A Survey on Secured Communication with High Speed using Public Key Cryptography

Dr.D.I.George Amalarethinam[1], J.Sai Geetha[2*]

Abstract— Nowadays, the use of internet is emerging very fast across the world. The beauty of the internet also includes its concern over security. Security is the most challenging issue in the internet applications. The risk of obtaining data free from an attack is hardly difficult because of advanced technology of today's computers. The better solution is to offer the maximum protection against security threats and the data intruders. Cryptography is an effective, efficient and essential component for secure transmission of information by implementing security parameters such as Confidentiality, Authentication, Accountability and Accuracy. The view on security is remaining incomplete by the attacks of intruders. This survey presents a package of reviews taking various parameters that are having a greater influence towards secured communication through an insecured channel. Four key stages of public key algorithm are identified, namely, message encoding, key generation, encryption and decryption. The factors such as key length, cipher text type and length, block size of plain text, effectiveness and attacks are also to be considered for enhancement of security and speed. This paper presents a detailed study of Asymmetric encryption techniques with their advantages and limitations over each other. Hence, the working principles, features and issues are identified with respect to network communication speed and security enhancement.

Keywords: public key Cryptography, Encryption, Decryption, public key, private key, plain text, Cipher Text

——————————   ◆   ——————————

1 INTRODUCTION

Cryptography is an ancient art developed in 1900 B.C. It is a vital part of computer networks which transforms (encrypts) the information (plain text) into an unreadable form (cipher text). Further this cipher text can be decrypted with the help of a secret key known only to the intended recipient to obtain the original text. Cryptography is a mathematical method of keeping the information secret from any unauthorised access. It is used to prevent the data from various attacks when communicating over any un-trusted medium. Authentication and digital signatures are the major applications of cryptography. Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing the original conversion.

Cryptology is a combination of cryptography and cryptanalysis. There are two main functions of cryptography such as encryption and decryption. The process of encoding plain text messages into cipher text messages is called as encryption. The reverse process of transforming cipher text back to plain text messages is called decryption. Both encryption and decryption can be done based on a secret value known as key.

In cryptosystem, there are two main classifications based on keys. If the same key is used for both encryption and decryption, it is called symmetric cryptosystem. If two different keys are used where one key is known as public key (for encryption) and another key is known as private key (for decryption), then it is called as asymmetric or public key cryptosystem.

1.2 Goals of Cryptography

- Confidentiality - Information in computer is transmitted and has to be accessed only by the authorised person and not by anyone else.
- Authentication - The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person
- Data Integrity - Ensuring that the information has not been altered by any unauthorized or unknown person. In other words no one in between the sender and receiver are allowed to alter the given message.
- Non Repudiation - Prevents either sender or receiver from denying a message.
- Access Control - Only the authorized parties are able to access the given information.

1.3 Cryptographic Strength

- The secrecy of the key.
- The difficulty of guessing the key or trying out all possible keys (a key search). Longer keys are generally harder to guess or find.
- The difficulty of inverting the encryption algorithm without knowing the encryption key (breaking the encryption algorithm).
- The existence of *back doors*, or additional ways by which an encrypted file can be decrypted more easily without knowing the key.

[1]*Associate Professor,Director-MCA, Jamal Mohamed College,Trichy,Tamilnadu,India; di_george@ymail.com*
[2*]*Assistant Professor in Computer Science, Nehru Memorial College,Trichy, Tamilnadu, India ; jsaigeetha99@gmail.com*

- The ability to decrypt an entire encrypted message if someone knows the way that a portion of it decrypts.
- The properties of the plain text and knowledge of those properties by an attacker.

In Table 1, the salient features of symmetric and asymmetric cryptosystems are compared. Asymmetric algorithms are more suitable for secured communication than symmetric algorithms [1]. Symmetric cryptosystem supports secured data storage, although, it has the problem in key distribution. In Asymmetric cryptosystem, the public key may even be distributed to all end users.

TABLE 1. COMPARISON OF FEATURES IN SYMMETRIC AND ASYMMETRIC CRYPTOSYSTEM

Method	Symmetric	Asymmetric
Keys	Same key	Different Keys
Encryption	Faster	Slow
Size of cipher text	Same or less than the plain text size	More than the size of plain text
Decryption	Faster	Slow
Key Distribution	Difficult	Easy
Scalability	Create issue	High
Security	Moderate	Highest
Nature	Closed	Open
Inherent Vulnerabilities	Brute Forced and Oracle attack, Linear and cryptanalysis Attack	Brute forced and oracle attack
Secure Services	confidentially	Integrity, confidentially and Non-repudiation

2. PUBLIC KEY CRYPTOGRAPHY

James Ellis of the British Communication Electronic Security Service Group (CSEG) proposed the idea of asymmetric key cryptography in 1960 [2]. It is not a suitable algorithm in the practical aspect. Simultaneously, the US National Security Agency (NSA) was also working on asymmetric cryptography. The introduction of public-key cryptography [3] by Diffie and Hellman in 1976 was an important improvement in the history of cryptography. In 1977, Ron Rivest, Adi Shamir and Len Adleman at MIT developed the first major asymmetric key cryptography system and published as RSA algorithm. Public-key cryptography was originally invented as an elegant solution to the key distribution problems associated with Symmetric key cryptography.

2.1 Components of Public key algorithms

In public key algorithms, there are two major parts. First one is the key generation which generates public and private key for encryption and decryption respectively.

Another part of the algorithm is encryption and decryption process. Multiplicative inverse and Greatest Common Divisor (GCD) are the major parts for key generation process. Random number generation, Modularization and Exponentiation are the common steps for most of the asymmetric algorithms which is represented in Table 2.

It is necessary to study and find the increasingly better public key algorithm to preclude various attacks. In the present literature survey of public key cryptography, speed and security enhancement are mainly focused. This can be achieved through the changes in any one of the components in Table 2. In most of the cases, the experiment was carried out through RSA since it is one of the highly secured algorithms in public key cryptosystem. The execution speed is the critical issue of PKC algorithm. The processing time is more on account of larger key size in PKC.

TABLE 2. VARIOUS COMPONENTS OF PUBLIC KEY ALGORITHMS

Algorithms	Key Generation			Encryption and Decryption	
	Random Numbers	Multiplicative Inverse	GCD	Modularization	Exponentiation
Knapsack (Super increasing Sequence)	Yes	---	---	Yes	---
RSA	Yes	Yes	Yes	Yes	Yes
McElliece	Yes	---	---	---	---
Rabin	Yes	---	---	Yes	Yes
Elgamal	Yes	---	---	Yes	Yes
Diffie_Hellman	Yes	---	---	Yes	Yes
Digital Signature	Yes	Yes	Yes	Yes	Yes

3. SECURITY BASED PKC ALGORITHMS

In public key cryptography, RSA is one of the highly secured algorithms [4]. The security based PKC algorithms are grouped on the basis of message encoding, key generation, encryption and decryption process. The efficiency of a cryptographic algorithm is based on the time taken for encryption and decryption process and the relationship between the plain text and cipher text.

The security can be enhanced through increasing the complexity of cipher text. Hence, it is necessary to change the numerical representation of plain text other than ASCII code.

Hence, the Magic Square (MS) algorithm [5] is presented by Gopinath Ganapathi and Mani.K, which is used for message encoding. The encryption and decryption process is done based on the magic square rather than ASCII values. This approach is used to increase the security due to randomness of the value within the magic square. It is constructed based on random values such as starting value, row and column sum of MS. When the file size is increased in double, the encryption and decryption time is also increased. This issue is resolved by carrying out encryption and decryption processes parallely.

Sapiee Jamel et al., [6] have proposed a new cryptographic algorithm based on combinations of hybrid magic cubes which are generated from a magic square and two orthogonal Latin squares used for message encoding. Using two random functions, i.e., random selection of thirteen magic cubes and random key selection from layers of hybrid, the generated cipher texts are free from any predicted pattern which might be used by cryptanalyst to decipher the original message.

Gayatri Kulkarni et al., [7] proposed a technique that includes two main steps of data transfer with protection. In Message encoding process, the plain text is converted into ASCII form, then by adding with the digits of the Armstrong numbers. Further, the ASCII value is encoded using a matrix to generate the required encrypted data. The encryption of colour is done by adding key values to the original colour values at sender's side. Three different keys are used, namely, the colours, key values added with the colours and Armstrong numbers. Data can be retrieved only after ascertaining all these three key values.

In order to provide better security and reliable data transmission, an effective method of Deoxyribo Nucleic Acid (DNA) based cryptography [8] was proposed by Snehal Javheri and Rahul Kulkarni. In this method the mixture of mathematical and biological concepts are used to get the encrypted data in the form of DNA sequences. The proposed algorithm has two phases. The primary cipher text is generated by using substitution method and subsequently the final cipher text is generated using DNA digital coding.

The image file is also encoded by the numerals before encryption to enhance the security. Varsha Bhatt and Gajendra Singh Chandel [9] proposed a new algorithm that deals with the representative image encryption techniques, position permutation, naive substitution, transposition and value transformation. Selective techniques will be described, assessed and matched up with respect to security level and encryption speed using stegnography [10].

Quist-Aphetsi Kester [11] proposed the work sets out to contribute to the general body of knowledge in the area of cryptography application and by developing a cipher algorithm for image encryption of m × n size by shuffling the RGB pixel values. Finally, the algorithm made it possible for encryption and decryption of the images on the basis of RGB pixel.

Hiral Rathod, Mahendra Singh Sisodia et.al., [12] introduced a new permutation technique based on the combination of image permutation and developed an encryption algorithm called "Hyper Image Encryption Algorithm (HIEA)". The selected image will be converted into binary value blocks, which will be rearranged into a permuted image using a permutation process and finally the generated image will be encrypted by using HIEA algorithm.

Another approach practiced for security enhancement is by strengthening the key generation process. It has been accomplished by increasing the randomness of the key value [13]. Alaa Hussien Al Hamami and Aldariesh.I.A. [14] have proposed enhancement of RSA algorithm through additional third prime number in the composition of public and private key. This will increase the factoring complexity of the variable (n). The existence of three prime numbers will give the ability to the enhanced encryption method so as to increase the difficulty of factoring of variable (n).

Particle swarm optimization (PSO) is a technique widely used to solve real optimization problems. In the recent years, the use of Graphics Processing Unit (GPU) has been proposed for some general purpose computing applications. The major benefit to implement the PSO for GPU is the possibility of reduction in execution time. It occurs due to the higher computing power presented nowadays on GPU platform. C.J.A Bastos-Filho et al., [15] proposed the random number generator on GPU based PSO and analysed the same in terms of RNG statistical quality.

The randomness of the key is improved by using PSO and Genetic Algorithm (GA). Smita Jhajharia et al., [16] proposed a new algorithm PSO_GA for the purpose of generating random numbers. The PSO initialization needed random variables which will be provided by GA. It ensures the algorithm runs every time with a unique random value which cannot be guessed. PSO uses a set of fine fit initial keys as input from key domain generated by GA and outputs the position of key having the highest fitness among the keys.

Narendra K Pareek et al., [17] exploited the interesting properties of chaotic systems to design a random bit generator called Cross coupled chaotic random Bit Generator (CCCBG), in which two chaotic systems are cross-coupled with each other. There is no repetition of patterns that have been observed in the bit streams generated by the proposed CCCBG. It can be used in many applications requiring random binary sequences and also in the design of secured cryptosystems.

If an attacker has opportunity of getting the encryption key (e) value, they can directly find decryption key (d) value and decrypt the message. Amare Anagaw Ayele and Vuda Sreenivasarao [18] have done an efficient implementation of RSA algorithm using two public key pairs and using some mathematical logic rather than sending the encryption key (e) value directly as a public key. This method overcomes the threat, even if the attacker got the encryption key incidentally.

The changes in encryption and decryption process are also useful to provide additional level of security. An alteration in RSA algorithm has been proposed that switches from the domain of integers to the domain of bit stuffing to be applied to the first function of Secure Socket Layer (SSL) so as to ensure secured communication. Parshotam et al., [19] introduced this technique of bit stuffing which will complicate the access to the message, even after getting the access to the private key. It will enhance the security which is an inevitable requirement for the design of cryptographic protocols for secured communication.

Nentawe Y Goshwe [20] presented a design of data encryption and decryption in a network environment using RSA algorithm with specific message block size. The algorithm allows the message sender to generate a public key to encrypt the message. The plain text is encoded before encryption. The receiver decrypts the message and then decodes the plain text. An incorrect private key will still decrypt the cipher text, but forms a different appearance of original message.

The extraction from various papers in relation to security is shown in Table 3.

TABLE 3. ANALYSIS ON SECURITY ENHANCEMENT IN PKC

S. No	Algorithm	Message encoding	Key Generation	Encryption	Decryption	Issues
1	Magic Square [5]	Represent the plain text as numerical value using MS	---	---	---	Need additional time for construction of MS
2	Random Numbers generation using PSO [15]	---	Particle Swarm Optimization (PSO)	---	---	Increases the time taken for key generation
3	Cross-coupled Chaotic Tent Map Based Bit Generator (CCCBG) [17]	---	Chaotic Map	---	---	Increases the time taken for key generation
4	Enhanced RSA [14]	---	Using Three numbers for key generation	---	---	Increases the time taken for key generation process.
5	Dynamic Encryption using Stegnography [21]	---	---	Stegnography in addition to encryption	Reverse of encryption process	Increases the total time of cryptosystem as well as communication time and cost.
6	Modifying RSA using Bit Stuffing [19]	---	---	Add random bits	Remove random bits	Increases the size of message
7	Random numbers generation using Genetic algorithm [22]	---	Genetic algorithm	---	---	Increases the time taken for key generation
8	Multiple Public keys [18]	---	Multiple Public keys	Encrypt the message using	---	Increases the key generation and Encryption time.

				two public keys		
9	RSA based storage security (RSASS) [23]	RSA Signature and Merkle hash tree	---	---	---	Increase the decryption time and fitted only for cloud environment
10	Key generation using PSO_GA [16]	__	PSO_GA	---	---	Increases the time taken for key generation
11	RGB pixel transposition and shuffling [11]	m × n image size by shuffling pixel values	---	---	---	Change the RGB values. Not be used in any Asymmetric algorithm
12	Message Security algorithm [7]	Armstrong number and colour	---	---	---	Stream cipher method and colour identification reduces the execution speed
13	Quantum Key Distribution (QKD) [44]	---	Quantum Keys	---	---	Reduces the execution speed
14	Secured RSA [24]	---	Two prime numbers and Two Random numbers	---	---	Increases the time taken for key generation
15	DNA based Message encoding [25]	Represent the plain text Using DNA	---	Two levels of Encryption	Two levels of Decryption	Increases the cipher text size and reduces the execution speed
16	Enhanced RSA [26]	---	---	Choose alternative Encryption key e'	Choose alternative decryption key d'	Increases the time taken for set of keys generation
17	Visual cryptography [27]	---	---	Cipher text hiding into Image	Extract plaintext from Image	Consumes more time for encryption and decryption process
18	Image encryption and decryption Using chaotic map [28]	---	---	Confusion and Diffusion method	Confusion and Diffusion Method	Cipher text is also in image format and hence can be identified easily
19	Multichannel random Discrete Fourier Transform [29]	---	---	Fourier transform	Fourier transform	Cipher text is also in image format and hence can be identified easily

4. SPEED BASED PKC ALGORITHMS

In PKC, the security level is assessed with the help of key size. On the other hand, it affects the speed of encryption and decryption process. The speed enhancement is to be done without reducing the key size and the original message. The processing speed is improved through the process of Modular exponentiation.

The optimization for big-numbers squaring has various usages and the most prominent one is RSA acceleration, which consumes a significant portion of the computations. Gueron Shay and Vlad Krasnov [30] introduced an algorithm for big-numbers squaring, that reduces the number of single precision add-with-carry operations, and trades several additions with a single left shift operation.

A famous approach to implement modular multiplication in hardware circuits is based on the Montgomery modular multiplication algorithm. To speed up the encryption / decryption process, many high speed Montgomery modular multiplication algorithms and hardware architectures employ carry-save addition (CSA). This architecture increases the utilization of memory area. In order to reduce the area of the CSA based multiplier, an area-efficient algorithm called Double Add Reduce algorithm is introduced by Anizha Radhakrishnan and Seena George [31].

Several deterministic and stochastic algorithms have been proposed to generate the shortest addition chains for exponentiation. Normally, stochastic algorithms produce the optimal addition chains, but it is not obtained from the single run, a time consuming process. As a consequence, a deterministic algorithm has been proposed by Mani.K. [32] which is simply based on division method to produce the addition chain.

Koon-Shik Cho et al., [33] presented a new radix-4 modular multiplication algorithm based on the sign estimation technique. It detects the sign of a number represented in the form of a carry-sum pair. It can be implemented with 5-bit carry look-ahead adder. The hardware speed of the cryptosystem depends on the performance of modular multiplication using large numbers. It needs only half of a clock cycle when compared to the existing system. It is efficient for modular exponentiation with large modulus used in RSA cryptosystem.

Vollala.S et.al., [35] proposed a Bit forwarding (BFW) algorithm to compute a^x mod n, and to compute $a^x b^y$ mod n two algorithms, namely, Substitute and Reward (SRW), Store and Forward(SFW). This algorithm was suitable for devices with low computational power and limited storage.

In Table 4, the algorithms used to produce high speed cryptosystems by applying various approaches have been analysed.

TABLE 4. ANALYSIS ON SPEED ENHANCEMENT IN PKC

S. No	Algorithms	Message encoding	Key generation	Encryption	Decryption	Issues
1	Optimized Multi precision squaring [30]	—	—	Squaring method	Squaring method	It helps to suitable for exponentiation. Recently Mantgomery function improves the speed of exponentiation.
2	ECC block Method [34]	Convert input text into block of Bits with equal size	—	—	—	Manipulation of points is more complicated.
3	Division based Method (DBM) [32]	—	—	Calculate exponentiation using addition chain	Calculate exponentiation using addition chain	Not suitable to generate optimized addition chain for all the values
4	Bitforward(BFW), Substitute and Reward (SRW) and Store and Forward (SFW) algorithms [35]	—	—	—	Modular exponentiation	Considers only the cryptosystem speed.
5	Double Add Reduce Algorithm [31]	—	—	Modular exponentiation	Modular exponentiation	High energy consumption.

5. SECURITY AND SPEED BASED PKC

In PKC, the message encoding and modula exponentiation processes are altered in order to reduce the time needed for encryption / decryption process besides security enhancement. Anil Hingmire [36] proposed a new algorithm that includes a phase of Substitution, Position and Zigzag encryption. It generates only a single key and takes a key level from the users as used in Substitution and Position method. Since it undergoes three phases, the overall complexity increases and the algorithm becomes quite immune to be attacked. It is ascertained that block cipher is the suitable method in symmetric cryptosystem [37].

The basic operation of RSA cryptosystem is modular exponentiation which is achieved by repeated modular multiplications. RSA can be speeded up by using the Chinese Remainder Theorem (CRT) and strong prime criterion. G.A.V.Rama Chandra Rao et al., [38] presented an efficient modulo n multiplication algorithm with reasonable factors of $2n$ and $2n+2$. This new technique can speed up the decryption process thus-by reducing the computational time compared to the traditional methods.

G.A.V.Rama Chandra Rao et al., [39] proposed a new algorithm based on the remainder with regards to the modulus value n. There is a possibility that $2n+1$ and $2n+2$ can easily be factorized, even if it is difficult to factorize the prime factors. This procedure was faster than the existing algorithms and the computational complexity was also calculated.

Shaina Arora and Pooja [40], proposed an algorithm to merge both enhanced RSA algorithm and El-Gamal algorithms to provide the user with a higher level of data security. The enhanced RSA algorithm enables faster encryption/ decryption process and generates public and private key faster than the original RSA. The enhanced RSA cryptosystem is based on Integer Factorization Problem (IFP), while the El-Gamal cryptosystem operated on the basis of Discrete Logarithm Problem (DLP). The basic principle of the proposed model is the combination IFP and DLP.

The proposed framework of Amin. A.E. and Abd Elbadea.A [41] integrated the concept of genetic algorithm to generates unique genetic key and use it to formulate patterns table. Then the secret message is divided into blocks with same size according to the length of key. After pattern recognition, it is used into blocks matched by weighted Euclidean distance. The

XOR operation plays a major role in modern cryptography, where the total length of the plain text is not multiple of the block length. Hence it is necessary to deal with the final short block. The final block must contain a count of the number of filler bytes, so that the message length is always increased by maximum block length bytes.

The Short Range Natural Number (SRNN) algorithm is similar to RSA algorithm with some modifications, as proposed by Sonal Sharma et al., [42]. In this algorithm, two extremely large prime numbers are used for key generation (similar to RSA). These two natural numbers are added with a pair of keys (public, private). These natural numbers increase the security of the cryptosystem. In the aspect of speed, the plain text is divided into blocks before encryption. The block size is fixed as half of the modulus value for speed enhancement.

LiuRui and Xiaoping Tian [43] introduced an algorithm 1D Logistic chaotic map to confuse the addresses of colour image pixels. The resultant image is divided into 24-bit planes to get a bit matrix containing a mixture of red, green and blue elements. Finally, utilized global diffusion is to permute the bit-matrix which makes the three elements, namely, R, G and B influence each other effectively without neglecting the relativity between each of them.

In public key algorithms, the security of the algorithm is decided on the basis of large size of key. It reduces the execution speed of encryption and decryption process. In most of the algorithms, exponentiation is the main component of encryption and decryption. The efficient Modular exponentiation methods are used to increase the speed without reducing the size of the key.

In general, the number of levels of encryption and decryption process is increased in the aspect of security. It increases the complexity of the algorithm. In addition to the key, the number of parameters used for encryption and decryption is also raised. The plain text cannot be derived by the intruders due to the complexity of encryption and decryption process. A detailed assessment of literature involving the parameters such as speed and security is listed in Table 5.

TABLE 5. SPEED AND SECURITY ENHANCEMENT IN PKC

S. No	Algorithms	Message encoding	Key generation	Encryption	Decryption	Issues
1	MREA (Homomorphic function) [45]	Change the plaintext and block cipher method	Four prime numbers	Using the parameters (e,n,m,g)	Using the parameters (d,λ,μ)	Increase the total time of cryptosystem. and block size is not suitable for High speed
2	Substitution , Position and Zigzag Method (PSZ) [36]	—	—	PSZ Encryption	PSZ Decryption	Suitable only for small size of text
3	Short Range Natural Number (SRNN) [42]	Block cipher and block size based on Modulus value	Using natural numbers	Public key (n,e,u^a)	Private key (d,a,u)	Reduce the execution speed
4	MulMod Algorithm [39]	—	—	Modular exponentiation	Modular exponentiation	Identify the factors of modulus value.
5	Cryptosystem based on Genetic Algorithm [41]	Block Cipher Method	Genetic algorithm	Pattern Recognition	Pattern Recognition	Reduce the execution speed and increase the size of cipher text
6	Hybrid RSA with Elgamal [40]	—	—	Two steps for encryption	Two steps for decryption	Additional time needed for encryption and decryption.

6. CONCLUSION

The development of internet application needs secured cryptosystem for data communication. Public key cryptosystem is suitable for secured communication. To obtain the user satisfaction, high speed algorithms with enhanced security has to be developed. The speed and security issues are discussed in this paper to encourage the researchers to propose new algorithms with multiple parameters towards better performance of secured network communication. In future, more secured public key algorithms will be implemented to satisfy the user specified deadlines.

REFERENCES

[1.] Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar and Mohsin Iftikhar, “A Survey about the Latest Trends and Research Issues of ryptographic Elements”, IJCSI International Journal of Computer Science Issues, Vol.8, Iss.3, May 2011.

[2.] J. Menezes, P. C. Van Oorschot and S. Vanstone, “Handbook of Applied Cryptography”, CRC Press, Boca Ration, Florida, USA, 1997.

[3.] Whitfield diffie, “The First Ten Years of Public key Cryptography”, Proceedings of IEEE, vol.76, No.5, 1998.

[4.] Xin Zhou, Xiaofei Tang, “Research and Implementation of RSA algorithm for encryption and decryption”, Strategic Technology (IFOST), 6th International Forum, Vol.2, pp.1118-112, Aug 2011.

[5.] Gopinath Ganapathy and Mani.K., “Add-On Security Model for Public Key Cryptosystem Based on Magic Square Implementation”, Proceedings of the World Congress on Engineering and Computer Science, Oct 2009.

[6.] Jamel.S, Herawan.T, Deris MM. “A Cryptographic algorithm based on hybrid cubes in Computational Science and Its Applications” – ICCSA, Springer Berlin Heidelberg, pp. 175-187, 2010.

[7.] Gayatri Kulkarni, Pranjali Gujar, Madhuri Joshi, Shilpa Jadhav, “Message Security Using Armstrong Numbers and Authentication Using Colors”, Vol.4, Iss.1, Jan 2014.

[8.] Snehal Javheri and Rahul Kulkarni, “Secure Data communication and Cryptography based on DNA based Message Encoding”, International Journal of Computer Applications, Vol.98, Iss. 16, Jul 2014.

[9.] Varsha Bhatt, Gajendra Singh Chandel, “Implementaion of new advance image Encryption Algorithm to enhance the security of Multimedia Component” International Journal of Advanced Technology & Engineering Research (IJATER), Vol.2, Iss.4, Jul 2012.

[10.] Sudipter Sahana, Madhusree Majumdar, Shilaitya Bose, Anay Ghosal, “Security Enhancement Approach for Data transfer using Elliptic Curve Cryptography and Image Stegnography”, International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Iss.4, 2015.

[11.] Quist-Aphetsi Kester, “Image Encryption based on the RGB Pixel Transposition and Shuffling”, International Journal Computer Network and Information Security, Vol.7, pp.43-50 Published Online June 2013.

[12.] Hiral Rathod, Mahendra Singh Sisodia and Sanjay Kumar Sharma, “Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)", International Journal of Computer Technology and Electronics Engineering (IJCTEE), Vol.1, Iss.3, pp.7-13, 2011

[13.] Kencheng Zeng, Chung-Huang Yang, Dah- Yea Ewi and T.R.N. Rao, “Pseudo Random Bit Generators in Stream Cipher Cryptography”, Vol.24, Iss. 2, pp:8–17, IEEE Xplore, 1991.

[14.] Alaa Hussein Al_Hamami and Ibrehem Abdallah Aldariesh, “Enhanced for RSA cryptosystem Algorithm”, International Conference on Advanced Computer Science Application and Technologies, IEEE xplore 2013

[15.] Bastos-Filho.C.J.A., Oliveira Junior.M.A.C., Nascimento.D.N.O. and Ramos.A.D., “Impact of the Random Number Generator Quality on Particle Swarm Optimization Algorithm Running on Graphic Processor Units”, 10th International Conference on Hybrid Intelligent System, IEEE Xplore 2010.

[16.] Smita Jhajharia Swati and Mishra Siddharth Bali, “Public Key Cryptography Using Particle Swarm Optimization and Genetic Algorithms”, International Journal of Advanced Research in Computer Science and Software, Vol.3, Iss.6, Jun 2013.

[17.] Narendra K Pareek, Vinod Patidar and Krishnan K Sud “A Random Bit Generator Using Chaotic Maps”, International Journal of Network Security, Vol.10, Iss.1, pp.32, Jan 2010.

[18.] Amare Anagaw Ayele and Vuda Sreenivasaro, “A Modified RSA Encryption technique Based on Multiple public keys”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.1, Iss.4, Jun 2013.

[19.] Parhotam, Rupinder Cheema and Aayush Gulati, “Improving the Secure Socket Layer by Modifying the RSA Algorithm”, International Journal of Computer Science, Engineering and Application (IJCSEA) Vol.2, Iss.3, Jun 2012.

[20.] Nentawe Y.Goshwe, “Data encryption and decryption using RSA Algorithm in a Network Environment”, International Journal of Computer Science and Network Security (IJCSNS), Vol.13, Iss.7, 2013.

[21.] Gajendra Singh Chandel, Ravindra Gupta and Swati Jain, “Proposed Model of Dynamic Encryption using Stegnography”, International Journal of Emerging Technology and Advanced Engineering (IJETAE), ISSN:2250-2459, Vol.2, Iss.9, Sep 2012.

[22.] Soniya Goyat, “Genetic Key Generation for Public Key Cryptography”, International Journal of Soft Computingsa and Engineering (IJSCE), Vol.2, Iss.3, Jul 2012

[23.] Khatri T.S and Jethava G.B, “Improving dynamic data integrity verification in cloud computing”, Computing, Communications and Networking Technologies (ICCCNT), Fourth International Conference, pp.1-6, Jul 2013.

[24.] Sarthak R Patel, Prof. Khushbu Shah, “Security Enhancement and Speed Monitoring of RSA Algorithm”, IJEDR, Vol. 2, Iss. 2, 2014.

[25.] Snehal Javheri and Rahul Kulkarni, “Secure Data communication and Cryptography based on DNA based

Message Encoding", International Journal of Computer Applications, Vol.98, Iss. 16, Jul 2014.

[26.] Motasem.A., Abu-Dawas and Abdulameer K.Hussain, "Enhancement of RSA Scheme using Agreement Secure Information for Nearest Parameters", International Journal of Computer and Information Technology, Vol.04, Iss.02, Mar 2015.

[27.] S.M.Poonkuzhali, M.Therasa, "Data Hiding Using Visual Cryptography for Secure Transmission", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Iss.4, Apr 2015.

[28.] Rezvaneh Babazade Gorji, Mirsaeid Hosseini Shirvani and Farhad Ramezani Mooziraji, "A new Image Encryption Method using Chaotic map", Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol.2, Iss.2, Feb 2015.

[29.] Xuejing Kang, Feng Zhang, "Multichannel Random Discrete Fractional Fourier Transform", IEEE Signal Processing Letters, Vol. 22, Iss. 9, Sep 2015

[30.] Guero Shay, and Vlad Krasnov, "Speeding up Big-Numbers Squaring", Information Technology: New Generations (ITNG), Ninth International Conference on. IEEE, 2012

[31.] Anizha Radhakrishnan, Seena George, "An Area-efficient Montgomery Modular Multiplier for Cryptosystems", Int. Journal of Engineering Research and Applications, Vol.4, Iss. 9, pp.210-214, Sep 2014

[32.] Mani.K, "Generation of Addition Chain using Deterministic Division Based Method", International Journal of Computer Science & Engineering Technology (IJCSET), Vol.4, Iss. 05, May 2013

[33.] Koon - Shik Cho, Je - Hyuk Ryu, and Jun - Dong Cho, "High speed modular multiplication Algorithm for RSA cryptosystem", Industrial Electronics Society, IECON'01, The 27th Annual Conference of IEEE. Vol. 1. IEEE Xplore 2001.

[34.] Jaspreet Singh and Sandeep Singh Kang,"Security Enhancement in WEP by Implementing Elliptic Curve Cryptography Technique", International Journal of Soft Computing and Engineering (IJSCE), Vol.2, Iss.5, Nov 2012.

[35.] Vollala.S.,Varadhan, V.V. Geetha,K. "Efficient modular multiplication algorithms for public key cryptography", Advance Computing Conference (IACC), IEEE International, pp: 74–78, Feb 2014.

[36.] Anil Hingmire, "Data Encryption / Decryption process using PSZ methodology and performance Analysis with RSA", International Journal of Engineering Research and Applications (IJERA), Mar 2012

[37.] Imran Alam M.D and Mohammad Rafeek Khan., "Performance and Efficiency Analysis of Different Block Cipher Algorithms of Symmetric Key Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.3, Iss.10, Oct 2013.

[38.] Rama Chandra Rao GAV, Lakshmi P .V and Ravi Shankar.N, "A Novel Modular Multiplication Algorithm and its Application to RSA Decryption", IJCSI International Journal of Computer Science Issues, Vol.9, Iss.6, 2012.

[39.] Rama Chandra Rao GAV, Lakshmi P.V and Ravi Shankar.N, "RSA Public Key Cryptosystem using Modular Multiplication", International Journal of Computer Applications, Vol.80, Iss.5, Oct 2013.

[40.] Shaina Arora and Pooja, "Enhancing Cryptographic Security using Novel Approach based on Enhanced-RSA and Elgamal: Analysis and Comparison", International Journal of Computer Applications, Vol.112, Iss.13, Feb 2015.

[41.] Amin.A.E. and Abd Elbadea.A., "Building Cryptosystem Based on Genetic Algorithm and Pattern Recognition Concepts for Academic Institution", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.4, Iss.10, Oct 2014.

[42.] Sonal Sharma, Jitendra Singh Yadav and Prashant Sharma, "Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol.2, Iss.8, Aug2012.

[43.] Liu, Rui and Xiaoping Tian. "New Algorithm For Color Image Encryption Using Chaotic Map and Spatial Bit-Level Permutation" Journal of Theoretical & Applied Information Technology, Vol.43, Iss.1, 2012.

[44.] Omer K. Jasim Mohammad, Safia Abbas, El-Sayed M. El-Horbaty and Abdel-Badeeh M. Salem, "A New Trend of Pseudo Random Number Generation using QKD", International Journal of Computer Applications, Vol.96, Iss.3, Jun 2014.

[45.] Ravi Shankar Dhakar and Anit Kumar Gupta, "Modified RSA Encryption Algorithm (MREA)", International Conference on Advanced Computing and Communication Technologies, IEEE Xplore 2012.