret message. When a plain text is encoded using any suitable scheme, then the resulting message is called a cipher text.

2.3.3 Key:

An important aspect of performing encryption and decryption is the key. It is the key used for encryption and decryption that makes the process of cryptography secured.

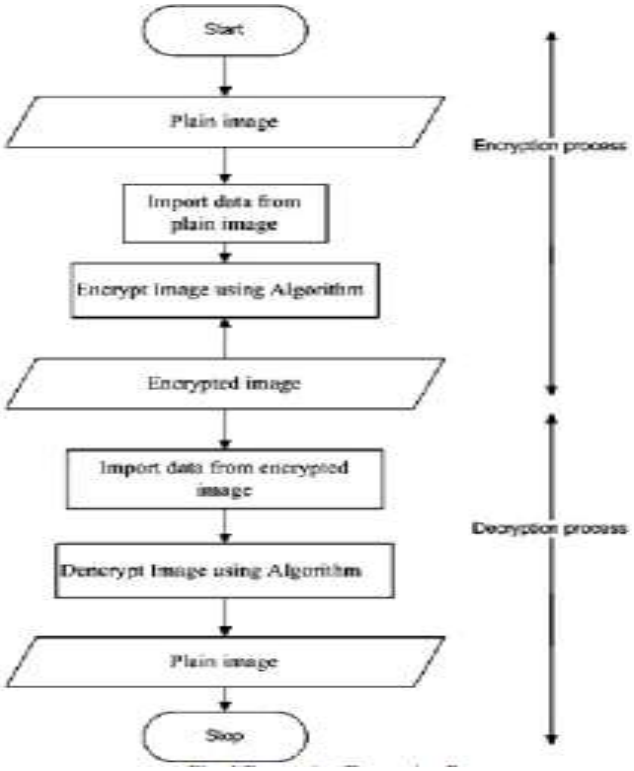

Fig-1: Encryption and Decryption Process

2.4 Bluecove

BlueCove is a Java library for Bluetooth (JSR-82 implementation) that currently interfaces with the Mac OS X, WIDCOMM, BlueSoleil and Microsoft Bluetooth stack found in Windows XP SP2 and above and WIDCOMM and Microsoft Bluetooth stack on Windows Mobile.

3. CLASSIFICATION OF CRYPTOGRAPHY

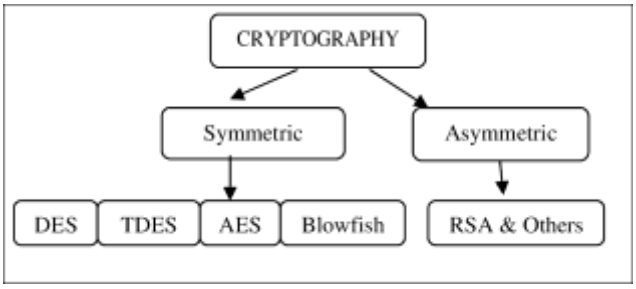

Fig-2: Classification of cryptography

3.1 Symmetric Cryptography:

- This type of cryptography uses a single key, which is used for encryption and decryption.
- The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. At the receiver side, same key will be used to decrypt the message and get the plaintext.
- Because there is common key used for encryption and decryption process, the secret key cryptography is also known as symmetric encryption.
- This was the only type of encryption method widely known until June 1976. There are various symmetric key algorithms such as DES, TRIPLE DES, AES and Blowfish.

3.2 Asymmetric Cryptography:

- Public-key cryptography, where key used to encrypt a message is differ from key used to decrypt a message.
- In asymmetric or public-key cryptography, there are two cryptographic keys: a private key and a public key are used.
- The private key is kept secret, while public key may be distributed. Messages are encrypted with recipients' public key and decrypted with private key.
- Asymmetric cryptography techniques are RSA (Rivest Shamir and Adleman), Diffie-Hellman, and DSA (Digital Signature Algorithm).
- A significant disadvantage of symmetric ciphers is the challenge in managing the key in a more secured manner.
- Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each cipher text exchanged as well.
- The number of keys required is directly propotional to the number of members in the network. This task is quite complex and challenging.

4. ALGORITHM

4.1 AES

- The most popular and widely used symmetric encryption algorithm is likely to be encountered as Advanced Encryption Standard (AES). AES on the other hand which encrypts all 128 bits in a single iteration.
- AES encryption is fast and flexible.
- It can be implemented on various platforms especially on small devices. It is the replacement for the Data Encryption Standard (DES) and to lesser degree of Triple DES.
- The specification called for a symmetric algorithm using block encryption of 128 bits in size. It also supports key sizes of 128, 192 and 256 bits.

4.2 Features of AES Algorithm

- Symmetric key - symmetric block cipher.
- Stronger and faster than Triple-DES.
- Provide full specification and design details.
- Implementation of AES is easy using C language and JAVA.

4.3 AES Encryption Process

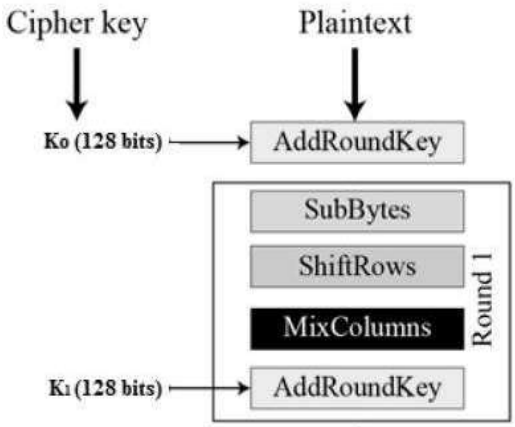

Fig-3: Encryption Process

4.3.1 Substituion Bytes:

The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

4.3.2 Shift Rows:

Process of shift rows is carried out as follows:

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

4.3.3 Mix Column:

Each column of four bytes is now transformed using a special mathematical function.

4.3.4 Add RoundKey:

The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext.

5. CONCLUSION

Cryptography plays an important role in increasing growth of digital data storage and communication. It is used to achieve the security goals like confidentiality, integrity, authentication, non-repudiation. It is analysed that in Diffie Hellman key exchange cryptography algorithm, secret keys are exchanged between two users. Whereas receiver in digital signature algorithm to verify that the signal received uses a digital signature is not altered. It is also concluded that all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Many new encryption techniques developing therefore fast and secure standard encryption techniques will always work out with high rate of security. Cryptography is used to ensure that the contents of a message are confidentiality transmitted and would not be altered. Confidentiality means nobody can understand the received message except the one that has the decipher key, and "data cannot be changed," means the original information would not be changed or modified.

6. REFERENCES

[1] Davis.R, "The Data Encryption Standard in Perspective", Proceeding of Communication Society magazine, IEEE, Vol 16, Nov 1978.

[2] Gurjeevan Singh, Ashwani Kumar Singla, K.S. Sandha "Performance Evaluation of Symmetric Cryptographic Algorithms", International Journal of Electronics and Communication Technology Vol 2 Issue 3, Sep 2011.

[3] Pratap Chandra Mandal "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, Sep 2012.

[4] E.Thmbiraja, G.Ramesh, Dr.R.Umarani, "A survey on various most common encryption techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 7, July 2012.

[5] ATUL KAHATE "CRYPTOGRAPHY AND NETWORK SECURITY", TATA MCGRAW-HILL COMPANIES, 2008.

[6] B.A. FOROUZAN, CRYPTOGRAPHY AND NETWORK SECURITY, INDIA: TATA MCGRAW HILL PUBLISHING COMPANY LIMITED, 2007.

[7] NehaTyagi, Ashish Agarwal, "Methods for Protection of Key in Private Key Cryptography", 2017 IEEE, ISSN: 2347-5552.

[8] E.THMBIRAJA, G.RAMESH, DR.R.UMARANI, "A SURVEY ON VARIOUS MOST COMMON ENCRYPTION TECHNIQUES", INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN COMPUTER SCIENCE AND SOFTWARE ENGINEERING, VOL 2, ISSUE 7, JULY 2012.

[9] MONIKA AGRAWAL, PRADEEP MISHRA", A COMPARATIVE SURVEY ON SYMMETRIC KEY ENCRYPTION TECHNIQUES", INTERNATIONAL JOURNAL ON COMPUTER SCIENCE AND ENGINEERING (IJCSE), VOL.4 MAY 2012.

[10] D. CROCKER, T. HANSEN, AND M. KUCHERAWY, DOMAIN KEYS IDENTIFIED MAIL (DKIM) SIGNATURES, TECHNICAL REPORT 6376, SEP 2011.

[11] D. EASTLAKE, DOMAIN NAME SYSTEM SECURITY EXTENSIONS, TECHNICAL REPORT RFC 2535, MAR 1990.

[12] B.A. FOROUZAN, CRYPTOGRAPHY AND NETWORK SECURITY, INDIA: TATA MCGRAW HILL PUBLISHING COMPANY LIMITED, 2007.