ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm

AnnapoornaShetty[1], Shravya Shetty K[2], Krithika K[3]

Assistant Professor, Department of Information Technology, St.Aloysius Institute of Management and Information Technology, Beeri, Mangalore, India[1]

MSc (ST) III Semester2, Department of Information Technology, St.Aloysius Institute of Management and Information Technology, Beeri, Mangalore, India[2]

MSc(ST) III Semester3, Department of Information Technology, St.Aloysius Institute of Management and Information Technology, Beeri, Mangalore, India[3]

ABSTRACT: Cryptography is used to make secure data transmission over networks. The algorithm selected for cryptography should meet the conditions of authentication, confidentiality, integrity and non-repudiation.The prevention of information from unauthorized access is the main concern in the area of cryptography.There are many cases where we need secure file transmission for example in banking transactions, e-shopping etc. RSA and El-Gamalalgorithm is asymmetric key cryptography also called Public Key cryptography.In this paper we are reviewing the two Asymmetric algorithms- RSA and El-Gamal.

KEYWORDS: RSA(Rivest-Shamir-Adleman**)**,El-Gamal,Symmetriccriptography,Asymmetric cryptography.

I.INTRODUCTION TO CRYPTOGRAPHY

Cryptography is the art and science of protecting information from unwanted person and converting it into a form undistinguishable by its attackers though stored and transmitted. The main aim of cryptography is keeping data secure form unauthorized persons. Data cryptography mostly is the scramble of the content of data, such as text data, image related data and audio, video related data to compose the data illegible, imperceptible or unintelligible during communication or storage called Encryption process. The reverse of data encryption process is called data Decryption.Cryptography provides a number of security goals to avoid a security issue. Due to security advantages of cryptography it is widely used today[1].

1.1 different goals of cryptography:

1. Confidentiality

Nobody can read the message not including the future receiver. Information in computer information is transmitted and has to be contact only by the authorized party and not by unauthorized person [2].

2. Authentication

This process is proving a one's identity. The information received by system then checks the identity of the sender that whether the information is incoming from an authorized person or unauthorized person or wrong identity.

3. Integrity

Only the authorized party is modifying the transmitted information or message. Nobody can change the given message.

4. Non Repudiation

This is a mechanism to prove that the sender really sent this message. So if any sender denies that he doesn't send the message; this method not allows doing such type of action to sender.

5. Access Control

Only the authorized parties are capable to contact the given information.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

1.2. SECURITY AGAINST ATTACK:

Cryptanalysis is an art and science of breaking the encrypted codes that are created by applying some cryptographic algorithm. Cryptanalysis attacks can classify the following:

1. Cipher text-only attack

In cipher-text only attack, the attacker has a part of the cipher text using available information, the attacker tries to find out the corresponding key and decrypt the plain-text [3].

2. Known-plaintext attack

The known- plaintext attack (KPA) is an attack model for cryptanalytic wherever the criminal has samples of each the plain-text and its encrypted version cipher-text. These will be revealing any secret data like secret keys and code books.

3. Chosen-plaintext attack

A chosen- plain-text attack (CPA) is an associate attack model for cryptography that presumes the potential to decide on arbitrary plain-text to be encrypted and procure the corresponding cipher-text.

4. Chosen-cipher text attackA chosen- cipher-text attack (CCA) is an attack model for scientific discipline within which the cryptologist gathers data, a minimum of partially, by selecting a cipher-text and getting its decipherment beneath an unknown key.

5. Chosen-text attack

A chosen text attack is a combination of choosing plain-text and chosen cipher-text attack [3].

6. Brute-force attack

This type of attack is a passive attack. The attacker can try all the possibilities of the key until the message is not broken. This is the very slow attack. Suppose that message is encrypted using the 56-bit key then the attacker can try all the possibilities up to 255 bit [2].

7. Dictionary attack

The extension to the Brute-force attack is the Dictionary attack. In the Dictionary attack, it will try also same possibilities but take only those key bit whose chances of success is more [2].

8. Timing attack

Timing Attack is a side channel attack in which the attacker attempts to compromise a cryptosystem by analyzing the time taken to execute cryptographic algorithms. Each consistent operation in a computer takes time to perform [2].

9. Man-in-the-middle attack

This is the type of active attack. This differs from the above in that it involves tricking individuals into compromise their keys. The attacker is placed in the two parties through communication channel who wish to exchange their keys for secure communication [2].

II. TYPES OF CRYPTOGRAPHY

[1] There are several ways to classify the cryptography algorithms. The most common types are:

· Secret Key Cryptography this is also called as Symmetric Key Cryptography

· Public Key Cryptography this is also called as Asymmetric Key Cryptography

2.1. Asymmetric Cryptography:

[4]Public-key cryptosystems help solve the key distribution problem by using separate keys forencryption and decryption, and making the encryption key public. Anyone can then encrypt a message, but only parties in possession of the private key can decrypt messages. Public key systems rely on one-way trap door functions, which are interesting mathematical functions that can be easily computed in one direction but are very difficult to reverse unless a secret key is known (the trap door). Since the encryption key is made public, finding the privateencryption key from the public encryption key must be intractable.

One application of public-key cryptography is secure email. Public keys are typically published on a user's website. However if the user's website is compromised, a different public key corresponding to a malicious adversaries private key can be substituted. For this reason, public key cryptography doesn't completely solve the key distribution problem. However digital signature can be used to fill the remaining gaps, allowing users to build a web of trusted public keys, and accept new keys if they are signed by an already trusted public key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

2.1.1 RSA Algorithm(Rivest-Shamir-Adleman):

[8] RSA is widely used in encrypted connection, digital certificates core algorithms. Public key algorithm invented in 1977 by Ron Rivest,Adi Shamir and Leonard Adelman(RSA).It is the main operation of RSA to compute modular exponentiation. Since RSA is based on arithmetic modulo large numbers, it can be slow in constraining environments[6].Especially, when RSA decrypts the cipher text and generates the signatures, more computation capacity and time will be required. Reducing modules in modular exponentiation is a technique to speed up the RSA decryption. The security of RSA comes from integer to find. Generation of random prime numbers gives the algorithm extra strength and efficiency.

Modified RSA for secure file transmission algorithm is divided in to 4 parts

1.Selecting file for transmission

2.Encryption of file

3.Transmission of encrypted file

4.Decryption of encrypted file

Secure RSA File Transmission Algorithm:

[8]MREA is an asymmetric-key cryptosystem,meaning that for communication, two keys are required: a public key and a private key.Furthermore,unlike RSA[9],it is one-way, the public key is used only for encryption,and the private key is used only for decryption. Following is a key generation algorithm for MREA cryptosystem.

Secure RSA File Transmission Algorithm can be summarized as follows

1. Choose four large prime numbers p,q,r and s randomly and independently of each other. All primes should be of equivalent length.
2. Compute n=p x q, m= r x s, φ= (p-1) x (q-1) and λ=(r-1) x(s-1).
3. Choose an integer e,1<e< φ such that Gcd (e, φ) =1
4. Compute the secret exponent d,1<d<φ, such that e xd mod φ =1.
5. Select an integer g=m+1.
6. Compute the modular multiplicative inverse:

μ=λ^(-1)mod m.

The public(encryption) key is (n,m,q,e).

The private(decryption)key is(d, λ, μ)

Encryption:

Let F be a file to be encrypted where the contents of file are taken into string S.

Select random number where r<m.

Compute cipher text as:c=g^(s^emodn) x r^(m)mod m^2.

Decryption:

Compute original message:

S=((((c^modm^2)-1)/m)x μ mod m)^d mod n

2.1.2 El-Gamal Algorithm

[8]The El-Gamal algorithm is a public-key cryptosystem based on the discrete logarithm problem. It consists of both the encryption and signature algorithms. The El-Gamal signature algorithm is similar to the encryption algorithm in that the public key and private key have the same form; However , encryption is not the same as signature verification.signature creation depends on the El-Gamal signature algorithm. The main disadvantage of El-Gamal is he need for randomness, and its slower speed(especially for signing).Another potential disadvantage of the El-Gamal algorithm is that the message expansion by a factor of two takes place during encryption. However, such message expansion is negligible if the cryptosystem is used only for exchange of secret keys El-Gamal encryption is used in the free GNU privacy Guard Software,recent versions ofPGP,and other cryptosystems.El-Gamal is not semantically secure.[8]El-Gamal algorithms can not only be used in data encryption, but in digital signature and the security relies on the problem of divergence logarithm in finite domains.Firstly, choose a prime number p, and two random number g, x, where g < p and x < p, calculate

Y=g^x(mod p) , of which y, g, and p are the public keys. The private key is x. G and p can be shared by a group of users.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

When El-Gamal is used in digital signature, signed information is M. Choose a random number k, in which k and p - 1 are relatively prime. Calculate a=g^k (mod p) and solve the following equation b: M=xa+kb(mod(p-1)). The signature is (a, b) and random number k must be discarded. The produce flow chart ofsignature (a, b) is shown in Figure 2:

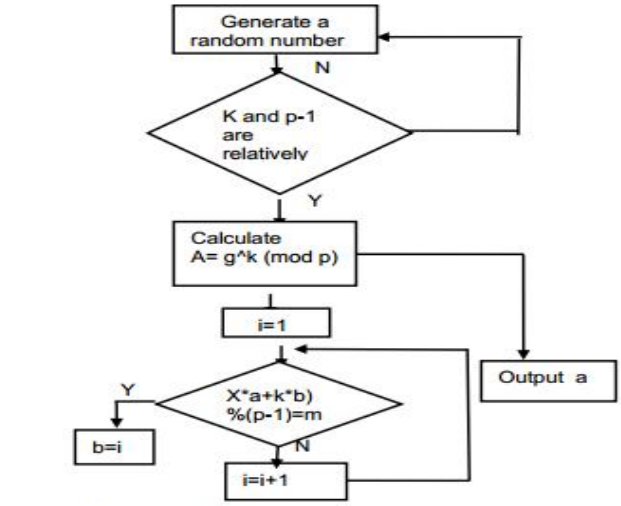

Figure 2. The Produce Flow Chart of Signature (a, b)

2.2 Symmetric key cryptosystems:

[4]Symmetric key systems use the same key for both encryption and decryption. In order to communicate securely using a symmetric system, two parties must agree on the key using some pre-existing secure channel. When more than two parties are involved key distribution becomes even more complicated, and historically key distribution has been a major obstacle for particle uses of cryptography. Typical symmetric ciphers use very convoluted transformations to obscure any patterns in the original message. The key controls how the transformations operate, and provides a map for reversing a transformations during decryption.

III.SUMMARY TABLE ON SYMMETRIC ALGORITHMS OF RSA AND EL-GAMAL

S.NO	Factors Analyzed	RSA [5]	El-Gamal
1	Developed	1978	1985
2	Key Length Value	>1024bits	1024bits
3	Type of Algorithm	Asymmetric	Asymmetric
4	Security Attacks	Timing Attack	Meet-in-The middle Attack
5	Simulation Speed	Fast	Fast
6	Scalability	No Scalability occurs	Good scalability
7	Key Used	Different key used for Encrypt and Decrypt Process	Different key used for Encrypt and Decrypt Process
8	Power Consumption	High	Low
9	Hardware and Software Implementation	Not very efficient	Faster and efficient

IV. LITERATURE SURVEY

In[1]this paper a performance evaluation of selected symmetric and asymmetric encryption algorithms such as DES, 3DES, AES, Blowfish, RSA and DiffieHellmen. The evaluation table that displays the encryption ratio is high in using the both encryption techniques. The tunability and key length is higher at the Asymmetric encryption technique .The key length is high in asymmetric encryption algorithm to break the code is complex in RSA. In the aspect of throughput, Throughput is increased so power consumption is decreased. Throughput is high in blowfish and blowfish is less power consumption algorithm hence speed is fast in the Symmetric key encryption is viewed as good. Finally, in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

the symmetric key encryption techniquesthe blowfish algorithm is specified as the better solution.The [7] author in this paper compares among two algorithms i.e. Elgamal, RSA, diffie Hellman, Knapsack are proposed with varying key length and key management methods using Neighborhood-Generated Keys. The size of encrypted message, key management method and algorithm efficiency is critical in respect of implementation in organizations that store large volumes of data. A new technical findings and viewpoint: efficiency, key length, plain text type dependency is found when implementing the any cryptographic algorithms. The all these technical viewpoints can further extended by focus on using intelligent systems such as Artificial Neural Network, Decision Tree algorithm Genetic Algorithm, etc. To encrypt message using keys generated by these algorithms.

The [8] author in this paper presents modified RSA algorithm for secure file transmission. RSA algorithm is asymmetric key cryptography also called Public Key cryptography. Two keys are generated in RSA, one key is used for encryption &other key which is only known to authenticated receiver can decrypt message. No other key can decrypt the message. Every communicating party needs just a key pair for communicating with any number of other communicating parties. Once someone obtains a key pair, he /she can communicate with anyone else. RSA is a well known public key cryptography algorithm and was one of the first great advances in public key cryptography. Even if it is efficient algorithm it is vulnerable to attackers. With the help of all brute force attacks hacker can obtain private key. Many improvements has been done to improve RSA like BATCH RSA, MultiPrime RSA, MultiPower RSA, Rebalanced RSA, RPrime RSA etc. As craze of internet is increasing exponentially, it is used for email, chatting, transferring data and files from one end to other. It needs to be a secure communication among the two parties [4].MREA algorithm is used to encrypt files and transmit encrypted files to other end where it is decrypted. The project works efficiently for small size while it consumes time for large size of files. At a instant only one file can be encrypted and transmitted. The project application was designed to take the efficiency and reusability into account. Great level of security is achieved using this algorithm. Modified RSA algorithm for file transmission algorithm can be used where high security file transmission required in public forums

The [10] author in this paper proposes a variant BEAIRSA (Batch Encrypt Assistant Improved RSA) to improve the Batch RSA decryption performance by transferring some decryption computations to encryption in modular exponentiation. The experimental results and the theoretical values show that the speed of the decryption has been substantially improved and the variant can be efficiently implemented in parallel on multi-core devices.

The [11] author in this paper literature survey on Cryptographic algorithms, include AES, DES, RSA, Diffie-Hellman, RC4, Blow Fish, El-Gamal, MD5 and Miller-Rabin. The aim of this paper is to provide a study of the research work done in the cryptography field and various cryptographic algorithms being used, through a literature survey between the years 2008 and 2013. This paper represents the published knowledge from IEEE online database. 270 papers were concerned and after doing content filtering, 50 best suited papers were taken into consideration. Key word indices were used to identify the significant papers. This paper will provide a direction to the naive users and will allow many new future applications. It is recapitulated that the RSA is used widely. Wide range of research is done in RSA. It used a search of keyword indices and article titles.

The main findings of the study are:

- RSA is most widely used algorithm.
- According to the survey, maximum research on cryptography is done in the year 2010.
- There is no remarkable improvement is the progress of integrated papers.
- Finally, through the better understanding of these algorithm's strengths and weaknesses further research can be conducted effectively.

The [12] author in this paper presents an analysis of ElGamal encryption system for securing data communication through the computer. The objectives of this paper are to study ElGamal algorithm in 32-bit integer computation and to implement data encryption using the ElGamal algorithm using 32-bit integers. ElGamal is a continuation of Diffie-Hellman key exchange algorithm. However, ElGamal encryption system uses asymmetric key encryption and decryption. ElGamal uses a public key to encrypt and private a key to decrypt messages where private key and public key are different. An experiment was conducted to evaluate the maximum number of integers that can be computed in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

32 bit computer system using standard 32 bit GCC compiler in Debian 6. Furthermore, an exploration of computing capabilities and performance measurement of the ElGamal algorithm using C language is presented in this paper Data performances have been collected for three different times. In conclusion data in real time are not suitable as a reference to be implemented because in real time mode this project is not being implemented on the networking process. Real time mode output is including other processing time, so the output time is not accurate. The actual times for the specific process are counted by using a combination of time in user mode and system mode. There are a few algorithms can be used as a technique to secure data through computer such as Diffie-Hellman key exchange and ElGamal algorithms. ElGamal is an improvement from Diffie-Hellman Key Exchange Protocol. In order to prove the ElGamal capabilities to secure data through a computer, an experiment have been performed and the result shows that an integer number equal or less than 32-bit is not capable to secure data through 32-bit computer system. For an improvement, to implement numbers bigger than 32-bit integer needs to use 64-bit computer. However, the usage of standard 32-bit or 64-bit GCC integer is not enough to meet security requirements for current cryptographic key strength which is at least 1024 bits. For that reason, implementation based on modern ElGamal needs to use 2 1024 bits computing integer that is using GMP bignum library to replace standard GCC integer number. GMP library allowed for C and C++ codes to computes integer numbers greater than 32-bits for 32-bit or 64-bit computer.

The [13] author in this paper describes the implementation of Rivest Shamir Adleman (RSA) and ElGamal Algorithm on JCryp Tool 1.0.0. Comparison of these two algorithms has been done on the basis of security and time consumption for encryption and decryption. The practical implementation of both these algorithms helps reader towards the best understanding and working differences between the two asymmetric key cryptography algorithms. This paper analyze that ElGamal algorithm is more secure as compared to RSA algorithm because it generates more complex cipher text and it was also slow because when we encrypt and decrypt it, it generates more than one public keys.

The [14] author in this paper presents the problem that ElGamal digital signature scheme's security is constantly being challenged and increasingly becomes increasingly serious, an improved ElGamal digital signature algorithm is proposed. As the original ElGamal algorithm has its own security disadvantages that only one random number is used, inorder to improve its security, the scheme presented in this paper improved this demerit by adding a random number to the original one and increasing difficulty of deciphering key. The security of the improved signature scheme is the same with the ElGamal signature scheme which is based on the difficult computable nature of discrete logarithm over finite fields. Then issues about how to increase the complexity between the random number and the key by adding a random number is discussed. Last, they have analyzed the improved signature scheme from the following two aspects: security complexity and time complexity. The analysis showed that the safety of the improved signature scheme was higher than that of the original one, and the improved one has a smaller time complexity. The paper systematically analyzes the security of ElGamal digital signature algorithm under the four attacks scheme. Analysis show that there are two attacks against random number, thereby indirectly access the value of private key. And these are the two of the most likely schemes to succeed. In order to enhance the security of algorithm in random, they proposed two improved ideas: (1) Enhanced security of random numbers, making it difficult for the success of the random number of hacks; (2) Establish more complex link between the random number and the private key, so it is difficult for a hacker to use random number to attack the private key indirectly. Based on ideas that established the more complex link between the random number and the private key, we proposed to add the signature equation of the same form of an equation with the improvement of the program, thereby increasing a random number and a signature data. The improved algorithm of security is enhanced, so that while a hacker needs greater computing capacity, the amount of signature and verification operations also will be increased. On the whole, the hacker's computational complexity is increased significantly. There are still some restrictions in the use of random numbers when the users sign. For example, we cannot make the two random numbers which were all the same and for the signature of two or more times. But generally speaking, the use of random numbers is restricted more lax than the restriction in the ElGamal digital signature algorithm. These are still to be continued to be improve. The analysis of the improved algorithm modeled on the ElGamal digital signature algorithm analysis is carried out by comparison. The new algorithm has its own characteristics. Especially, after the increase in random numbers, there may be an attacked method, which in the ElGamal-type digital signature algorithm it has not had. This is also the need for further study. In this paper, security and efficiency analysis showed that the improved ElGamal algorithm in these two areas had significant increase or improvement, making the application wider in the production and life. But I still have to find a fact that, though in the vast majority of cases we can prevent the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

hacker from a variety of attacks, there are two real problem closely related to its vitality: (1) the current mathematical community for the discrete logarithm problem is still difficult for an effective solution; (2) the signer must be very careful for the choice of random numbers. If there is a little vulnerability in these two areas, the ElGamal digital signature algorithm in relation should fade into history. In conclusion, in terms of the improved algorithm in terms of security has been greatly improved, which makes its scope of application even greater. The impact due to the increase of computation in the signature and verification operations will be weakened with the enhancement of the computing power of the processor.

The [15] author in this paper explains how Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key system for constrained environments, because of the small key sizes and computational efficiency, while preserving the same security level as the standard methods. The memory performance of ECC algorithms was scarcely investigated. They have developed a set of kernel benchmarks to examine performance of standard and corresponding elliptic curve public-key methods. In this paper, they characterize the operations and their memory impact on performance in Diffie-Hellman key exchange, digital signature algorithm, ElGamal, and RSA publickey cryptosystem, as well as elliptic curve Diffie-Hellman key exchange, elliptic curve digital signature algorithm and elliptic curve El-Gamal algorithm. They modeled a typical mobile device based on the Intel XScale architecture, which utilizes an ARM processor core and studied the benchmark set on that target. Different possible variations for the memory hierarchy of such basic architecture were considered. They compared our benchmarks with MiBench/Security, another widely accepted benchmark set, in order to provide a reference for our evaluation. The main contributions of this paper are: i) setup of kernel benchmark set for studying elliptic curve and standard public-key methods and ii) studying the impact of memory hierarchy in mobile systems. We found that using ECC does not involve a higher number of dynamically executed instructions. Even if ECC uses a lower number of memory operations, the working set is larger or the locality of instruction and data accesses is worse than in standard cryptography. Instruction and Data locality matters to ECC performance and appropriate caches should be adopted in order to keep total execution time at acceptable levels. The importance of memory stall and thus the importance of appropriate caches are more relevant in the case of binary field than in the case of prime field.

V. CONCLUSION

We have surveyed the two algorithms that are commonly used in the previous paper. The paper comparestwo RSA and El-Gamal for secure file transmission.In this paper the summary table reports the key length value, type of algorithm, security attacks, simulation speed, scalability, key used, power consumption, and hardware/ software implementation difference between RSA and EL-Gamal. In future we are implementing and performing comparative analysis of time taken for 2 Asymmetric key cryptography algorithms RSA and El-Gamal by changing some of the parameters. The size of encrypted message, key management method and algorithm efficiency is critical in respect of implementation in organizations that store large volumes of data.The execution time as a function of the encryption key and the file size will be examined and complexity and security will be checked.

REFERENCES

[1]“Comparative Study of Symmetric and Asymmetric Cryptography Techniques”using Neighborhood-Generated Keys [4], Ritu Tripathi1, Sanjay Agrawal2. National Institute of Technical Teachers’ Training and Research Bhopal, India.
[2] “Survey on Modular Attack on RSA Algorithm”,.Satish N .chalurkari ,Nileshkhochare ,B.B. mashram,International Journal of Computational Engineering & Management, ISSN: 2230- 7893
[3] Cryptography and network security, Express Learning, ITL Education Solution ltd.
[4]Implementing several attacks on plain ElGamalencryption,BryceAllen,A thesis submitted to the graduate facultyin partial fulllment of the requirements for the degree ofMASTER OF SCIENCE
[5]”A Survey on Performance Analysis of DES, AES and RSA Algorithm along with LSB Substitution Technique”,B. Padmavathi, S. RanjithaKumari
[6]"The Research of the Batch RSA Decryption Performance", Qing LIU, YunfeiLI,Tong LI, Lin HAO,Journal of Computational Information Systems 7:3 (2011) 948-955
[7] Comparison among different Cryptographic Algorithms using Neighborhood-Generated Keys, Lalit Singh and R.K. Bharti, nternational Journal of Computer Applications (0975 – 8887) Volume 73– No.5, July 2013
[8]”File Encryption and Decryption Using Secure RSA”,,Rajan.S.Jamgekar, GeetaShantanuJoshi,nternational Journal of Emerging Science and Engineering (IJESE)ISSN: 2319–6378, Volume-1, Issue-4, February 2013

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

[9]http://www.rsa.com/rsalabs/node.asp?id=2255
[10] "The Research of the Batch RSA Decryption Performance", Qing LIU1,3, Yunfei LI2,†, Tong LI1,3, LinHAO2, School of Software, Yunnan University, Kunming 650091, China2,School of Information Science and Engineering, Yunnan University, Kunming 650091, China3,Key Laboratory in Software Engineering of Yunnan Province, Kunming 650091, China, ournal of Computational Information Systems 7:3 (2011) 948-955
[11] "Study of Various Cryptographic Algorithms", Mini Malhotra1, Aman Singh21, 2, Department of Computer Science, Lovely Professional University, Punjab, India, International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878 Volume 1 Issue 3, November 2013
[12] "Cryptographic Computation Using ElGamal Algorithm in 32-bit Computing System", Nurul 'AtiqahRosly, MohdZafran Abdul Aziz, HabibahHashim,SyedFarid Syed Adnan,MohdAnuar Mat Isa, Faculty of Electrical Engineering, UniversitiTeknologi MARA, 40450 Shah Alam, Malaysia syed_farid@salam.uitm.edu.my Third International Conference on Control, Automation and Systems Engineering (CASE 2013)
[13] "Implementation & Analysis of RSA and ElGamal Algorithm", Ankush Sharma, JyotiAttri, Aarti Devi &Pratibha Sharma, *Deptt. Of CSE, Career Point University, Hamirpur (H.P.) 176041Email ID: ankushasp@gmail.com*
[14] "ElGamal Digital Signature Algorithm of Adding a Random Number", Xiaofei Li, XuanjingShen and Haipeng Chen, College of Computer Science and Technology, Jilin University, Changchun, China,Email: xiaofei09@mails.jlu.edu.cn, {xjshen, chenhp}@jlu.edu.cn, JOURNAL OF NETWORKS, VOL. 6, NO. 5, MAY 2011
[15] "Memory Performance of Public-Key Cryptography Methods", in Mobile Environments", Branovic, R. Giorgi, E. Martinelli University of Siena Via Roma 56 - Siena, Italy *{branovic,giorgi,martinelli}@dii.unisi.it*