Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 293 – 298

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

A Novel Idea on Multimedia Encryption using Hybrid Crypto Approach

Sridhar C. Iyer[a,] , R.R. Sedamkar[b,] , Shiwani Gupta[c]

[ab,c] *Thakur College of Engg. and Tech., Mumbai -400101, Maharashtra, India*

Abstract

Data security is of utmost importance in today's world. Especially when the data is travelling through an insecure communication network. There are symmetric key encryption techniques which use only one key for both encryption and decryption of the data. They are simple in design but can be easily cracked using brute force attacks. The entire security of such a cipher could be compromised if the attacker anyhow gets access to the keys. On the other hand, there are asymmetric key based algorithms which use a pair of keys, one for encryption, and the other for decryption, whose security is higher as compared to the symmetric ones but lack in time efficiency. It is also difficult to manage such a huge base of key-pairs efficiently and safely. This paper mainly focusses on the implementation of a system capable of encryption and decryption of multimedia data (Text, Images, Videos, Audio etc.) using a hybrid model based on the amalgamation of symmetric encryption techniques such as AES and asymmetric techniques such as ECC. ECC is based on the toughness of the discrete logarithm problem (DLP), whose public key is short, network bandwidth is little and ability to resist to attack is strong which makes it really difficult to guess the keys. Even if the attacker gets access to any of the keys, he or she won't be in a position to decipher it in a relatively finite amount of man-years.

Keywords: ECC; Hybrid Encryption; Multimedia Encryption; Cryptography; Symmetric Encryption; Asymmetric Encryption

1. Introduction

There are a number of existing techniques such as cryptography, steganography, hashing, etc. which could provide security to the data. These techniques date back to hundreds of years where conventional techniques such as "Caesar Cipher" was used to scramble the contents of the message in order to make the confidential message unreadable or unrecognizable. With the advancements in modern technology and easy access to the internet, traditional methods such as the Caesar Cipher was not a huge bottleneck in front of cryptanalysts or adversaries who like to break into a system or message just for the sake of pride, enjoyment or fame.

*Corresponding author. *Email id* : c.sridhar89@gmail.com

doi:10.1016/j.procs.2016.03.038

The scope of this project mainly focusses on providing security to multimedia data such as images, text files, audio, video, etc. using a hybrid encryption technique composed of Advanced Encryption Standard (AES) and ECC/ECIES.
The hybrid encryption technique using a mixed encryption model based upon using the symmetric and asymmetric keys in tandem. The existing standards provide encryption to text files at a really good stand-off but they fail to provide the same security to multimedia data such as audio, video, images etc. Even if they try to achieve it using existing symmetric algorithms such as AES, DES etc., they become vulnerable to brute force attacks.

Hence a hybrid system is thought of which could provide the same security or even better using a hybrid of symmetric-asymmetric algorithms. ECC keys provide the same level of security with 160 bits as compared to RSA with 1024 bits length. Hence ECC is space efficient as compared to the existing algorithms and chosen for our research work as the asymmetric key provider.

2. History of Existing Techniques

An array of researches have been made in the field of cryptography and encryption. Symmetric encryption algorithm such as DES was used for a long time before its inherent limitations were started to be exploited. DES use a 56 bit key for encrypting the 64 bit plaintext to convert it into a 64 bit cipher-text. The small key length makes it a fairly simple and straightforward cipher to be broken into using brute force attacks.

These limitations were overcome using Triple DES (3DES) which use a pair of keys and does a triple encryption of the plaintext using 112 or 168 bit keys but the time it takes to complete the encryption is relatively higher as compared to simple DES. To overcome the limitations of DES, two Belgian cryptographers, Joan Daemon and Vincent Rijmen came up with a cryptographic standard proposal named as AES[1] or Rijndael cipher. It uses a single key of either 128,192 or 256 bit keys depending upon the number of rounds i.e either 10, 12 or 14 rounds respectively. AES broadly consists of substitution, shifting or rows, mixed columns transformations and adding a round key for each round except the last round to ultimately yield the corresponding cipher-text. The performance comparison of the existing techniques [2] show that although DES is faster as compared to AES, it lacks in terms of security which AES provides.

On the other hand, asymmetric key based encryption algorithms use a pair of keys; a public and a private key. These keys are mathematically bound to each other. The message is encrypted using the public key of the receiver and sent along the communication medium. The message is received by all the entities present in the network but only the person whose public key is matching with the one used for encryption can decrypt the same using his/her private key. The most popular asymmetric key based encryption technique till date is RSA [3]. It uses a 1024 bit key stream to share the information between the sender and the receiver. RSA solely depends upon large prime integer numbers and the discrete logarithm problem for the secrecy of the message.

RSA is really helpful for providing security to online transactions and highly confidential transactions over a network but has some inherent limitations as well. Boneh [4], in his research article has discussed the various attacks possible on an RSA cryptosystem. Timing attacks if planned well could be used to identify the timing between generation of encryption and decryption keys which can then subsequently be used to launch an attack on the system. In their paper "On the Power of Simple Branch Prediction Analysis"[5] the authors have claimed to have obtained 508 out of 512 bits of RSA in just 10 iterations. To overcome these problems, researchers came up with an advanced asymmetric encryption standard known as the “Elliptic Curve Cryptography(ECC)” which depends upon a relatively difficult and virtually unbreakable concept of the elliptic curve discrete logarithm problem(ECDLP) which makes the system unbreakable with commonly known or even sophisticated concepts of cryptanalysis. ECC and related concepts are discussed in the subsequent sections of this paper.

3. Problem Statement

Keeping all the inherent limitations of the existing technologies in mind and sensing the need of a better encryption model for multimedia data, in terms of security as well as time, a system is proposed, which addresses the problems such as:

- *Key Size*

The Symmetric ciphers use only a single key for encryption and decryption, hence the size of the key should be huge so that it cannot be easily guessed by any adversary using the brute force attacks. Asymmetric ciphers on the other hand use 2 keys for doing the same which impacts the memory adversely but provides better security.

- *Time Complexity*

Complex design methodologies add up to the time complexity and simple ones provide better time complexity at the cost of security. Hence a trade-off between the two needs to be established.

- *Memory Efficiency*

Text encryption systems offer a better memory efficiency as compared to multimedia encryption systems but lack in terms of variety, whereas multimedia encryption requires a lot of free memory space to store the keys, input files, ciphered files and the output files. Hence, again a trade-off between variety and memory needs to be established.

- *Types of Inputs supported*

All the literatures reviewed were all single functioned, i.e they all support encryption for text inputs directly from the user or in the form of files containing textual information or even text messages in the form of SMS's. When it comes to high requirement multimedia inputs such as images, audio, video, graphical contents, etc. such systems lack in performance because of issues such as high memory requirement and time required to encrypt/decrypt them.

4. Techniques used for Hybrid Crypto Approach

The proposed methodology uses a hybrid of the Advanced Encryption Standard and the Elliptic Curve Cryptography which are explained as follows:

- *Advanced Encryption Standard (A.E.S)*

The Advanced Encryption Standard was proposed as a suitable replacement of the existing Data Encryption Standard (DES). It is a block cipher which takes as input a 128 bit plaintext, which is subject to an encryption with 128 , 192 and 256 bit key depending upon the number of rounds i.e 10,12 or 14 respectively. AES is different in concept from DES i.e it is not based on the Feistel cipher.

Fig.1 explains the various internal rounds that take place for encryption and decryption using AES. It broadly consists of Substitution i.e bit by bit substitution, shifting of rows i.e transposition, mixing of columns based on modular arithmetic multiplication followed by adding of round key till n-1 rounds. Mix column round is omitted in the final n^{th} round. After the n^{th} round a 128 bit ciphertext is obtained.

- *Elliptic Curve Cryptography (E.C.C)*

The use of elliptic curves in public key cryptography was independently proposed by Koblitz [7] and Miller in 1985 and since then, an enormous amount of work has been done on elliptic curve cryptography. A general elliptic curve takes the general form as: [8]

$$E: y^2 = x^3 + ax + b \qquad \ldots\ldots.. \qquad (1)$$

Where x, y are elements of GF (p) and a, b are integer modulo p, satisfying

$$4a^3+27b^2 \neq 0(\text{mod } p) \quad (2)$$

The basic EC operations are point addition and point doubling. Simple multiplication could not be found in the case of elliptic curves. A single point suppose A(x,y) on the elliptic curve could yield a resultant point B(x',y') by following a series of point addition and point doubling instead of directly multiplying the point A with a scalar, hence A=zB , where z is a scalar multiple.

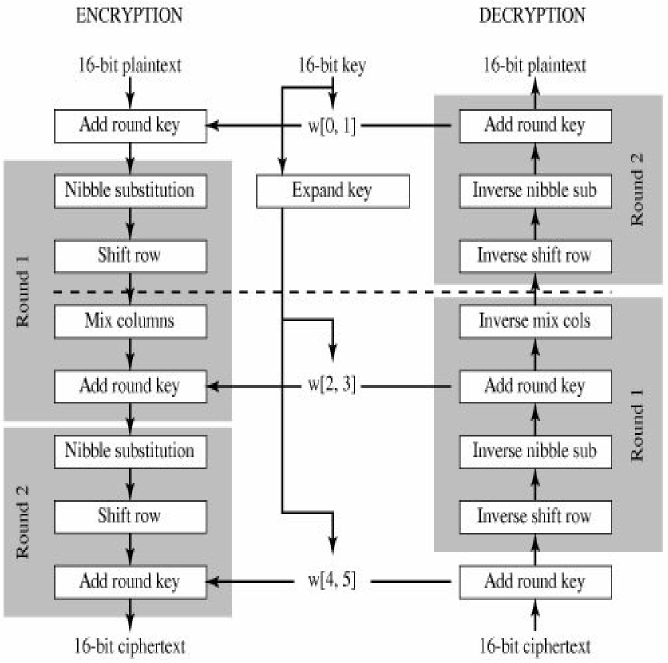

Fig 1. Advanced Encryption Standard [6]

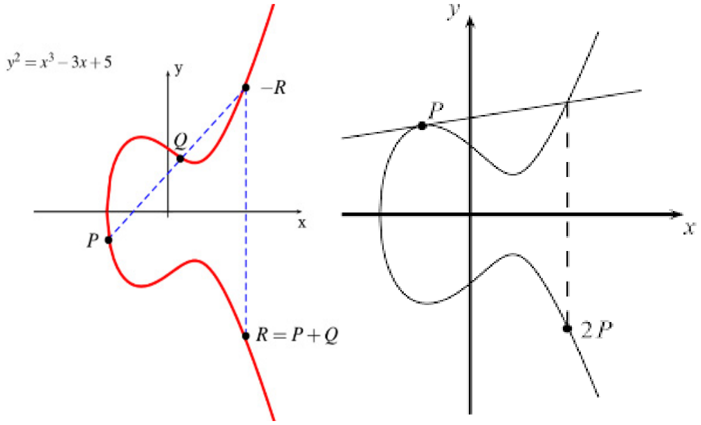

Fig 2. a) ECC Point Addition b) ECC Point Doubling

Fig 2.(a) and Fig 2.(b) show elliptic curve addition and doubling respectively. In Elliptic addition, a straight line joining the two points are allowed to fall on the curve in the x-y plane at point R. The negative equivalent is obtained on the other side of the plane to produce the final result. Similarly in point doubling, the point P itself is doubled by allowing a tangent on P to fall in the x-y plane and taking a negative intercept of the same.RSA had been the mainstay of PKC for over a quarter-century. ECC, however, is emerging as a replacement in some environments because it provides similar levels of security compared to RSA but with significantly reduced key sizes.[9,10,11]

5. Proposed Idea and Methodology

The hybrid encryption model makes use of two cipher technologies, AES and ECC. The proposed model is based upon the robustness of the ECDLP and the simplicity of AES. The system is intended to provide security to a variety of multimedia data ranging from text documents, images, audio, video etc. by first converting them into a base64 encoded version in text format. The same is then subjected to an initial encryption using AES, the keys for which are generated randomly. A QR code equivalent of the keys are generated in an image form which is then used by the system to extract the key in text form. This provides an extra level of security to the AES keys. For the second level of security, the AES keys are encrypted using ECC public key, the keys for which are generated from the input base64 encoded text file. The ECC key pairs are stored at designated file-system directories. The encrypted AES key is then further used to encrypt the base64 encoded plaintext to convert it into a corresponding ciphertext. The resultant ciphertext is already compressed and has undergone two levels of mixed encryption comprising of ECC and AES. Such a hybrid model of encryption provides a much better level of security as compared to a single model applied individually. The decryption process is exactly the reverse process involving a slightly complex methodology. The Methodology proposed in this research work is based on a hybrid system based on symmetric encryption using AES (128,192,256) and asymmetric encryption using ECC. The implementation is proposed using Java as the high level programming language. Java supports in built libraries to develop cryptographic implementations. There are many third party organisations and developer communities like Bouncy castle and Flexi provider which provide cryptographic extensions to develop projects.

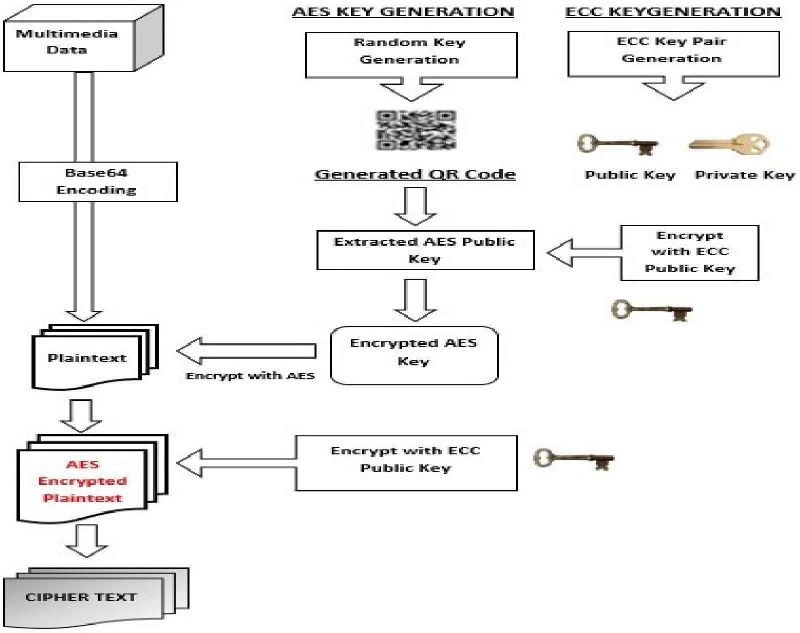

Fig 3. Proposed model of Encryption

Fig 3. shows the proposed methodology to be adopted for encrypting the multimedia data. The overall modules and operations are highlighted.

6. Expected Results

The research work focusses on encrypting the multimedia data i.e either audio, video, images, text, graphics, Pdf files etc. and storing them on the receiver's directory as an encrypted file. The receiver in turn uses his/her private key components to decipher the encrypted data back to its original form. The following directories and their respective contents as expected are as follows:

The overall expected results are as follows:

- Overall **Time** taken for encryption and decryption is expected to go up slightly as a mixed model of encryption will be used. Time taken is expected to range between Symmetric and Asymmetric ciphers.
- Overall **Space Complexity** for storing the encrypted files and source files is expected to be reduced as compression of multimedia files are done prior to encryption and keys used are of smaller size.
- **Security level** is expected to be high as compared to the existing systems as a hybrid of symmetric and asymmetric ciphers are used.

7. Conclusion

The research is done extensively to develop a hybrid system capable of encrypting and decrypting the sensitive data to protect it from unauthorized access and attacks. The various limitations of the existing systems were analyzed and a system capable of removing such limitations and providing novelties to the concept of encryption is proposed. This system will aim to provide better security in terms of key size to time ratio and improve the overall encryption process.

References

1. Daemen, Joan, Rijmen, Vincent. (March 9,*),*AES Proposal: Rijndael. *National Institute of Standards and Technology* 2003; p. 1. Retrieved 21 February 2013.

2. Jawahar Thakur, Nagesh Kumar. DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. *International Journal of Emerging Technology and Advanced Engineering* December 2011; vol 1(2), p.6-12.

3. R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.*Communications of the ACM* 1977; p. 120-126.

4. D. Boneh. Twenty Years of Attacks on the RSA. *Notices of the American Mathematical Society* 1999; vol 46(2),p.203–213.

5. O. Acıi cmez, C. Kaya Ko and J.P. Seifert, On the power of simple branch prediction analysis. *IACR Cryptology* 2006; ePrint Archive.

6. wikipedia.org,"Advanced Encryption Standard", https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

7. N.Koblitz, Elliptic Curve Cryptosystems. *Mathematics of Computation* 1987; volA8, p.203 -209.

8. S.M.Celestin ,V.K.Muneeswaran, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography. *IEEE International Conference on Advanced Computing* Dec 2009; p. 82-85.

9. Hafid Mammass and Fattehallah Ghadi, Implementation of Smartcard Personalization Software. *International Journal of Future Generation Communication and Networking* 2012; vol 5(4).p.39-54.

10. F. Amounas and E.H. El Kinani, A Novel Encryption Scheme of Amazigh Alphabet Based Elliptic Curve using Pauli Spin ½ Matrices. *International Journal of Information & Network Security (IJINS)* 2013; vol 2(3),p. 190-196.

11. Md.Zaheer Abbas, Dr.JVR Murthy, Authenticated And Policy - Compliant Source Routing. *International Journal of Engineering Research and Applications (IJERA)* 2012;vol 2(3),p.1347-1352.