An Extensive Review on Elliptic Curve Cryptography for Ciphering Images

Mansingh Mali[1], Prof. Kailash Patidar[2]

[1]Mtechscholar,[2]Guide & HOD

Department of Computer Science and Engineering, SSSIST, Sehore

Abstract - Cryptography is the science of hiding information which can be revealed only by legitimate users. It is used to ensure the secrecy of the transmitted data over an unsecure channel and prevent eavesdropping and data tampering. Another field called 'cryptanalysis' concerns with attacking and decrypting these ciphers[1]. Many cryptography schemes were proposed and used for securing data, some use the shared key cryptography, while some others use the public key cryptography (PKC). The shared key cryptography is a system which uses only one key by both sender and receiver for the purpose of encrypting and decrypting messages. On the other hand, public key cryptography uses two keys, namely private-key and public-key. To encrypt a message in the public key scheme, the public-key is used, while the private-key is used to decrypt it. Elliptic curves are algebraic curves which have been studied by many mathematicians for a long time. In 1985, Neal Koblitz (Koblitz 1987)and Victor Miller (Miller 1986)independently proposed the public key cryptosystems using elliptic curve. Since then, many researchers have spent years studying the strength of ECC and improving techniques for its implementation In this research we are presenting an extensive review on Ciphering Images using elliptic curve Cryptography technique.

Keywords – ciphering images, elliptic curve, encryption, decryption.

I. INTRODUCTION

Security for wireless communication devices has received increasing attention over the past few years. This is partially due to privacy issues, which might hamper the acceptance of wireless communication technology. A second reason is the applicability of wireless communication technology for online transaction purchases and mobile internet [1].

As compared to the shared key cryptography, the public key cryptography is rather slow. However, the public-key cryptography can be used with the shared key cryptography to get the best of both. In particular, the public key cryptography has many advantages over the shared key; among others, it increases the security and convenience where distributing the private key to other party is not required [6].

The Elliptic curve cryptosystem (ECC) provides a smaller and faster public key cryptosystem. In addition, the ECC is also a realistic and secured technology to be implemented in constrained applications, such as the RFID.

Generating curves to work as cryptographic curves must go through numerous algorithms and procedures so as to create a reliable cryptographic curve. An elliptic curve over a finite field F_q, where $q = p^m$, is supersingular if p divides t, where t is the trace of curve [1].

The ECC has been commercially accepted, and adopted by many standardizing bodies such as American National Standards Institute ANSI, Institute of Electrical and Electronics Engineers (IEEE), International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST). ANSI in their standard provides the needed algorithms to generate an elliptic curve and generating Elliptic Curve Digital Signature (ECDSA) signatures. It provides step-by-step examples to generate and verify ECDSA to differentiate key sizes[4].

A. Security Goals

Network Security is most important to provide security in a public network, because we place most critical information in this network. To provide security in public network we must consciously of the three primary goals of network security. These goals are:

- Confidentiality: Confidentiality ensures that data or information can't access by unauthorized users.
- Integrity: This primary goal of network security prevents unauthorized modification of data at the time of transmission.
- Availability: This goal ensures that network resources are always accessible to authorized parties when needed.

Message encryption and digital signature schemes are cryptographic tools for providing confidentiality, integrity, authentication, and non-repudiation.

Confidential can be achieved by encryption. Integrity, authentication and non-repudiation can be achieved by digital signature.

II. SYSTEM MODEL

A. Cryptography

Cryptography is based on hard mathematical problems like prime number factorization, Elliptic curve discrete logarithm problem and discrete logarithm problem. The idea behind these problems is the computation can be easily done in one direction, but it is very difficult in the opposite direction. It is not difficult to find the result of multiplying two numbers, but it is extremely challenging to find prime factors of a number. Thus, cryptography is concerned with the design and the analysis of mathematical techniques which can offer secure communications in the presence of malicious adversaries. It is an area which is concerned with the transformation of data for security reasons.

Before moving further, these are a number of terms which are commonly associated with cryptography:

Plaintext: The message which is transmitted to the recipient.

Encryption: The procedure of changing the content of a message in a way that it conceals the real message.

Ciphertext: The output which is produced after encrypting the plaintext.

Decryption: The reverse function of encryption. It is the process of retrieving the plaintext from the ciphertext.

B. Message Encryption

Encryption is the process of encoding messages that only authorized users can access it. In an encryption scheme, the message or information, known as plaintext, is encoding using an encryption algorithm, converted it into an unreadable ciphertext. This is generally done with the use of an key along with encryption algorithm. So, any adversary can't be able to settle anything about the original message. An authorized user, however, is capable of decode the ciphertext by using a decryption algorithm, that normally requires a secret decryption key, that adversaries do not have access to it. Cryptography has two way of an encryption process called symmetric key encryption and asymmetric key encryption or public key encryption is given below Figure 2.1(a) and Figure 2.1(b).

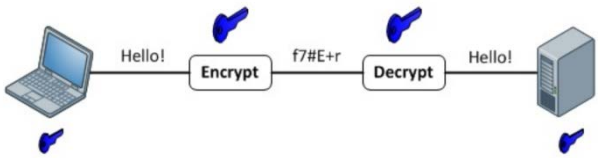

Figure 2.1 (a) Symmetric Key Encryption Process.

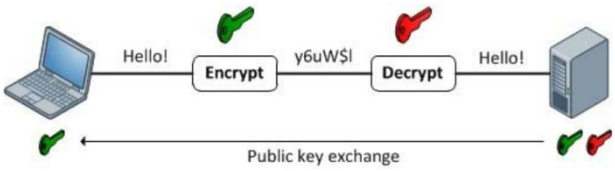

Figure 2.1(b) Asymmetric Key Encryption Process.

C. Elliptic Curve Cryptography (ECC)

Elliptic Curves have been studied by mathematicians for more than a century. One example is proving Fermat's Last Theorem which indicates that the equation $x + y = z^n$ has no non-zero integer solutions for x, y and z, in case that integer n is larger than 2. The elliptic curve was introduced in the cryptography field in 1986. It is quite a new cryptosystem, which was suggested separately by Miller (Miller 1986) and Koblitz (Koblitz 1987).

Nowadays, the ECC is adopted by many standardizing bodies such as ANSI (ANSIX9.62 1999), IEEE (IEEE-P1363-2000 2000), ISO (ISO/IEC15946 2002) and NIST (NIST 2000).

The elliptic curve cryptography system is based on Discrete Logarithm Problem (DLP). A group structure, provided by the elliptic curves and defined over a finite field, is used to implement the cryptographic schemes. The elements of the group are the rational points on the elliptic curve, together with a special point ϑ which is called as the point at infinity.

III. RELATED WORK

N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal,[1] The growing dire need for more and more secure systems has led researchers worldwide to discover and implement newer ways of encryption. Public key cryptography techniques are gaining worldwide popularity for their ease and better strength. With the rapid developments of the communication and applications of multimedia techniques in recent years lead the researchers to focuses on the security of digital data over the internet. This research has discussed the use of Elliptical Curve Cryptography for ciphering color images. ECC has been proved to score over RSA on the basis of its strength and

speed. This research used NIST Curves for ciphering color image.

B. Aissa, D. Nadir and M. Ammar,[2] This research treats the protection of images. We are dealing with the problem of image encryption and decryption. The encryption scheme is done by using the stream cipher system based on the nonlinear combination generator. The proposed keystream generator consists of fourteen binary primitive nonlinear feedback shift registers (NLFSRs) and one Boolean function. The Boolean function combines the output sequences of the fourteen NLFSRs to produce the keystream. All feedback shift registers employed in the keystream generator are primitive and nonlinear. The proposed encryption scheme is simple and highly efficient. Security analysis covers key sensitivity analysis, key space analysis, correlation coefficient analysis, noise analysis, statistical attacks, Berlekamp-Massey attack, correlation attack and algebraic attack. Based on experiment results and the security analysis it can be concluded that the proposed encryption scheme is highly key sensitive, highly resistance to the noises and shows a good resistance against brute-force, statistical attacks, Berlekamp-Massey attack, correlation attack and algebraic attack.

Ranjith Kumar R. and Saranraj B.[3] In this research image encryption algorithm based on confusion and diffusion using dynamic key space is proposed. Confusion of pixels is done by triangular confusion, method proposed in this work and diffusion is done by values obtained from logistic map iterations. An internal key generator is used to generate the initial seeds for the overall encryption scheme proposed, with these initial seeds, logistic map generates pseudo random numbers which are then converted into Confusion order (CO) for confusion. Confusion order is applied to the blocks which have undergone triangular confusion. The diffusion bits (DFB) are generated in parallel using the logistic map and manipulated with pixels confused according to confusion order. The image pixels are iteratively confused and diffused with CO and DFB respectively to produce cipher image in minimum number of rounds. This work focuses on key generation using logistic and tent maps with iterative reconstruction to secure the image. Chaos based method provides a dynamic changes for confusion and diffusion architecture in the image encryption. A single bit change in the key will dramatically change the result in the internal key generation structure proposed. The simulation results confirm that the satisfactory level security is achieved in three rounds and the overall encryption time is saved.

A. N. Borodzhieva and P. K. Manoilov,[4] The research describes an algorithm and developed MATLAB-based module with options for interactive e-learning for encryption/decryption of texts using bifid ciphers. It will be used in the course “Telecommunications Security”, included as compulsory in the curriculum of the specialty “Telecommunication Systems” for Bachelor degree at the University of Ruse. The application allows selecting the language and the parameters of the encryption/decryption key through menus. It illustrates step by step the process of encryption/decryption of the plain-text/cipher-text entered by the user, using bifid ciphers. The novelty is that the algorithm for encryption/decryption of texts in English using bifid ciphers is modified to be used for texts in Bulgarian, Russian and Romanian. The module has a possibility to display information on bifid ciphers and to illustrate the principle of its operation in a separate graphical window.

R. U. Ginting and R. Y. Dillak,[5] Doing a digital image transmission over internet need a secure protection againts ilegall copying. Unfortunately, many current data encryption methods such as DES, RSA, AES, and other only suitable for test data, but not for digital image. This research propose new secure algorithm for image encryption, which based on RC4 stream cipher algorithm and chaotic logistics map. The proposed algorithm works as follows: (i0 converting the external key into initial value, (ii) using he initial value to generate a key stream using chaotic logistic map function, and (iii) processing a permutation and the result is then XOR-ed with bytes stream of digital image. The experiment results show that the proposed algorithm (i) is able to make the cipher-image can not be visually identified, (ii) can eliminate the statistical correlation between the plain-image and cipher-image, (iii) is very sensitive to small changes of key, and (iv) has no change in image contents (lossless encryption) during encryption and decryption process which is indicated by the hash value (MD5) of plain-image has the same hash value (MD5) wth decrypted image.

M. Savari, M. Montazerolzohour and Y. E. Thiam,[6] The main role of encryption algorithms is to keep devises safe from attack. Using the best and more efficient algorithm for a device according to its storage and amount of data transfer is the most important part. This research compares Elliptical Curve Cryptography algorithm (ECC) with RSA algorithm on a multipurpose smart card. There are three applications in our multipurpose smart card which is named health, credit and passport card. ECC is compared with 160 bit key size and RSA with 1024 bit key size. The result of comparison is described in the final section.

IV. PROBLEM STATEMENT

The ECC applications produce their private keys using a secured random key generator, to increase the security and make use of the biometric features by generating private keys and producing Elliptic Curve domain parameters the elliptic curve used to generate the curve against the cryptanalysis. The cryptography process used to generate intended elliptic curve parameters which can be used to different Elliptic Curve Digital Signature Algorithm (ECDSA) like applications.

V. CONCLUSION

Elliptic curve cryptosystem (ECC) have recently received significant attention by research due to their low computational and communicational overhead. Elliptic curve cryptography (ECC) is the hardest computational problems the elliptic curve discrete logarithm problem and elliptic curve Deffie-Hellman problem are the most reliable cryptographic technique in ECC. The advantages of ECC that it requires shorter key length compared to other public-key algorithms. The security properties with a saving in computational cost compared to the traditional signature the encryption scheme which makes the new scheme more appropriate for environment with limited power.

REFERENCES

[1] N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal, "Elliptic Curve Cryptography for ciphering images," 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), Visakhapatnam, 2015, pp. 1-4.).

[2] B. Aissa, D. Nadir and M. Ammar, "An approach using stream cipher algorithm for image encryption and decryption," 2014 15th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA), Hammamet, 2014, pp. 498-503.

[3] Ranjith Kumar R. and Saranraj B., "A novel chaotic color image encryption / decryption based on triangular confusion," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, 2014, pp. 94-100.

[4] A.N. Borodzhieva and P. K. Manoilov, "MATLAB-based module for encryption and decryption using bifid ciphers applied in cryptosystems," 2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME), Bucharest, 2014, pp. 287-291.

[5] R. U. Ginting and R. Y. Dillak, "Digital color image encryption using RC4 stream cipher and chaotic logistic map," 2013 International Conference on Information Technology and Electrical Engineering (ICITEE), Yogyakarta, 2013, pp. 101-105.

[6] (M. Savari, M. Montazerolzohour and Y. E. Thiam, "Comparison of ECC and RSA algorithm in multipurpose smart card application," Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), Kuala Lumpur, 2012, pp. 49-53.

[7] Padma Bh, D.Chandravathi, P.prapoorna Roja: “Encoding and decoding Of a message in the implementation of Elliptic Curve Cryptography using Koblitz Method”. International Journal on Computer Science and Engineering (IJCSE) Vol. 02, No. 05, 2010, 1904-1907

[8] Hankerson, Menezes, Vanstone. “Guide to elliptic curve cryptography”

[9] Springer, 2004 ISBN 038795273X 332s_CsCr

[10] http://www.nsa.gov/business/programs/elliptic_curve.shtml

[11] Kamlesh Gupta1, Sanjay Silakari, “ECC over RSA for Asymmetric Encryption: A Review” http://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/2/

[12] http://www.nsa.gov/business/programs/elliptic_curve.shtml

[13] Santoshi Ketan Pote, Usha Mittal “Elliptic Curve Cryptographic Algorithm”

[14] Christof Paar, Jan Pelzl /’Understanding Cryptography”