International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 2, March - April 2016 ISSN 2278-6856

Comparative Study of Different Cryptographic Algorithms

Ankita Verma[1,*], Paramita Guha[2] , Sunita Mishra[3]

[1] Department of computer science and engineering, Thapar University, 147001 Patiala
*** Corresponding Author**

[2] CSIR-Central Scientific Instruments Organization, 160030 Chandigarh

[3] CSIR-Central Scientific Instruments Organization, 160030 Chandigarh

Abstract

Since large amount of data has debouched in the coming years, Data security has become the most important aspect of information sharing. We put more private data in the cloud ever since cloud came into the technology life. Practically, the quantity of data to be transferred is not the concern. The important factor is the Channel, through which the data is transferred, should be secured. Cryptography is one such technique which is responsible for secure transmission of the data. And, using cryptographic techniques we can provide security to the information, over the air. This paper classifies the two types of Encryption Algorithm, Symmetric and Asymmetric Encryption Algorithm, and presents a comparative survey on its types like AES, DES, RSA and BLOWFISH.

Keywords: Cryptography, Symmetric Algorithms, Asymmetric Algorithms, AES, DES, RSA and BLOWFISH

1. INTRODUCTION

Cryptography also termed as “secret writing” is a science of concealing information so that only the intended parties can have access to the private information. It protects the privacy and modification of data which may occur due to active and passive attacks in the channel. Cryptographic techniques such as symmetric and asymmetric encryption algorithm ensure integrity, confidentiality, non-repudiation and authenticity of secret data. These days millions upon millions of secure and encoded transmissions happen online every day and cryptographic standards are used to protect the dozens of data processed from different sectors. Cryptography consists of two things – Plain text and Ciphertext [1]. Plain text in the original data which the sender intends to send and Ciphertext is the encrypted format of the plain text. The plain text is converted to the Ciphertext and vice versa with the help of an encryption and decryption algorithm. The encryption-decryption algorithms are mainly classified into two type e.g. symmetric key algorithm and

asymmetric key algorithm. In this paper, different encryption algorithms are discussed along with their applications. The paper is organized in the following way. In the next section, different symmetric key algorithms are discussed in detailed. In Section III, classification of asymmetric algorithms is given. A comparative analysis of the above algorithms is explored in Section IV. Finally, the paper is concluded with the subsequent Section.

2. SYMMETRIC KEY ALGORITHMS

Symmetric algorithm is also called shared key cryptography [1],[2]. During data transmission, the sender and the receiver share the same key for encryption and decryption. To maintain confidentiality, this key needs to be kept secured. If the key for communication is leaked out the data can be stolen by the attacker. There are different types of symmetric algorithms like Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Blowfish.

2.1 Data Encryption Standard (DES)Algorithm

Data Encryption Standard (DES) is a symmetric key block cipher algorithm which was developed by IBM in 1977. It uses a block size of 64-bits and a key size of 56-bits (where 8bits are the parity bits) to encrypt the plain text which is 64bit in size. It consists of a *fiestal* network which divides a block into two equal Halves where the right half passes through a function. DES has series of S-boxes and P-boxes [1]. After passing through the initial permutation and substitution box the cipher text is obtained by the EX-or operation which takes place within the set of rounds. Decryption is just the reverse process. Since DES is vulnerable to brute force attacks therefore it is proven inadequate in terms of security. In [3] the DES algorithm has been modified (called M-DES) to improve the Bit Error Rate(BER)rate caused due to avalanche effect and is made more secure so that it can be used in wireless communication. To carry out this modification the authors have made use of S-box mapping tables. The second modification has been done from the work in [4] where the authors have shown that DES can be cracked from the differential cryptanalysis attack if 247 pairs of Plain text and Ciphertext are present. After the simulation the author in [3] observed that BER rate is much better than DES because there is no Avalanche effect in MDES and as expected the algorithm came out with good results. After plotting and comparing the values of throughput obtained in [3] and [4], it was observed that the proposed algorithm outperforms the use of the fixed 256-AES algorithm. It proved be powerful when the channel conditions were worst. Apart from BER rate throughput of the Encryption Algorithm must also be kept in mind so, in [5] the author maintained a tradeoff between security and throughput.

2.2 Triple Data Encryption Standard (3DES) Algorithm

Triple Data Encryption Standard (3DES) is a modified version of DES and was introduced by IBM in 1978 to enhance the security of the data. It uses block size of 64-bits with a key length of 56bits. As the name suggests it performs the same DES algorithm 3 times to each data block. Although the algorithm is vulnerable to brute force attack but it is comparatively more secure than DES [2]. In [4] the author has shown a round addition attack in Triple DES using Differential analysis [6]. The secret key extracted by the attack can easily obtain one correct Ciphertext and two incorrect Ciphertext. Since triple DES is used in many applications today counter measures must be taken to implement a modified algorithm. In [7] the application of the triple DES has been discussed in the implementation of VLSI. Three different hardware implementations have been proposed where the first two are related to pipeline techniques and the third one is used for consecutive iterations for data transformations. T-DES has been implemented by look up tables and ROM blocks providing information regarding throughput and design area. With these implementations simulation was done to check out for the correct functionality. It was found that the result was validated by the know answer test vector mentioned in [8]. The authors have shown that ROM blocks provide better performance and throughput results as compared to the look up tables.

2.3 Advanced Encryption Standard (AES) Algorithm

After looking up the vulnerabilities in DES and 3DES, the National Institute of Standard and Technology (NIST) developed a new algorithm called Advanced Encryption Standard (AES) as a replacement to the two algorithms. AES consists of basically 3 block ciphers, AES-128, AES -192 and AES-256. AES-128 has a key of length 128 bits consisting of 10 rounds, AES-192 has a key of length 192 bits consisting of 12 rounds, AES-256 has a key length of 256 bits consisting of 14 rounds. Each round goes through a series of steps i.e. Substitution Byte, Shift rows, mixed columns and Add Round Key [9]. AES Algorithm is comparatively more secure and has a strong avalanche effect. Attackers cannot easily decrypt the encrypted text by the brute force attack. Therefore AES has been used in many applications. In [9], the implementation of AES for PDA secure communication has been described. The author introduces a linear complexity in the design of AES to make it more secure. There are many attacks the AES algorithm has undergone. An attack which is a combination of boomerang and rectangle attack with related key differentials introduced in [10]. This attack can break the round versions of AES. In [9] short cut attacks have been defined which are dangerous to the three AES block ciphers. There are attacks which occur due to the vulnerability of S-box in AES algorithm. In [11] authors have introduced a new way of generating S-box which can help from the algebraic attack. Authors also added their contribution to make up for the weakness of S-box and introduced an iterated hill climbing algorithm for the design of S-box [12]. After further discussions new Algorithms were proposed to overcome the weakness in S-box design [13], [14]. In [15] author describes the security that AES Algorithm provides in accounting information where (Accounting Information Security System) AISS protect the accounting information data. The design of AISS based on AES is made which provides security from both internal and external attacks. Data security with Steganography and AES is also discussed [16]. Since AES algorithm is secure, it is used in hybrid form with other encryption algorithm, forming an onion layered structure and providing more security [17]. A modified version of AES was introduced to carry out MPEG video encryption. The algorithm was modified just to overcome calculations and computer overhead. A drastic improvement in the speed and encryption performance has been observed [18].

2.4 Blowfish Encryption Algorithm

Out of all the symmetric key algorithms, Blowfish Encryption Algorithm is the most efficient one. Blowfish Algorithm was developed by Bruce Schneier in 1993 as an alternate to another encryption algorithm and providing effective data encryption. It has a variable key length up to 448 bits. It has a block size of 64-bits. Blowfish algorithm consists of two phases. In the key expansion phase, 448 bit key is converted into number of sub keys totaling 4168 bytes [19]. In encryption phase, a function is iterated 16 times and the encrypted text is obtained using EX-OR operation. Blowfish is a strong encryption algorithm so it has been used in many applications. In [19] the author has shown nested watermarks which are embedded in a main image and these watermarks are encrypted before embedding using blowfish algorithm. Results show a remarkable embedded capacity and security in the watermarks. Tests were done to check the performance of blowfish algorithm by increasing the file size and the key length [20]. The equations derived from the result are kept for evaluating future performances. The design and implantation of Password Management System is also based on Blowfish Algorithm [21].The algorithm has also been used in bitmap image plotting instead of using secret algorithm like Skipjack algorithm in the Clipper and Capstone chips [22], [23]. Blowfish Algorithm has been used with other encryption Algorithms in hybrid form to enhance security and performance [24], [25]. Performance was also evaluated by modifying its function which brought up subsequent impressive results [26]. In the next section, different asymmetric algorithms available for the cryptography along with their applications are discussed in detail.

3. ASYMMETRIC KEY ALGORITHM

Asymmetric Algorithm is also called public key cryptography. It uses two keys ‘Private key’ and ‘Public key’. During data transmission, the sender encrypts the plain text with the help of public key known as the cipher text and the receiver decrypts this cipher text with the help of its private key. The different types of asymmetric algorithms are Rivest Shamir Adlemen (RSA), Diffie-Hellman and Digital Signature Algorithm.

3.1 Rivest Shamir Adlemen (RSA)

The algorithm was developed by Rivest, Shamir and Adlemen in 1977. It is a public key algorithm because it uses two keys pairs to encrypt and decrypt the message. Public key is used by the sender to encrypt the text and is known to all. However, to decrypt the encrypted text private key of the receiver is used. This private key, as the name suggests is known only to the receiver. No one else in the network has any knowledge about the key. The RSA consists of some mathematical operations through which one can calculate the encryption and decryption keys (e and d), after that one can easily calculate the cipher text and the plain text by the following formulae

$$C = M^{e} \bmod(n) \qquad (1)$$

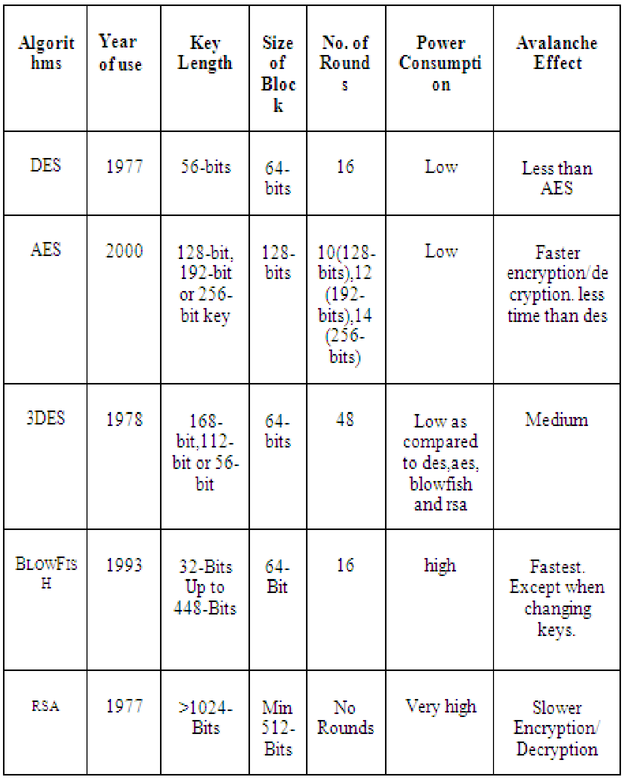
$$P = M^{d} \bmod(n) \qquad (2)$$

Where in (1) and (2) M is the original message, e and d are public and private keys and n is a value obtained from mathematical operations in RSA [27]. To carry out performance analysis RSA was modified. In [28], the author has introduced an improved version of RSA which is based on complex numeric operation resulting in comparatively low computational power. The authors have proposed a mechanism to speed up large mathematical calculations by implementing the numeric operation on the array resulting in a low computational power . With this the loop time is decreased and the calculation speed is improved greatly. Although RSA is a secure algorithm, but in [29] an experiment was done in the application of low private exponent attack in RSA where the author found out that there can be some new weak keys in RSA. Therefore, digital signature concept was introduced in combination with RSA [30]. Keeping all the flaws in mind, in [31] an algorithm implementing Digital Signature with RSA Algorithm was proposed to double the security of the algorithm. The RSA has been used in various applications like in electronic commerce trade which ensures integrity, confidentiality, authentication and non-repudiation. This algorithm is also used in the construction of mercurial commitments and with this it has shown its contribution in zero knowledge databases as well [32]. In the next section, a comparative analysis of different algorithms is given.

4. COMPARATIVE ANALYSIS

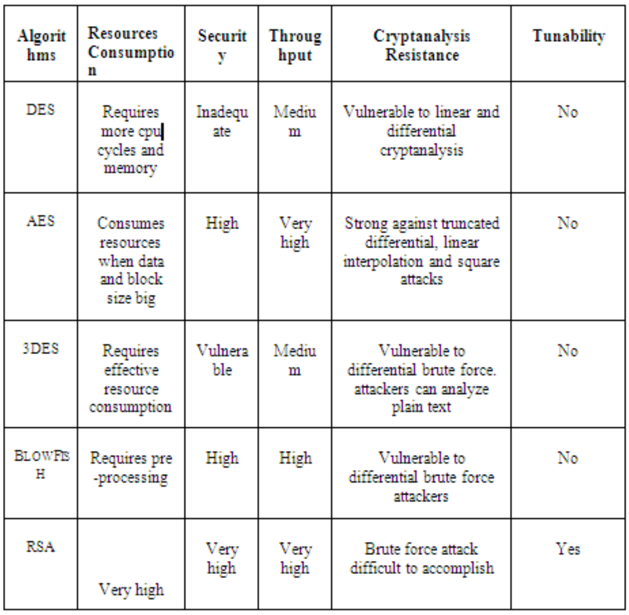
The Table I shows the comparative analysis between different symmetric and asymmetric algorithms at different settings of key algorithms such as the key length, block size, rounds, power consumption, avalanche effect, processing time resource consumption and many other platforms. Authors in [33] have made many comparisons between the algorithms of the same type and reached to a conclusion that AES is faster and efficient than all other encryption algorithms. In [34] the authors have encrypted files with different contents and sizes. The results proved that Blowfish showed a good performance than the other encryption algorithms and therefore the processing time of the blowfish algorithm was high. AES performance was better than DES and 3DES and it took less time in encryption and decryption. Next property, Avalanche effect is a property of block ciphers in which the output bits change significantly on a slight change of the input bits. Blow fish has a maximum avalanche effect due to the number of EX-or operations which changes the output drastically. DES has avalanche lower than AES [35]. RSA also has high avalanche effect as it involves the mathematical calculation of two large prime numbers. Now, talking about cryptanalysis resistance, authors have explained differential cryptanalysis for each of the algorithm. It was observed that DES is highly vulnerable to linear and differential cryptanalysis. It was also found that 3DES and Blowfish were vulnerable to brute force attacks whereas in case of RSA brute force attack was difficult. AES proved to be strong against differential, linear interpolation and square attacks [36]. Therefore the crack to AES algorithm has not been found yet. Comparing with the other algorithms only DES is the most insecure algorithm as it has already been declared inadequate to use.

Table1: Comparative analysis of different cryptography algorithms



Algorithms	Year of use	Key Length	Size of Block	No. of Rounds	Power Consumption	Avalanche Effect
DES	1977	56-bits	64-bits	16	Low	Less than AES
AES	2000	128-bit, 192-bit or 256-bit key	128-bits	10(128-bits),12 (192-bits),14 (256-bits)	Low	Faster encryption/decryption. less time than des
3DES	1978	168-bit,112-bit or 56-bit	64-bits	48	Low as compared to des,aes, blowfish and rsa	Medium
BLOWFISH	1993	32-Bits Up to 448-Bits	64-Bit	16	high	Fastest. Except when changing keys.
RSA	1977	>1024-Bits	Min 512-Bits	No Rounds	Very high	Slower Encryption/ Decryption

Table2: Comparative analysis of different cryptography algorithms



Algorithms	Resources Consumption	Security	Throughput	Cryptanalysis Resistance	Tunability
DES	Requires more cpu cycles and memory	Inadequate	Medium	Vulnerable to linear and differential cryptanalysis	No
AES	Consumes resources when data and block size big	High	Very high	Strong against truncated differential, linear interpolation and square attacks	No
3DES	Requires effective resource consumption	Vulnerable	Medium	Vulnerable to differential brute force. attackers can analyze plain text	No
BLOWFISH	Requires pre -processing	High	High	Vulnerable to differential brute force attackers	No
RSA	Very high	Very high	Very high	Brute force attack difficult to accomplish	Yes

5. CONCLUSION

This paper presents a comparative study of different key algorithms like, AES, DES, 3DES, Blowfish and RSA. Each algorithm has been compared on different set of parameters. From the results it has been found that among the symmetric encryption algorithm, AES and Blowfish are the most secure and efficient algorithms. The speed and power consumption of these algorithms are better compared to the others. In case of asymmetric encryption algorithm, RSA is secure and can be used for application in wireless network because of its good speed and security.

References

[1]. T. Bala and Y. Kumar, “Asymmetric Algorithms and Symmetric Algorithms: A Review,” International Journal of Computer Applications (ICAET), pp.1-4, 2015.

[2]. W. Stallings, Cryptography and Network Security, 4th Ed, pp. 58-309, Prentice Hall,2005.

[3]. W. Y. Zibideh and M. M. Matalgah , “Modified-DES Encryption Algorithm with Improved BER Performance in Wireless Communication,” IEEE Radio and Wireless Symposium (RWS) Phoenix, pp.219-222 , Jan 2011.

[4]. H.Yoshikawa, M. Kaminaga, A. Shikoda, and T. Suzuki,“Round addition DFA for microcontroller implemented the Triple DES,” IEEE Consumer Electronics (GCCE) Tokyo, pp. 538-539, October 2013.

[5]. W.Y Zibideh. and M. M. Matalgah , “An Optimized Encryption Framework based on the Modified-DES Algorithm: A Trade-Off between Security and Throughput in Wireless Channels,” IEEE Radio and Wireless Symposium (RWS) CA , pp.419-422, Jan 2012.

[6]. E.Biham and A.Shamir, “Differential Cryptanalysis of the Full 16- Round DES,” Proceedings of Crypto’92,vol. 740, Santa Barbara, CA, December 1991.

[7]. P. Kitsos, S. Goudevenos and O. Koufopavlou, “VLSI implementations of the triple-DES block cipher,” IEEE Electronics Circuits and Systems, Vol. 1, pp.76-79, December 2003.

[8]. NIST Special Pubilication 800-20, “Modes of Operation Validation System for the Triple Data Encryption Algorithm,” National Institute of Standard and Technology, 2000.

[9]. LIU Niansheng , G. Donghui, and H. Jiaxiang, “AES Algorithm Implemented for PDA Secure Communication with Java,” IEEE Anti-counter. Sec. Ident. Fujian, pp. 217-222, April 2007.

[10]. E.Biham, O. Dunkelman, and N. Keller, “Related-Key Boomerang and Rectangle Attacks,” Lecture Notes in Computer Science, vol. 3494, pp. 507-525, Berlin: Springer-Verlag,2005.

[11]. Y. A. Zhang and D.G. Feng, “Equivalent Generation of the S-box of Rijndael,” Chinese J. Computers, Vol. 27, no.12, pp.1593-1600, December 2004.

[12]. W. Millan, “How to Improve the Nonlinearity of Bijective S-boxes,” Lecture Notes in Computer Science, Vol. 1438,pp.181 - 192, Berlin: Springer-Verlag, 1998.

[13]. Chen and D. G. Feng, “An Evolutionary Algorithm to Improve the Nonlinearity of Self-inverse S-Boxes,” Lecture Notes in Computer Science, vol. 3506, pp.352 - 361, Berlin: Springer-Verlag, 2005.

[14]. J. M. Liu, B. D. Wei, and X.G. Cheng,“An AES S-Box to Increase Complexity and Cryptographic Analysis, ” IEEE Proc. of the 19th International Conference on Advanced Information Networking and Applications China, Vol. 1, pp. 724-728, March 2005.

[15]. Q. X. Zhu, L. li , J. Liu, N. Xu, “The analysis and design of accounting information security system based on AES algorithm,” IEEE Machine Learning and Cybernetics Boading , vol. 5, pp. 2713 -2718, July 2009.

[16]. S. Mare, M. Vladutiu and L. Prodan, “Secret data communication system using Steganography, AES and RSA,” IEEE Design and Technology in Electronic Packaging (SIITME) Timisoara, pp.339-344, October 2011.

[17]. V. Mahalle , A.K Shahade , “Enhancing the Data Security in Cloud by Implementing Hybrid(Rsa & Aes) Encryption Algorithm,” IEEE Power, Automation and Communication (INPAC)Amravati, pp. 146-149,October 2014.

[18]. P. Deshmukh and V. Kolhe, “Modified AES Based Algorithm for MPEG Video Encryption,” IEEE

Information Communication and Embedded Systems (ICICES) Chennai, pp.1-5, Feb 2014.

[19]. J. Bhalla, P. Nagrath , "Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm," ISSN International Journal of Scientific and Research Publications, Vol. 3, pp.1-6,April 2013.

[20]. A.

Mousa , "Data Encryption Performance Based on Blowfish," IEEE ELMAR Symposium Zadar, pp.131-134, June 2005.

[21]. M. Wang and Y. Que, "The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm," IEEE Computer Science-Technology App. IFCSTA Chongqing, Vol. 2, pp.24-28, December 2009.

[22]. N.Palaniswamy, D.Dugar M, D.K. Jain, R. Sarabhoje, " Enhanced Blowfish Algorithm using Bitmap Image Pixel Plotting for Security Improvisation," Education Technology and Computer (ICETC) Shanghai, Vol.1, pp.V1-533 - V1-538, June 2010.

[23]. National Institute of Standards and Technology, "Clipper Chip Technology," 30 Apr 1993.

[24]. R.Rivest, A.Shamir, and L.Adleman, "A Method For Obtaining Digital Signatures and Public Key Cryptosystems," ACM Transactions on Communications, Vol. 21, pp. 120-126, 1978.

[25]. T. Nie and T. Zhang "A Study of DES and Blowfish Encryption Algorithm," IEEE TENCON Singapore, pp.1-4, Jan 2009.

[26]. G.N. Krishnamurthy, V. Ramaswamy , G.H. Leela "Performance Enhancement Of Blowfish Algorithm By Modifying Its function," SPRINGER Innovative Algorithms and Techniques in Automation Industrial Electronics Telecom. Netherlands , pp 241-244, 2007.

[27]. Ying-yu Cao, Chong Fu, "An Efficient Implementation of RSA Digital Signature Algorithm," IEEE Wireless Communications Networking and Mobile Computing (WiCOM) Dalian, pp.1-4, October 2008.

[28]. Hongwei Si, Youlin Cai, Zhimei Cheng, "An Improved RSA Signature Algorithm based on Complex Numeric Operation Function," IEEE Challenges in Environmental Science and Computer Engineering (CESCE) China, Vol.2, pp.397-400, March 2010.

[29]. Yong-Hui Zheng, Yue-Fei Zhu, Hong Xu , "An Application of Low Private Exponent Attack on RSA," IEEE Computer Science & Education(ICCSE) Nanning ,pp.1864-1866, July 2009.

[30]. U.Somani , K.Lakhani , M.Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," IEEE Parallel Distributed and Grid Computing (PDGC) Solan , pp.211-216, October 2010.

[31]. LIU Dong-liang, CHEN Yan-ping, Z. Huai-ping, "Secure Applications of RSA System in the Electronic Commerce," IEEE Future Information Technology and Management Engineering (FITME) Changzhou, Vol. 1, pp.86-89, Oct. 2009.

[32]. Huafei Zhu, " Mercurial Commitments from General RSA Moduli and Their Applications to Zero-knowledge Databases/Sets," IEEE Computer Science and Engineering WCSE Qingdao, Vol. 2, pp.289-292, Oct. 2009.

[33]. M. Ebrahim, S.Khan and U.B.Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications, Vol. 61,pp.12-19, January 2013.

[34]. A.

Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms," Information and Communication Technologies, ICICT 2005, pp.84-89, 2005.

[35]. Singhand and Supriya , "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security, " IEEE International Journal of Computer Applications, ,vol.67,pp.33-38, April 2013.

[36]. M. Ebrahim, S. Khan and U. Khalid , "Symmetric Algorithm Survey: A Comparative Analysis," International Journal of Computer Applications,Vol. 61, pp. 12-19, January 2013.

AUTHORS

Ankita Verma received the B.tech degree in Computer science engineering from Punjabi university in 2013. During 2014-2016 she did her masters from Thapar University, Patiala. Her research interests are in security, cryptographic Algorithms and networking.

Paramita Guha graduated from Jalpaiguri Government Engineering College, India in 2001. She received her master's degree from Bengal Engineering College (Deemed University), India in 2003 and Ph.D. degree from Indian Institute of Technology (IIT), Delhi, India in 2012, both in electrical engineering. She is presently working as a scientist in CSIR-Central Scientific Instruments Organization, Chandigarh, India. She has published several papers in international journal and conferences. Her research interests include distributed parameter systems, coupled systems, modeling and simulation, model reduction and control theory.

Sunita Mishra did her graduation and post-graduation in physics in the year 1983 and 1985, respectively from Allahabad University, Allahabad. She obtained her Ph.D. degree in physics-electronics engineering from Institute of Technology, Banaras Hindu University, Varanasi in 1993. At present she is working as a principal scientist in CSIR-Central Scientific Instruments Organization, Chandigarh. She has published about 25 papers in journals and conference proceedings. Her research interests include sensors, semiconductor devices, and NIR spectroscopy.