An Extensive Review on Elliptic Curve Cryptography for Ciphering Images

Sakshi Shrivastava[1], Prof. Lokesh Malviya[2]

[1]*M. Tech. Scholar,* [2]*Research Guide*

Department of Computer Science Engineering, SAM College of Engineering, Bhopal

Abstract- Cryptography is the area of mathematics that disguises the information or data of communications. The purpose of cryptography is to secure the message between two persons so another person or adversary cannot understand the enciphered message. Only the recipient can decipher the message. For instance, military, government and diplomatic communications are suitable applications for cryptography. The growing dire need for more and more secure systems has led researchers worldwide to discover and implement newer ways of encryption. In this review we have studied analyze the use of Elliptical Curve Cryptography for ciphering color images. The objective of this research is to compare the encryption and decryption between the RSA cryptosystem and elliptic curve cryptography techniques.

Keywords- Encryption, Elliptic Curve Cryptography, decryption, RSA, NIST.

I. INTRODUCTION

The Handbook of Applied Cryptography [MvOV01] defines cryptography as the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication and data origin authentication. It further stipulates that cryptography is not the only means of providing information security, but rather a set of techniques.

Information security and cryptography are interwoven with antics of three entities: Alice, Bob and Eve. It seems impossible to detail the concepts of information security without these three and it would be a stark omission not to mention them here.

Alice and Bob want to talk. They usually do so over an insecure communications channel and depending on the details of the scenario with optional high background noise.

Specifically Alice and Bob want to

- talk in private, without being overheard
- be certain that what they hear is what the other said, and not garbled by background noise
- know for sure that Alice is Alice and Bob is Bob and not someone else
- ascertain that what one hears originated with the other party and not some hidden ventriloquist

Eve on the other hand wants to listen in, mutilate the content of the communication between Alice and Bob, alternatively impersonate Alice or Bob and intersperse bogus messages that the recipient beliefs have originated with the authorized conversation partner.

Eve is very powerful and it is generally understood that she is has full access to the communication channel used by Alice and Bob. Thus, she is capable to perform the above mentioned malicious actions. The goal of cryptography is to prevent Eve from doing so in spite of her facilities.

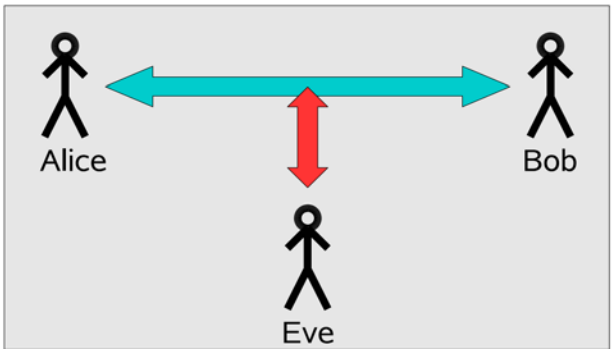

Figure 1.1 Alice, Bob and Eve example of cryptography.

Although there has been some speculation on the nature of Alice, Bob and Eve [Gor84], introducing them as entities was deliberate. In the following considerations they represent actors in a communication scenario. This of course encompasses flesh and blood people but also their virtual agents in today's in-formation networks. Alice might be a human who wants to communicate with Bob, but could as well be a smart card authenticating itself to an ATM or an Email application sending a message. Alice et al. will consequently help to provide descriptive examples for the aspects of information security.

Goals of Cryptography

- Confidentiality

Concerns itself with the protection of data from eavesdropping by illicit third parties. One way to achieve this is to use encryption. Alice

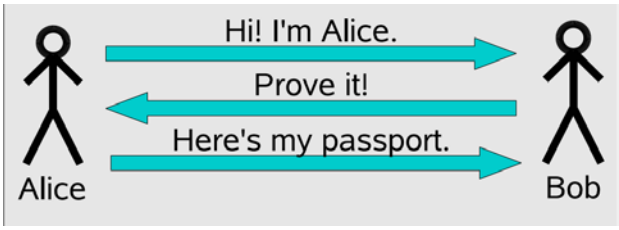

Figure 1.2: Bob challenges Alice

Encrypts a message before she sends it to Bob. Even if Eve intercepts the data, without knowledge on how to decrypt it will be impossible for her to discover its contents. Bob on the other hand has this additional knowledge and thus has access to the content of the message.

- Data integrity

Tries to protect the content of messages against accidental or unauthorized modification. Eve might not just be content with reading messages passed between Alice and Bob, she could go a step further and try to alter the data with malicious intend. Multiply Accumulate (MAC) are the cryptographic tools of choice to achieve this goal.

- Entity authentication

Has the goal to ascertain the identity of one party to another. In information security it is important to differentiate between identification and authentication. The difference is best explained by an example:

Alice and Bob meet. If Alice claims to be Alice to Bob she identifies herself. To authenticate herself to Bob she needs corroborating evidence. In this example Alice could show adequate photo identification, issued by a third party that Bob trusts.

The corresponding attack by Eve is impersonation, whereas Eve attempts to persuade Alice or Bob that she is the respective other. The cryptographic counter approach is to use challenge-response authentication protocols. Confer to figure 1.2 for a simple illustration of the concept.

- Data origin authentication

Ensures that a message originates from the claimant source. If Eve is not capable of impersonating an authorized communication party, she might be able to intersperse messages into the communication, that the recipient beliefs to have originated from a valid source. Eve could send information to Bob claiming that it originated from Alice. Cryptography applies a technique called keyed-hash functions to combat this hazard.

II. SYSTEM MODEL

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 0 which is called as the point at infinity.

The elliptic curve applications are by default using secure random generator to generate the seed which will be used to produce either the curve or the private key. This generated random number is not fully secured, where the cryptanalysts may exploit it. One alternative is using the random class, which is not secured but faster in generating the seed. Similarly, iris can be considered as an alternative to secureRandom function which is used to produce random seeds. secureRandom is a method being used in many algorithms that require unpredictable seed such as DSA and RSA.

A. Elliptic Curve over Finite Fields

The Elliptic curve cryptography calculations are based on finite fields. Deciding the Elliptic curve equation, which will calculate the points, is dependent on the selected underlying field. We studied two fields (prime, binary) with the needed operations over each field using affine coordinates.

B. Elliptic Curve Parameter

The implementation of an elliptic curve cryptosystem demands on a number of considerations on three different levels (finite field, ECC level, protocol level) of the implementation. Depending on the fundamental hardware and the targets, those are needed to be accomplished.

At the field level, selecting the fundamental field (binary, prime) and the representation which the field follows, as well as the algorithms to be used in this level.

At the elliptic curve level, affine coordinates are used with the appropriate algorithms to calculate the point addition and point doubling. The design was built to issue the ECDSA signature on the protocol level and the scalar multiplication, using the most significant bit (MSB), is used.

III. LITERATURE REVIEW

N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal,[1] The developing desperate requirement for more secure

systems has driven scientists worldwide to find and actualize more current methods for encryption. Public key cryptography procedures are increasing overall ubiquity for their straightforwardness and better quality. With the fast improvements of the communication and utilizations of media systems as of late lead the analysts to concentrates on the security of advanced data over the web. In this exploration author have talked about the utilization of Elliptical Curve Cryptography for Ciphering color images. ECC has been demonstrated to score over RSA on the premise of its quality and speed. utilized NIST Curves for Ciphering color image.

M. A. S. Eldeen, A. A. Elkouny and S. Elramly,[2] The Data Encryption Standard (DES) was an across the board symmetric key piece Cipher Algorithm. It was the most well known utilized cryptographic scheme. DES's security was an exceedingly disagreeable and dubious viewpoint until it turned into an uncertain calculation in 1999. In this exploration, an adjustment that beats the security issue of the DES calculation is presented. The improvement is relying upon the specialty of the Elliptic Curve Cryptography (ECC). The ECC approach is additionally used to accomplish the required key era and dissemination to set up a communication session. Our new ECC-based DES calculation can be connected to any record organizes, in this research it is utilized to scramble and decode an image document. Exploratory outcomes are completed with definite investigations, the outcomes show that the proposed plot has a vast key space to oppose the animal compel assault and it is exceptionally invulnerable to measurable assaults. The received data demonstrate that the ECC-based DES Algorithm could be utilized as an exceedingly secure algorithm.

S. Sowmya and S. V. Sathyanarayana ,[3] As of not long ago, Cryptography has been of intrigue essentially to the military and strategic groups. Be that as it may, the unfolding of the data age has uncovered a pressing requirement for cryptography in the private division as well. Cryptography is the investigation of strategies for guaranteeing the mystery and confirmation of the data. cyclic elliptic bend of the shape y2 = x3 + hatchet + b,a,b ∈ GF(p) with request M is considered and key Sequences are gotten from irregular grouping of cyclic elliptic Curve focuses. Elliptic Curve is a cubic condition in two factors, x and y, with coefficients from a field fulfilling certain conditions. For cryptographic applications the coefficients are browsed limited fields. A point on the Elliptic bend is a couple of (x,y) which fulfills the Elliptic curve condition. The aggregate number of focuses (x,y) which fulfill the elliptic curve condition alongside x=∞,y=∞ is known as the Order of the curve`M'. The slightest number N for which NP is equivalent to point at interminability O is called request of the pointP. Elliptic curves for which there exists a point P having a similar request N, as that of the bend M are called cyclic elliptic curves. A pseudorandom clustering generator in light of confused capacity and Elliptic Curve number organize over GF(p) is proposed here. The calculated Map is utilized as a disorderly capacity which creates an arbitrary grouping of genuine numbers. This irregular genuine grouping is changed over to binary which drives an Elliptic Curve number organize module producing an arbitrary succession of Elliptic Curve focuses. The grouping of focuses {P,2P,...,NP} is computed from a base point P, and put away in a document. Each component in this grouping is a point on the cyclic elliptic curve. The Chaotic binary succession chooses x or y-directions of elliptic bend focuses, pre-registered and put away. This structures an arbitrary whole number grouping. The arbitrariness properties of this succession have been tried utilizing different strategies like, autocor-joy dissemination, crosscorrelation circulation and first return outline. It is watched that the succession created fulfills the required haphazardness properties. These arrangements discover applications in Stream Cipher Systems. An added substance Stream Cipher system is outlined utilizing this succession as the key arrangement to scramble images. Aftereffects of image encryption and decoding for a restorative image are talked about and broke down in this research. The outcomes are additionally contrasted and the plan proposed by Lap-Piu Lee and Kwok-Wo Wong . The security examination of the proposed system is likewise talked about. It is intriguing to watch that, proposed calculation is better thought about than Lap-Piu Lee plan .

A. Baheti, L. Singh and A. U. Khan, [4] as multimedia applications is utilized progressively; security turns into a critical issue of security of images. The mix of clamorous hypothesis and cryptography shapes an imperative field of data security. In the previous decade, bedlam based image encryption is given much consideration in the exploration of data security and a great deal of image encryption calculations in light of disorderly maps have been proposed. However, the majority of them postpones the system execution, security, and experiences the ill effects of the little key space issue. This exploration presents an effective symmetric encryption conspire in light of a cyclic elliptic bend and turbulent system that can defeat these hindrances. The Cipher encodes 256-piece of plain image to 256-piece of Cipher image inside eight 32-bit registers. The plan creates pseudorandom bit successions for round keys in view of a piecewise nonlinear tumultuous guide. At that point, the produced arrangements are blended with the key successions got from the cyclic elliptic bend focuses. The proposed calculation has great encryption impact, substantial key space, and high affectability too

little change in mystery keys and quick contrasted with other focused algorithms.

S. Maria Celestin Vigila and K. Muneeswaran,[5] With the blast of systems and the tremendous measure of data transmitted along, securing data substance is turning out to be increasingly vital. Data encryption is generally used to guarantee security in open systems, for instance, the web. This exploration displays the utilization of stream Cipher, where the key stream is created in perspective of the properties of Linear Feedback Shift Register and cyclic Elliptic Curve over a constrained prime field. the procedure of encryption/unscrambling of an image in spatial space furthermore scramble key record parameters required for creating the key stream to different gatherings utilizing Elliptic Curve Cryptography. Hence the scrambled key record parameters are just transmitted and not the whole full length key. Since Elliptic Curve Cryptography is swapping RSA for key trade and Elliptic Curve based stream Cipher offers a decent decision for encryption progressively application. The quality of the proposed Cipher lies in the era of arbitrary succession utilizing Linear Feedback Shift Register over GF(p), trouble of Elliptic Curve Discrete Logarithmic Problem and the whole key need not be transmitted in the encryption procedure. This exploration likewise talks about the security parts of the proposed Cipher which is secure against a wide range of assaults.

K. Gupta, S. Silakari, R. Gupta and S. A. Khan, [6] in the improvement of 3G devices, all components of mixed media (content image sound and video) is utilized. To utilize this data, a channel of high transmission capacity and more secured system is required. In this period, arrange security has turned into an issue of significance, on which parcel of research is going on. We have proposed image encryption technique utilizing elliptic bend cryptography (ECC). RSA is too easing back contrasted with ECC since ECC required littler key size. In this strategy, each pixel of the first image is transformed into the elliptic bend point (Xm,Ym), these elliptic bend point change over into Cipher image pixel. The subsequent system gives relatively little square size, fast and high security.

IV. PROBLEM IDENTIFICATION

The ECC applications produce their private keys using a secured random key generator. In addition, it also uses a randomly generated seed to produce the curve domain parameters. This generates random number where cryptanalysts may exploit it. This also creates the need to have an alternative way to make the seed used in producing the private key and the curve domain parameters difficulty to acquire or counterfeit it. Instead of the random generator,

V. CONCLUSION

Elliptic curve cryptography provides a methodology for obtaining high-speed, efficient, and scalable implementations of a messaging system. In this research, have review in detail the working and implementation of elliptic curve cryptographic technique. The methodology for this research work is a software based development of system offering the features appropriate to the secure messaging system. These functions are then integrated and results are analyzed primarily for the offered speed and security. Using a different hardware to regenerate the results again of the secure ECC messaging application then results may vary according to the hardware configuration.

REFERENCES

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

[2] M. A. S. Eldeen, A. A. Elkouny and S. Elramly, "DES algorithm security fortification using Elliptic Curve Cryptography," 2015 Tenth International Conference on Computer Engineering & Systems (ICCES), Cairo, 2015, pp. 335-340.

[3] Sowmya and S. V. Sathyanarayana, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)," 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, 2014, pp. 1345-1350.

[4] Baheti, L. Singh and A. U. Khan, "Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network," 2014 Fourth International Conference on Communication Systems and Network Technologies, Bhopal, 2014, pp. 664-668.

[5] S. Maria Celestin Vigila and K. Muneeswaran, "Elliptic curve based key generation for symmetric encryption," 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies, Thuckafay, 2011, pp. 824-829.

[6] K. Gupta, S. Silakari, R. Gupta and S. A. Khan, "An Ethical Way of Image Encryption Using ECC," 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, Indore, 2009, pp. 342-345.

[7] Maryam Savari and Yeoh Eng Thiam, “Comparison of ECC and RSA in Multipurpose Smart Card Application”.

[8] Elsayed Mohammed and A.E Emarah and Kh.El-Shenawwey, "Elliptic Curve Cyrptosystems on Smart Cards".

[9] 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

[10] Hankerson, Menezes, Vanstone. "Guide to elliptic curve cryptography" Springer, 2004 ISBN 038795273X 332s_CsCr