Analysis and Implementation of Combined Approach of RSA and ECC Algorithm for Enhanced Data Security

Vaibhav Bhujade
Mtech Student
IET Alwar

Deepak Chaudhary
Asst. Profrssor
IET, Alwar

ABSTRACT
Cryptography is one of the important and useful technique in which usually a particular file is converted into unreadable format by using public key and private key system called as public key cryptosystem. Then as per the user requirement that file is send to another user for secure data or file transmission between original sender and receiver. In this transmission file of unreadable format is send, after receiving this file receiver used the similar algorithm technique and private key for getting the original file data. In this procedure various algorithms are used as a processing function and depending on that algorithm, used the private key. The power or strength of any algorithm is depending on the secret key used in sender client and receiver side client. For this type of secure transmission we traditionally used RSA algorithm which is more secure for use so most of the system used the same type of algorithm for secure way of communication. Even most of the financial transaction is done by the use of this algorithm as it used the strong key while encryption and decryption. But In today's new digital world there is a numerous growth in the use of the Internet service. Behind every software generator there is lots of hacker present. So, very little amount of time will be enough to explore the security. Hence we require more strong and complex algorithms, which provide the security the Internet work of transmitting and receiving. So this proposed system enhanced the security of existing RSA algorithm by using elliptical curve cryptography (ECC) algorithm. This system secures the important data of the administrator and safely sends to the registered user by text encryption and image encryption. Also proposed system provide good authentication for the user.

Keywords
Cryptography, Authentication, Plain Text, cipher text, RSA, ECC

1. INTRODUCTION
Cryptography is one of the scientific techniques in information security. The word cryptography is derived from the Greek word kryptos, it means hidden thing [1]. Cryptography is very similar to both the disciplines of cryptology and cryptanalysis. This cryptography includes various techniques which involve in hiding any kind of info in storage unit or transmit the data through various ways. However in this computer specific world cryptography is related with the scrambling the normal text which is available in readable form called plaintext into unreadable text called cipher text this process is known to be encryption procedure and the process which is exact oppose of this process used to recover the normal text known as process of decryption and the persons who used this techniques called as cryptographers [2] [3].

Current cryptography worries itself with the following four things:

1.Confidentiality : Student grade information of college or school is the thing which is very important as per their point of view and its confidentiality is also a serious issue. In the country like United States publication this important information is controlled by Family Educational Rights and Privacy Act (FERPA). This student personal and confidential information should be available to the students, their parents and the staff who required such data for their own job only. Enrolled student information will be of specific confidentiality ranking. As FERPA is available to control this information about the students, but still this information is view by many people regularly and there may be possible damaging by using this information. Many time the information like various list that may be list of students, list of faculties or any departmental important lists are assigned as a low confidential rating in worst no rating in some cases. This data is easily available on the college or organization website to the public [4].

2. Integrity: Many examples can be given which explain several aspects of the term integrity like medical information about any person stored in the database of that hospital. The doctor must trust all the information kept in the database that it is correct and current. But on the other hand if any person (e.g., a nurse) who have right to see, view and update the information about any patient in database and that person use this to harm the hospital. The database of that hospital must be restored properly and this restoration must be trustable, also this error or mistake needs to be traceable by the responsible person. Patient sensitive data or information is a good example of high level requirement for integrity. Wrong information about the patient may result in harm or death to him and also for that hospital liability [4].

Let us take an example of one of the asset in which a website offer a forum or blog for discussion on any current issue or topic to only the user who are authorized or who are previously registered and verified by the administrator. So in this case a registered user or any hacker might modify or entered some entries on his behalf. If this type of forum exist and used only for the pleasure of the registered user, no used to generate any revenue through this discussion and not that much important for research then there is no major problem in this type of cases but the administrator who manage all this things will experience little loss in terms of financial and time only.

Also one case of low integrity is online poll on any specific website. Several websites such as news websites offer this type of poll for their user that may be recorded or not with low level security so we cannot believe on the accuracy of such type of poll for any type of analysis on any topic or current issue.

3 Non-repudiation: The technical term non-repudiation of beginning denotes a service whereby the recipient is given

guarantee of the message's authenticity, in the sense that the receiver can subsequently prove to a third party that the message is trustworthy even if its originator subsequently revokes it. This term is used to avoid the transmitter and recipient form rejecting the transmitted message that this message is sending from them only. So in this case after sending the message, the one user called recipient can prove that suspected transmitter send the message with the proof of sending which is available in sent block. Also on the another side when a message is reached to the destination, the sender can easily show that the suspected recipient received the sent message which is normally present in the inbox section so no one deny for the same [5][3].

4 Authentication In many environments, it is more essential that transmission be authenticated rather than encrypted. That is, both parties should be convinced of each other's identity. We need to establish identity and verify identity before allowing access to resources. There are three methods we can use to authenticate someone:

- Use something you have, for example, a key or a card. The problem is that these can be stolen.
- Use something you know. Passwords and PINs (personal ID numbers) fall into these categories. These can be guessed, shared, and stolen by snooping.
- Use something you are. This involves biometrics. For example, a system may examine a user's fingerprint or iris pattern. In general, these types of systems require various types of hardware, can be costly, and are imprecise.

Authentication methods can be collective to toughen the confirmation. Using a single one of these methods is known as one-factor authentication. Using two techniques is two-factor authentication. Withdrawing cash at an ATM machine is an example of two factor authentication. To authenticate, you present the ATM card (something you have) and enter PIN (something you know). Most of the operating systems maintain a notion of a user identifier (user ID) which is a unique token that identifies each user on a system. Typically, systems employ a user name (a unique alphanumeric string that a user may use to identify himself / herself to the system) as well as well as a numeric user ID. The system uses the user ID to store and verify access permissions.

The most frequently used way of authentication is with a simple password authentication scheme. The system prompts us for a user name and then for a password. It then looks up the name in a password table and sees if the passwords match. This is known as a reusable password since the similar password is used for each login. One major weakness here is that if any unauthorized person try and finally manages to break into the system and in this way that person can steal the entire password file [6].

2. RELATED WORK

S. Maria Celestin Vigila1 proposes an Elliptic Curve (EC) based key stream generator that makes use of the basic operations in Elliptic Curve Cryptography (ECC).In 1985 elliptic curve was proposed by Koblitz and Miller, making its utilization in public key cryptography therefore, a huge amount of effort put on elliptic curve cryptography. ECC provides more security level which is obtained by small key rather than existing methods as that are depend on finding solution on discrete logarithm over integers or integer factorization. Elliptic curve cryptography algorithm utilizes elliptic curves. In elliptic curve every entity is bounded not only by variables but also by coefficient. For improving the security level of stream cipher using key stream generator which is based on elliptic curve of propose system. [7]

Muhammad Hammad Ahmed Implementation presented in this paper chooses ECC based authentication technique and its focus is moving towards the key size of 160 bits as it deals with strong security strength which can also be used for large period of time. In 1980's Miller and Koblitz proposed Elliptic curve (EC) cryptography. Elliptic curve cryptosystem is based on the concept of Galois Field (GF) which can be defined over a prime field (i.e. GF (p)) or over polynomial field (i.e. GF (2'")) [8][9]. Each and every types of field have its own merits and demerits. Polynomial field has advantages in hardware while the field over prime numbers has advantages in software. In selection of field one has to focus on efficient hardware implementation for constrained devices [10] [11].

3. PROBLEM STATEMENT

Due to the different number of problems versions and minor variations within these, the paper set out the particular problem that the paper is addressing. The problem is the secure data accessing for the client are not available to the other users. Various technique is implemented in this area but some having limitation regarding to security, limitation regarding file format.

In this paper, couple of algorithm is used that is RSA and Elliptical curve cryptography for convincing security and these both algorithms has their own security standard. So the security issue will be solved and this proposed system can used for the image so more useful as compare to previous system. Also this system provide better authentication technique for every registered user so security on individual level also increased because whenever any user want to access the secured data from the administrator, admin firstly verify that user then allowed by providing a different key so only the confirmed register user will get the access of required data.

Here the paper propose the combination of two well-known algorithm to provide good security for data which has to be kept secret and better authentication technique for every user who is already register on this proposed system to access the secret data.

Objective

Before initiating this paper, substantial amount of time has been spent to study algorithms correlated to cryptography and arriving to a deduction that there exists an ample scope to simplify/improve/enhance/redevelop/redesign/rearrange these methods.

Objectives of this work are:

i. To arrange the algorithm which offers more security to the stored data on server side.

ii. To provide the enhanced security by image file to transmit the message safely to the system user.

iii. To provide better authentication technique for the each registered user more individual level security.

The basic cryptographic algorithm RSA is known to everywhere, it is proficient and trustworthy too. But as it is used in everywhere so there may issue of cracking this algorithm. So our system is using the advantages of RSA but also this system enhanced this security by using elliptical curve cryptography. This combined approach of both algorithms provides better security mechanism.

Also this system provide the server client mechanism in which the file uploaded on the server side can also be downloaded by the client who is successfully register on this system. So when any client needs to access any file on server side, client will request to download that file. If server finds that requested client is authorized and permit table then server gives the access of that file by providing the secret key to the requested client. Then client can easily download the required file by using the server generated secret key. The previous system are developed for the document file of image file with single algorithm who is not that much secure. But this system is based on the combined approach on both algorithm and also offers the service not only for the document but also for image file.

4. OVERVIEW OF PROPOSED APPROACH

The offered system is a combine approach of two most secure algorithms that are globally accepted for the security as well as for accuracy in work. These are RSA and elliptical curve cryptography. RSA is well known algorithm used globally. RSA implements both i.e., a public-key cryptography and digital signatures. RSA is inspired by the published works of Diffee and Hellman from several years before, who designated the idea of such an algorithm, but never actually industrialized it. Announced at the time when the period of electronic email was estimated to rapidly arise.

transactions. Recently, a challenging system that has arisen is elliptic curve cryptosystem (ECC).

The resultant system in paper is most secure as compare to previous developed system as this paper using the power of both the algorithm. In this system first of all the particular file is encrypted by RSA algorithm and that encrypted data is again encrypted by elliptical curve cryptography algorithm so the resultant output is most secure data in unreadable form. After getting this output the system decrypt it on the client side by using the elliptical curve cryptography algorithm and with the help of that algorithm in the combined approach. In between this process of encrypting and decrypting the system permit the user who have access of that file and this permission is given by the server. Before giving the permission server verify the user about his identity from his information which is entered by that user at the stage of registering. After verifying that user server allow and send a secret key to that user to allow the download for the same file. This system conserves the database of the entire registered user. So any one can registered on to this system but only allowed user can access the secure files of the server. This system provides the uploading option to the server only and that uploaded file can be access by any registered user who is allowed by the server. This all means that this system is secure in positions of security as this paper are using the power of two of the algorithm and also provide a better authentication mechanism for the registered user for file accessing.

4.1 RSA

The RSA cryptosystem is developed by the three scientists named Ron Rivest, Adi Shamir, and Len Adleman, was first broadcasted in the August 1977 issue of Scientific American [12]. The cryptosystem is most commonly used for providing secrecy and also for ensuring the truthfulness of digital data. RSA is installed in many profitable business systems during those days. It is used for many purposed such as web servers and various browsers used it to secure web traffic, used for the purpose of ensuring confidentiality and genuineness of Email, used for protected remote login periods. It is located at the heart of electronic credit-card payment systems. In short words, RSA algorithm is frequently used in applications where security of digital data is worry.

The process latest numerous months during this Rivest proposed methods, Adleman attacked that methods and Shamir recalls doing some of each. In cryptography, RSA is an algorithm meant for public-key cryptography which was given by all three scientists Rivest, Shamir and Adleman. The RSA algorithm is recognized on the mathematical part which looks easy but tough for practical implementation. It simply means anyone can easily find the prime numbers and even can very easily multiple two sufficient large prime numbers together, but the actual difficulty arises during factoring their product. It is tremendously difficult to factor the product of those two large prime numbers. The RSA algorithm contains some specific steps for solving a problem. The respected steps are described below:

Step 1: Select two sufficiently large prime numbers P and Q.

Step 2: Calculate N = P * Q

Where N is the factor of two large prime number as per above calculations.

Step 3: Select the public key (Encryption key) E such that it is not factor of (P - 1) and (Q - 1)

Step 4: Select the private key (Decryption key) D such that the following equation is true

(D * E) mod (P - 1) * (Q - 1) = 1

Step 5: For Encryption process calculate the cipher text CT from the plain text PT as follows:

$$CT = PT^{E} \bmod N$$

Step 6: Send CT as a cipher text to the receiver

Step 7: For Decryption, calculate the plain text PT from the cipher text CT as follows

$PT = CT^{D} \bmod N$

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is nothing but a public key cryptosystem. In public key cryptosystem, each and every participant or the device taking part in the transmission or communication normally have a pair of keys. The two keys are simply a public key and a private key. Also it includes a set of various operations associated with the keys for performing the cryptographic operations. Only the specific participant has the idea about the private key whereas the public key is circulated to all users participating in the communication. Only some public key algorithm may require a set of predefined constants to be known by all the devices participating in the communication. The 'Domain parameters' in ECC is a sample of such constants. Public key cryptography, contrasting private key cryptography, it does not require any shared secret between the interactive parties but it is so slower as compared to private key cryptography which is a disadvantage [13].

The mathematical processes of ECC is shown on the elliptic curve $y2 = x3 + ax + b$, where $4a3 + 27b2 \neq 0$. The value of the variable 'a' and 'b' gives a diverse elliptic curve [14] [15]. All points (x, y) which fulfills the above equation plus a point at infinity lies on the elliptic curve. The public key present on a point in the curve and the private key will be a random

number. The public key is acquired by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', collected with some more constants constitutes the domain parameter of ECC. One main benefit of ECC is its lesser key size. A 160-bit key in [16].

4.2 Key Generation

Key generation is an important part where this system have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, system have to select a number 'd' within the range of 'n'.

Using the following equation system generate the public key

Q = d * P

d is the random number that system have selected within the range of (1 to n-1).

P is the point on the curve.

'Q' is the public key and 'd' is the private key.

4.2.1 Encryption

Let 'm' be the message that system is sending. System has to represent this message on the curve.

Consider 'm' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)].

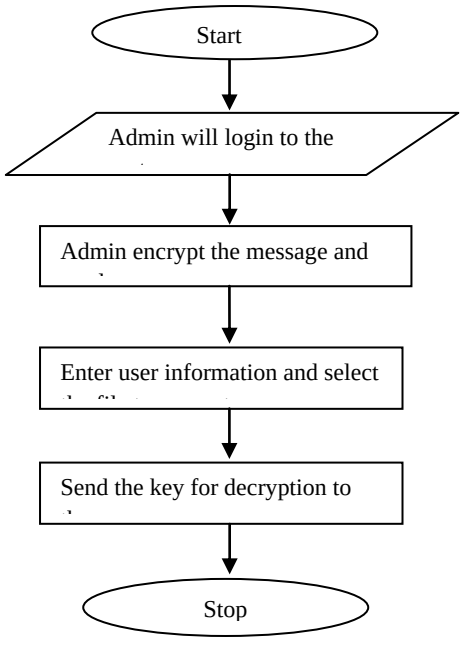

Figure 1 Flow Chart for the Encryption Process

4.2.4 Decryption Steps

The Decryption of the picture will be reverse of the above steps.
The resultant picture will be carried by the receiver.
When the picture will reach to receiver then first he will decrypt the resultant picture with the same data picture as a key. System generate the cipher picture.
Apply decryption cipher picture with key picture as key. The plain text will be created.
The receiver will get the plain message.

Two cipher texts will be generated let it be C1 and C2.

C1 = k*P

C2 = M + k*Q

C1 and C2 will be send.

4.2.2 Decryption

System will get back the message 'm' that was send to us,

M = C2 – d * C1

M is the original message that system has send.

A classic example of the size in bits of the keys used in various public key systems, with a comparable level of safety, is that a 160-bit ECC key is equivalent to RSA and DSA with a modulus of 1024 bits. The lack of a sub-exponential attack on ECC proposals potential decreases in processing power and memory size. These advantages are especially significant in applications on constrained devices.

4.2.3 Encryption Steps

The Encryption steps.
Admin will login into the system
Select the type of technique (message or image) encryption
Perform the encryption process.
Send file to the respective registered user and key on his email ID.
The receiver will get the key on his email. Then the user will go for the decryption process and get the
original data.

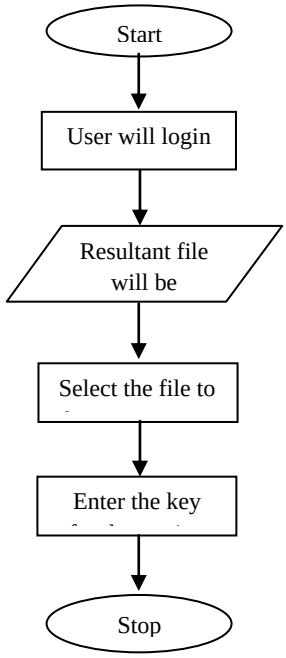

Figure 2 Flow chart for the decryption process

5. RESULTS AND ANALYSIS

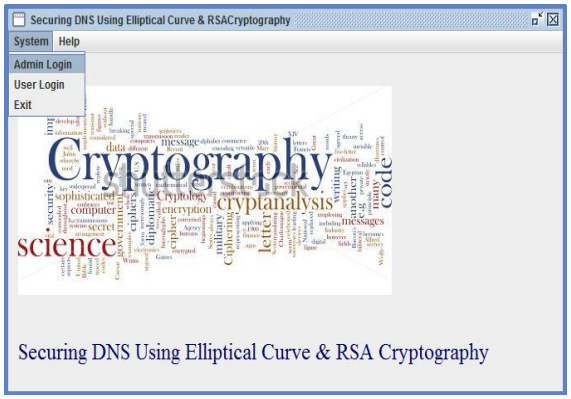

Figure 3 Snapshot of System

In figure 3 shows the first snapshot of proposed system contain two options system and help. From which system contain three sub options admin login which used to login for the administrator who have all the privilege to control the proposed system, user login is used to get the access for previously registered user and exit is used to leave the system. While other menu help shows the current version of system

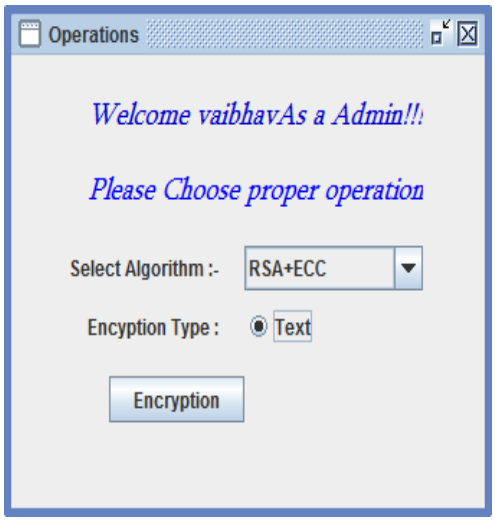

Figure 4 Selection of Operation

After selection the option form message encryption or image encryption administrator will go for the encryption process of the selected file type.

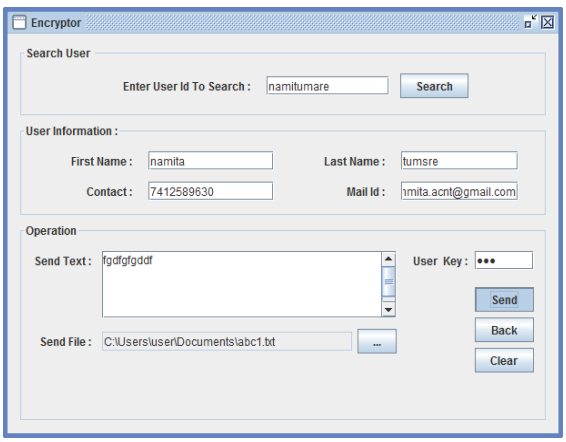

Figure 5 Text Encryption

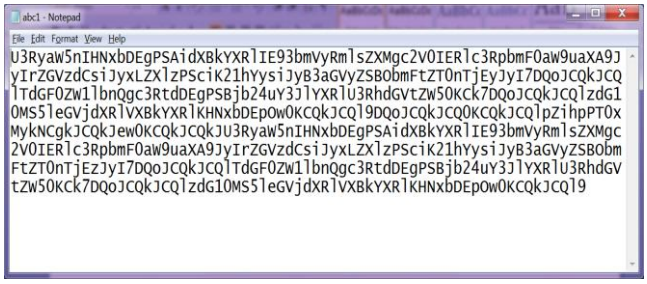

Figure 6 Encrypted Text

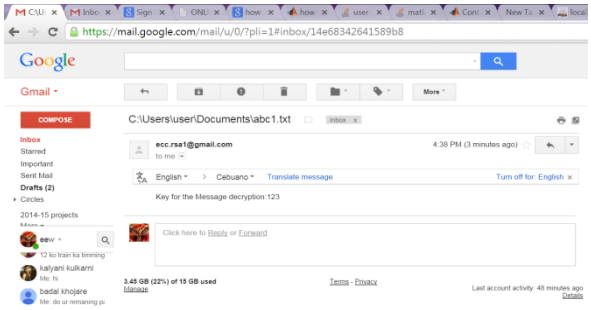

Figure 7 Key Received on User ID

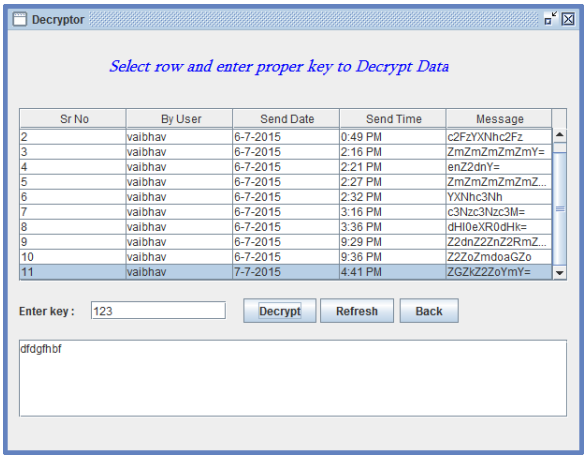

Figure 8 Before Decryption

Applications

It was noted that many security applications are specific instances of the protecting access pattern problem. However, due to the impracticality of the best private information retrieval constructions, considerable efforts were made to design specific solutions to these applications. This paper mentioned above that the data in the form of text and image can be securely send to the sender from the receiver who is successfully registered onto our proposed system so secure communication and data sending is easily possible in real time system. Another application of this system is, this paper use this combined approach in the transaction as system uses the security arrangement by RSA in real time.

6. CONCLUSION

In this paper has presented a novel software-based scheme to prevent the attack from the unauthorized person and provide more enhanced security for data communication and data transfer between the two persons. Cryptographic provision is significant mechanism of safeguarding sensitive data. In this work, this paper introduce combined approach of two well-known and secured algorithms RSA and ECC. This algorithm is simple and fast enough for most applications. RSA is one of

the oldest, secured methods of cryptographic and already in use in most of the application globally, this system add the one more secured technique called elliptical curve cryptography to enhance its security for every user. So in this way administrator can securely send the data by using text encryption and image encryption with more secure authentication technique.

7. REFERENCES

[1] Alfred J. Menezes and Paul C. van Oorschot and Scott A. Vanstone: "Handbook of Applied Cryptography", pp. 1-2, August 1996

[2] Rafael pass and Abhi shelat: "A course in cryptography", pp. 1-2, January 2010

[3] Darrel Hankerson, Alfred Menezes and Scott Vanstone: "Guide to Elliptic Curve

[4] William Stallings: "Cryptography and Network Security Principles and Practice", ISBN 13: 978-0-13-609704-4, 5th Edition, Pearson Publication, pp. 10-13, 2011

[5] Bart Preneel: "Analysis and Design of Cryptographic Hash Functions", pp. 24-26, February 2003

[6] Paul Krzyzanowski: "Cryptographic communication and authentication", Rutgers University – CS 417: Distributed Systems, pp. 1-2, 1997

[7] S. Maria Celestin Vigila and K. Muneeswaran: "Elliptic Curve based Key Generation for Symmetric Encryption", International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), ISSN 978-1-61284-653-8, pp. 824-829,IEEE, 2011

[8] Victor S. Miller: "Use of Elliptic Curves in Cryptography", H.C. Williams (Ed.): Advances in Cryptology - CRYPT0 85, LNCS 218, pp. 417-426, 1986

[9] Z. Guitouni, R.Chotin-Avot, M. Machhout, H. Mehrez and R. Tourki: "High Performances ASIC based Elliptic Curve Cryptographic Processor over GF (2m)", IJCA Special Issue on Network Security and Cryptography, NSC, 2011

[10] CH. Suneetha, D. Sravana Kumar, A. Chandrasekhar and K. Vanitha: "Secure Key

[11] Muhammad Hammad Ahmed, Syed Wasi Alam, Nauman Qureshi and lrum Baig: "Security for WSN based on Elliptic Curve Cryptography", ISSN 978-1-61284-941-6, pp. 75-79, IEEE, 2011

[12] R.L. Rivest, A. Shamir, and L. Adleman: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" ACM

[13] Anoop MS: "Elliptic Curve Cryptography an Implementation Guide"

[14] D. Sravana Kumar and CH. Suneetha A. Chandrasekhar: "Encryption of Data Using Elliptic Curve Over Finite Fields", International Journal of Distributed and Parallel Systems (IJDPS), Vol. 3, No.1, pp. 301-308, January 2012

[15] Vassil Dimitrov, Laurent Imbert, and Pradeep Kumar Mishra : "Efficient and Secure Elliptic Curve Point Multiplication Using Double-Base Chains", International Association for Cryptologic Research, B. Roy (Ed.): ASIA CRYPT 2005, LNCS 3788, pp. 59–78, 2005

[16] T. Abdurahmonov, Eng-Thiam Yeoh, and Helmi Mohamed Hussain: "A Proposed Implementation of Elliptic Curve Exponentiation over Prime Field in the Global Smart Cards", International Journal of Information and Electronics Engineering (IJIEE), Vol. 3, No. 1, pp. 72-76, January 2013