Cryptography Algorithms: A Review

Anjula Gupta[1] Navpreet Kaur Walia[2]

Department of Computer Science
Sri Guru Granth Sahib World University, Fatehgarh Sahib, India
[1]anjula21gupta@gmail.com, [2]navpreet.walia12@gmail.com

***Abstract*--Cryptography is derived from Greek word 'crypto' means secret 'graphy' means writing that is used to conceal the content of message from all except the sender and the receiver and is used to authenticate the correctness of message to the recipient. Today information security is the challenging issue that touches many areas such as computers and communication. Cryptography is such a way that make sure of integrity, availability and identification, confidentiality, authentication of user and as well as security and privacy of data can be provided to the user. In this paper we have defined and analysed various cryptographic symmetric algorithms like DES, Triple DES, Blowfish, AES and IDEA and asymmetric key cryptographic algorithms like RSA. They have been analysed on their ability to secure data, key size, block size, features.**

***Keywords*-- Cryptography, Encryption, DES, Diffie Hellman, RC5, Triple DES, AES, RSA.**

I. INTRODUCTION

Cryptography is derived from Greek word . It has 2 parts: 'crypto' means "hidden, secret" and 'graphy' means "writing". It is a study of techniques for secure communication in the presence of third parties to maintain information securities such as data integrity, confidentiality , authentication, and non-repudiation. It is an art to transform the messages to make them secure and immune against security attacks. The art of protecting information by transforming into an unreadable format, called cipher text or decrypt the message into plain text. The cipher text is only understood by someone who only knows how to decrypt it. The information is encrypted using an encryption algorithm, which specifies how the message is to be encoded. Any intruder that can see the cipher text should not be able to determine about the original message. Only an authorized party is able to decode the cipher text which requires a secret decryption key.

A. *Types of Cryptography*

There are two types of cryptography:

1) Secret key cryptography or Symmetric-key cryptography: In SKC, the sender and the receiver know the same secret code, which is known as key. With the same key messages are encrypted by the sender and decrypted by the receiver. It can be of 2 types : Stream Buffer, Block Buffer.Stream Buffer: Stream buffer encrypts the digits of a message one at a time. Stream Cipher functions is used on a stream of data one at time by operating on it by bits. It consists of two components: 1) a key stream generator and 2) mixing function. Mixing function uses XOR function, and key stream generator is unit in stream encryption algorithm.Block cipher : In Block cipher, it takes a number of bits and then encrypt them as a single unit. Data is encrypted/decrypted if data is in the forms of blocks. In simple words , the plain text is divided into blocks which are used to produce blocks of cipher text padding the plaintext in blocks. 64 bits blocks have been commonly used.

2) Public key cryptography or Asymmetric-key cryptography: Asymmetric key (or public key) encryption is used to solve the problem of key distribution. In PKC, two keys are used; private keys and public keys. For encryption public key is used and for decryption private key is used . Public key is known to public and private key is known to the user.

B. *Cryptography Goals*

There are some goals of cryptography that are given below:

1) Authentication: Sender and data receiver must be authenticated before sending and receiving data.
2) Confidentiality: The user who is authenticated, can access the messages
3) Integrity: Data is free from any kind of modification between sender and receiver.
4) Non-Repudiation:The sender the receiver cannot deny that they had sent a message.
5) Service Reliability: Attackers can attack on secure systems, which may affect the service of the user.

The remainder of this paper is organized as follows.: In Section 2. we briefly mention Cryptography Algorithms , Section 3. Literature Survey, Section 4. Comparison of Cryptography Techniques , Section 5. Conclusion .

II. CRYPTOGRAPHY ALGORITHMS

The various cryptography algorithms are as follows :

A. Data Encryption Standard (DES)

DES is a block encryption algorithm. It was the first encryption standard published by NIST. It is a symmetric algorithm, means same key is used for encryption and decryption. It uses 64-bit key. Out of 64 bits, 56 bits make up the independent key , 8 bits are used for error detection. The main operations are bit permutations and substitution in one round of DES. Six different permutation operations are used both in key expansion part and cipher part. Decryption of DES algorithm is similar to encryption, only the round keys are in reverse order. The output is a 64-bit block. Many attacks and methods recorded weaknesses of DES, which has made it an insecure block encryption key.

B. 3DES (Triple DES)

3DES is an enhancement of Data Encryption Standard. It uses 64 bit block size with 192 bits of key size. The encryption method is similar to the original DES but it applied 3 times to increase the safe time and encryption level . Triple DES is slower than other block encryption methods. It has the advantage of reliability and a longer key length that eliminates many shortcut attacks. 3DES can be used to reduce the amount of time to break DES.

C. AES (Advanced Encryption Standard)

AES also known as the Rijndael's algorithm , is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power. It encrypts data blocks of 128 bits using symmetric keys. It has a variable key length of 128, 192 or 256 bits : by default 256 is used. AES encrypts 128 bits data block into 10, 12 and 14 round according to the key size. AES can be implemented on various platforms suxh as small devices encryption of AES is fast and flexible . AES has been tested for many security applications. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies.

D. Blowfish

It is one of the most public domain encryption algorithms. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length from 32 bits to 448 bits. Blowfish has 16 rounds or less. Blowfish is a very secure cipher and to use encryption free of patents and copyrights. No attack is successful against Blowfish, although it suffers from weak keys problem.

E. IDEA(International Data Encryption Algorithm)

IDEA is a block cipher algorithm and it operates on 64-bit plaintext blocks. The key size is 128 bits long. The design of algorithm is one of mixing operations from different algebraic groups. Three algebraic groups are mixed, and they are easily implemented in both hardware and software: XOR, Addition modulo 216 , Multiplication modulo 216 + 1. All these operations operate on 16-bit sub-blocks. This algorithm is efficient on 16-bit processors. IDEA is symmetric key algorithm based on the concept of Substitution-Permutation Structure, is a block cipher that uses a 64 bit plain text with 8 rounds and a Key Length of 128-bit permuted into 52 sub- keys each of 128- bits. It does not contain S- boxes and same algorithm is used in reversed for decryption .

F. RC4

RC4 is a stream cipher symmetric key algorithm. as the data stream is simply XOR with generated key sequence. It uses a variable length key 256 bits to initialize a 256-bit state table. A state table is used for generation of pseudo-random bits which is XOR with the plaintext to generate the cipher text.

G. RC6

RC6 is a derivative of RC5. RC6 is designed by Matt Robshaw, Ron Rivest Ray Sidney and is a symmetric key algorithm that is used to congregate the requirements of AES contest . RC6 was also presented to the CRYPTREC and NESSIE projects. It is patented by RSA Security . RC6 offers good performance in terms of security and compatibility. RC6 is a Feistel Structured private key algorithm that makes use a 128 bit plain text with 20 rounds and a variable Key Length of 128, 192, and 256 bit. As RC6 works on the principle of RC that can sustain an extensive range of key sizes, word-lengths and number of rounds, RC6 does not contain S- boxes and same algorithm is used in reversed for decryption.

H. Serpent

Serpent is an Advanced Encryption Standard (AES) competition, stood 2nd to Rijndael, is a symmetric key block cipher, designed by Eli Biham, Ross Anderson, and Lars Knudsen. Serpent is a symmetric key algorithm that is based on substitution-permutation network Structure. It consists of a 128 bit plain text with 32 rounds and a variable Key Length of 128, 192 and 256 bit. It also contains 8 S- boxes and same algorithm is used in reversed for decryption. Security presented by Serpent was based on more conventional approaches than the other AES finalists. The Serpent is open in the public sphere and not yet patented.

I. Twofish

Twofish is also a symmetric key algorithm based on the Feistel Structure and was designed by Bruce Schneier along with Doug Whiting, John Kelsey, David Wagner, Niels Ferguson and Chris Hall,. The AES is a block cipher that uses a 128 bit plain text with 16 rounds and a variable Key Length of 128, 192, 256 bit. It makes use of 4 S-boxes (depending on Key) and same algorithm is used in reversed for decryption. The inventors extends the Blowfish team to enhance the earlier block cipher Blowfish to its modified version named Twofish to met the standards of AES for algorithm designing. It was one of the finalists of the AES , but was not selected for standardization. The Twofish is an open to public sphere and not yet patented.

J. TEA

TEA is also a Feistel Structured symmetric key algorithm. TEA is a block cipher that uses a 64 bit plain text with 64 rounds and a Key Length of 128-bit with variable rounds having 32 cycles. It does not contain S- boxes and same algorithm is used in reversed for decryption. TEA is designed to maximize speed and minimize memory footprint. Cryptographers have discovered three related-key attacks on TEA. Each TEA key can be found to have three equal keys, thus it can be used as a hash function. David Wheeler and Roger Needham have proposed extensions of TEA that counter the above attacks.

K. CAST

CAST is symmetric key algorithm based on the backbone concept of Feistel Structure. It is designed by Stafford Taveres and Carlisle Adams, is considered to be a solid algorithm. The CAST is a block cipher that uses a 64 bit plain text with 12 or 16 rounds and a variable Key Length of 40 to128-bit. It also contains 4 S- boxes and same algorithm is used in reversed for decryption. Bruce Schneier , John Kelsey, and David Wagner have discovered a related-key attack on the 64 bit of CAST that requires 2^{17} chosen plaintexts, one related query, and 2^{48}offline computations. CAST is patented, which was generously released it for free use.

L. RC2

RC2 is designed by Ron Rivest and a variable-key-size encryption algorithm from 0 bytes to the maximum string length that the computer system supports. RC2 is a variable-key-size 64-bit block cipher. It is designed to be a replacement for DES. RC2 is three times faster than DES in software implementations. The algorithm encryption speed is independent of key size.

M. RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. It was named after the mathematicians who invented it. RSA was first published in 1997. RSA uses variable size key and encryption block. It uses the 2 prime no. to generate the public and private key based on mathematical fact and then multiplying large numbers together. It uses the block size data in which plaintext and cipher text are integers between 0 and n1 for some n values. Size of n is considered 1024 bits or 309 decimal digits. In RSA two different keys are used for encryption and decryption purpose. As sender knows encryption key and receiver knows decryption key. Main advantage of RSA algorithm is enhanced security and convenience. Using PKC is also an advantage of this algorithm. RSA lacks in encryption speed. RSA may be used to provide both secrecy and digital signature .

N. Diffie-Hellman

This algorithm was introduced in 1976 by Diffie-Hellman. In it, each party generates a key pair and distributes the public key. After obtaining an authentic copy of public keys, then shared secret can be used as the key for a symmetric cipher .The Diffie-Hellman algorithm grants two users to establish a shared secret key and to communicate over an insecure communication channel . One way authentication is free with this type of algorithm. The biggest limitation of this kind of algorithm is communication made using this algorithm is itself vulnerable to man in the middle attack.

O. MD5

MD5's full form is message-digest algorithm. MD5 is derived from MD4 & was designed by Ron Rivest in 1991 . MD5 is widely used hash function producing a 128-bit hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

III. LITERATURE SURVEY

[1] Chia Long et al. had a goal of study time-efficient and space-efficient algorithms, such as RSA cryptography and El-Gamal cryptography.

In RSA cryptography , encryption and decryption operations are accomplished by modular exponentiation. Fast modular exponentiation algorithms were often considered of practical significance in RSA cryptosystem. By using the technique of recording the common parts in the folded sub strings could improve the efficiency of the binary algorithm, thus can effective reduce the computational complexity of modular exponentiation. [2] Qing Liu et al. aimed at speeding up RSA decryption. EAPRSA (Encrypt Assistant Multi-Power RSA) was proposed to improve RSA decryption performance by transferring some decryption computations to encryption. The experimental result showed that the speed of the decryption has been substantially improved .

[3] Mandal et al. designed an algorithm to merge both RSA algorithm and Diffie-Hellman Algorithm to provide a higher level of data security. Actually, their intent was to secure data of smaller as well as larger size by obtaining one randomly chosen key pair from set of RSA keys and one randomly chosen secret key using Diffie-Hellman algorithm and then applying RSA encryption to make even public components of Diffie-Hellman algorithm inaccessible for any eavesdropper freely.

[4] Wang et al. described a complete set of practical solution to file encryption based on RSA algorithm. With analysis of the present situation of the application of RSA algorithm, they found the feasibility of using it for file encryption..The conventional RSA algorithm used C + + Class Library to develop RSA encryption algorithm and realized Groupware encapsulation with 32-bit windows platform.

[5] Silva et al. proposed a very simple and direct algorithm. The technique only applied to the product of two different but equal-sized primes and was based on reversing the decimal digits of the modulus. This algorithm required little memory and was easily parallelized .

[6] Geethavani proposed a new modified blowfish algorithm and resultant cipher text that was embedded into a cover audio file using discrete wavelet transform (DWT). The resultant stego audio was transmitted to the receiver and the reverse process was done in order to get back the original plain text. The proposed method presented a steganographic scheme along with the cryptographic scheme which enhanced the security of the algorithm.

[7] Nagar et al. aimed to speed up the implementation of RSA algorithm during data transmission between networks and Internet which was calculated to generate the keys and then save the values of keys in the databases. In this paper a new method was used to exchange the values of keys between gateways that contain values of public and private keys that were stored in tables inside the database.

[8] Accc to Chong Fu et al. RSA was most widely used in e-commerce . The complexity of large integer operation was the main factor that affects efficiency of RSA system. This paper proposed a n carry array approach was to speed up the large digit calculation in RSA key generation and process of data encryption/decryption process is used to improve the efficiency of a RSA system. RSA algorithm and its mathematics were discussed in detail and then feasibility of RSA algorithm was proved.

[9] Chen Hong et al. to reduce the time and space complexity, this paper presented a study on key generation of RSA public-key cryptosystem. An improved algorithm was introduced to make a screen for the large random number which was generated by the generator. After that Miller-Rabin algorithm was used to make a final prime test. At last Stain algorithm was introduced to generate the public and private keys. The results showed that the research effectively improved the efficiency of RSA key generation.

[10] Turki et al. evaluated the performance of these algorithms in terms of CPU execution time. The analyzed time was the CPU execution time for generating the secret key, encryption and decryption on a 10MB file. The results showed that the Blowfish

algorithm was the fastest algorithm followed by the DES algorithm then the Triple-DES algorithm. The Triple-DES algorithm was slow in its performance due to the added complexity and security it had over the DES algorithm.

[11] Hongwei Si et al. can be realized by using RSA algorithm. RSA was widely used in public-key cryptosystem and digital signature But RSA needs lots of time and memory when it is running . This paper proposed a RSA signature algorithm to fit for the devices with low computational power. The new signature algorithm was based on complex numeric operation function. The realization of RSA algorithm included the generation of RSA cryptographic key and the encryption and decryption of data. In this paper , by using RSA algorithm they used the private key of the sender to sign the plaintext and the public key of the receiver to encrypt. For the receiver, he could use his private key to decrypt and the public key of the sender to verify the signature.

[12] In this paper, the quantization of the RSA key security , the concept of key security coefficient, the evaluation model of security coefficient and the algorithm to extract security strength were initiated. In addition an improved method was used to generate secure keys. Some experiments were operated on the platform of computation Cluster, time performance of key and distribution of key-amount to key security coefficient was analyzed and summarized . The experiment data demonstrated that their mechanism was able to improve the security of RSA.

[13] Gupta et al. gives a new encryption technique called Modified RSA Encryption Algorithm (MREA). MREA was secure as compared to RSA as this scheme was an additive homomorphic cryptosystem , it means from public-key and encryption of m1 and m2, one can compute the encryption of m1 + m2.

[14] Abdul. et.al, (2009) presented a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points were concluded from the experimental results: 1. in the case of changing packet size with and without transmission of data using different architectures and different WLANs protocols, it had been concluded that Blowfish had better performance than other algorithms used for encryption.

[15] Pradhan et al. proposed and performed the test cases on the two PKC methods such as RSA and NTRU Though the encryption, decryption and complexity were high in NTRU, the RSA provided the highest security to the business application. He presented all these parameters with computational running times for all the methods, so it to select the appropriate method .

[16] Karim et al . showed that Blowfish had a better performance than other encryption algorithms by simulation results which makes it an excellent candidate as a standard encryption algorithm. AES showed poor performance results compared to other algorithms because requires more processing power.

[17] Singhal et al. presented the comparative analysis of algorithms that were on throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments showed that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis it was clear that RC4 was better than AES.

[18] Mandal provided a fair comparison between four most common and used symmetric key algorithms: DES, 3DES, AES and Blowfish. A comparison had been made on the basis of these parameters: rounds, block size, key size, encryption/decryption time, CPU process time in the form of throughput and power consumption. These results showed that blowfish is more suitable than AES.

[19] Gurjeevan Singh et al. tested the performance for the algorithms. The performance matrices were throughput. The throughput of encryption time and in the case of decryption scheme was calculated. This work presented the performance evaluation of selected symmetric algorithms such as AES, 3DES, Blowfish and DES that Blowfish had better performance than other algorithms followed by AES in terms of throughput. Secondly 3DES had least efficient of all the studied algorithms .

[20] Kumar et al. analysed Power comparison analysis of Blowfish Algorithm, AES, IDEA and Rijndael Algorithm. In this paper it was clear that blowfish consumed least amount of power as compared to other algorithms. AES consumed most amount of power. IDEA And Rijndael consumes less power than AES but more than blowfish. The result also showed superiority of blowfish algorithm over other algorithms according to time.

[21] Mehrotra et al. analysed the performance of encryption algorithms on parameters like Computation Time, Memory usage and Output Bytes and RSA consumed longest encryption time and memory usage was also very high but output byte was least RSA algorithm.

[22] Singh et al. evaluated the performance of four symmetric algorithms; AES, DES, 3DES and Blowfish which were commonly used for data encryption in terms of throughput and encryption/decryption time. Experimental results showed that Blowfish encryption algorithm was more suitable for wireless networks and Blowfish gave better performance than AES, DES and 3DES in terms of encryption/decryption time & throughput.

[23] Agarwal et al. had a goal of guiding the design of any encryption algorithm against unauthorized attacks. This paper provided the performance comparison between four of the commonly used encryption algorithms such as DES, Triple DES, BLOWFISH and AES. The comparison had been conducted by running different sizes of the data blocks to evaluate the speed of the encryption and decryption algorithm. From the performance analysis of these algorithms, it had been concluded that the Blowfish was the best performing algorithm under the security against unauthorized attack and speed.

[24] Acc. to Ramesh et al. information security had become an important issue in data communication. Encryption algorithms played an important role in information security system. Those algorithms that consumed a computing resources such as CPU time, battery power, memory so it becomes essential to measure the performance of cryptographic algorithms. DES, AES and Blowfish were analyzed by measuring performance such as memory, execution time required for throughput and implementation. Thus from experiments, it had been showed that the Blowfish is the best algorithm that is chosen for implementation.

IV. COMPARISON ANALYSIS

The comparison of all above cryptography techniques is given in Table 1

COMPARISON OF VARIOUS CRYPTOGRAPHY TECHNIQUES								
Algorithm	**Created By**	**Year**	**Key Size**	**Block**	**Round**	**Structure**	**Flexible**	**Features**

				Size				
DES	IBM	1975	64 bits	64 bits	16	Festial	No	Not Strong Enough
3DES	IBM	1978	112 or 168	64 bits	48	Festial	Yes	Adequate Security
AES	Joan Daemen & incent Rijmen	1998	128, 192, 256 bits	128 bits	10,12, 14	Substitution Permutation	Yes	Replacement for DES, Excellent Security
Blowfish	Bruce Schneier	1993	32-448	64 bits	16	Festial	Yes	Excellent Security
RC4	Ron Rivest	1987	Variable	40-2048	256	Festial Stream	Yes	Fast Cipher in SSL
RC2	Ron Rivest	1987	8-128 64 by default	64 bits	16	Festial	-	Stream Cipher
Twofish	Bruce Schneier	1993	128- 256	128 bits	16	Festial	Yes	Good Security
Serpent	Anderson,, Lars Knudsen	1998	128- 256	128 bits	32	Substitutionpermutation	Yes	Good Security
IDEA	James Massey	1991	128 bits	64 bits	8.5	SubstitutionPermutation	No	Not Strong Enough
RC6	Ron Rivest, Matt Robshaw	1998	128 bits to 256 bits	128 bits	20	Festial	Yes	Good Security
RSA	Rivest,, Shamir, Adleman	1977	1,024 to 4,096	128 bits	1	Public Key algorithm	No	Excellent Security, low speed
Diffie Hellman	Whitfield Diffie , Hellman	1976	1024 to 4096 bits	512	-	Asymmetric algorithm	Yes	Many attacks
MD5	Ronald Rivest	1992	Series of MD	512	4	Merkle–Damgård construction		Hash Function

V. CONCLUSION

Internet is mainly used by Individuals, Co-operatives and Governments. They have send information through internet. But there is a possibility to hack the information. So to protect information, we need to encrypt/decrypt information by using cryptography algorithms. In this paper the existing encryption techniques are studied and analysed to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all techniques are unique in its own way, which might be suitable for different applications. By Surveying many papers, I have found that throughput value of BLOWFISH is greater than all symmetric algorithms. Power Consumption value of BLOWFISH is least. The experimental results of many papers showed that BLOWFISH has better performance and efficiency than all other block ciphers . The next technique that is widely used to protect our information is RSA. I have read many papers on Cryptography that mainly used RSA algorithm for information security. RSA is the most secure & widely used by researchers. RSA can be used with many techniques like RSA & DES, RSA & AES, RSA & DIffie Hellman, RSA & IDEA , RSA & Blowfish, RSA & Twofish by combining cryptography algorithms to improve security. I have studied many papers on cryptography. Some papers were very good and effective and can be used for future work . This paper provides beginners to work in this field. If the beginners read this paper, then they have not to read the all papers completely. They just go to read this review paper and may get many ideas for their work. Of course other tools provide a best information security but its importance can't be ignored.

VI. REFERENCES

[1] Chia Long Wu , Chen Hao Hu ,"Computational Complexity Theoretical Analyses on Cryptographic Algorithms for Computer Security Application", Innovations in Bio-Inspired computing and Applications(IBICA), 2012, pp. 307 – 311.

[2] Qing Liu, Yunfei Li, Lin Hao, "On the Design and Implementation of an Efficient RSA Variant", Advanced Computer Theory and Engineering (ICACTE), 2010, pp.533-536.

[3] Mandal, B.K. , Bhattacharyya , Bandyopadhyay S.K. , "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm ", Communication Systems and Network Technologies (CSNT), 2013, pp. 453 – 461.

[4] Wang, Suli , Liu, Ganlai , "File encryption and decryption system based on RSA algorithm", Computational and Information Sciences (ICCIS), 2011, pp. 797 – 800.

[5] Da Silva, J.C.L ,"Factoring Semi primes and Possible Implications for RSA", Electrical and Electronics Engineers in Israel (IEEEI), 2010, pp.182–183.

[6] Geethavani, B. , Prasad, E.V. Roopa, R. "A new approach for secure data transfer in audio signals using DWT" , pp.1-6, Sept 2013.

[7] Nagar, S.A. , Alshamma, S. , "High speed implementation of RSA algorithm with modified keys exchange", Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) , Page(s): 639 – 642 , 2010.
[8] Chong Fu , Zhi-liang Zhu , "An Efficient Implementation of RSA Digital Signature " , Wireless Communications, Networking and Mobile Computing, Oct. 2008 , pp.1-4.
[9] Li Dongjiang ,Wang Yandan , Chen Hong, "The research on key generation in RSA public- key cryptosystem", 2012, pp. 578–580.
[10] Turki Al-Somani ,Khalid Al-Zamil , "Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems".
[11] Hongwei Si , Youlin Cai , Zhimei Cheng , "An Improved RSA Signature Algorithm Based on Complex Numeric Operation Function", Challenges in Environmental Science and Computer Engineering (CESCE), 2010 , pp.397–400.
[12] Wenxue Tan ,Wang Xiping , Jinju Xi , Meisen Pan , "A mechanism of quantitating the security strength of RSA key", Electronic Commerce and Security (ISECS), 2010, Page(s): 357 – 361.
[13] Dhakar, R.S. ; Gupta, A.K. ; Sharma, P., "Modified RSA Encryption Algorithm (MREA)", Advanced Computing & Communication Technologies (ACCT), 2012, pp.426–429.
[14] Abdel-Karim Al Tamimi," Performance Analysis of Data Encryption Algorithms "
[15] Challa Narasimham, Jayaram Pradhan," Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files" , Journal of Theoretical and Applied Information Technology, pp. 55-59, 2008.
[16] Abdel-Karim Al Tamimi, Swati.," Performance Analysis of Data Encryption Algorithms " , International Journal of Advanced Research in Computer Science and Software Engineering 3(2), pp. 147-149 , February – 2013.
[17] Nidhi Singhal1, J.P.S.Raina2, " Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technologypp.177-181, Aug 2011,
[18] Pratap Chandra Mandal, " Evaluation of performance of the Symmetric Key Algorithms: DES, 3DES ,AES and Blowfish ", Journal of Global Research in Computer Science Department of Computer Application, vol 3, pp 67-70, August 2012.
[19] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.
[20] Deepak Kumar Dakate, Pawan Dubey , " Performance Comparison of Symmetric Data Encryption Techniques " , International Journal of Advanced Research in Computer Engineering & Technology , Volume 3, No. 8, August 2012, pp . 163-166.
[21] Shashi Mehrotra Seth, Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Issue 2, pp.192-192 , June 2011.
[22] Gurjeevan Singh , Ashwani Kr. Singla , K.S. Sandha, "Superiority of Blowfish Algorithm in Wireless Networks" , International Journal Computer Applications (0975 – 8887) Volume 44 – No11, pp.23-26 , April 2012.
[23] Agarwal, R. , Dafouti, D., Tyagi, S. "Peformance analysis of data encryption algorithms ", Electronics Computer Technology (ICECT), 2011 3rd International Conference , vol.5 , April 2011, pp. 399 - 403 .
[24] Ramesh, A. , Tirunelvei, "Performance analysis of encryption algorithms for Information Security " Circuits, Power and Computing Technologies (ICCPCT),March 2013 , pp. 840 - 844
[25] http://en.wikipedia.org/, Cryptography.