Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.522 – 531

SURVEY ARTICLE

A Survey for Performance Analysis Various Cryptography Techniques Digital Contents

[1]Pushpendra Verma, [2]Dr. Jayant Shekhar, [3]Preety, [4]Amit Asthana

1. Research Scholar, Department of CSE, Swami Vivekanand Subharti University, Meerut, U.P., INDIA
   Correspondence: mail2_pushpendra@rediff.com
2. Professor, Swami Vivekanand Subharti University, Meerut, Uttar Pradesh, INDIA
   Correspondence: jayant_shekhar@hotmail.com
3. Assistant Professor SIMC, Swami Vivekanand Subharti University, Meerut, U. P, INDIA
   Correspondence: mailpreity81@gmail.com
4. Assistant Professor, CSE, Department, Swami Vivekanand Subharti University, Meerut, U. P, INDIA
   Correspondence: amitasthana80@gmail.com

Abstract

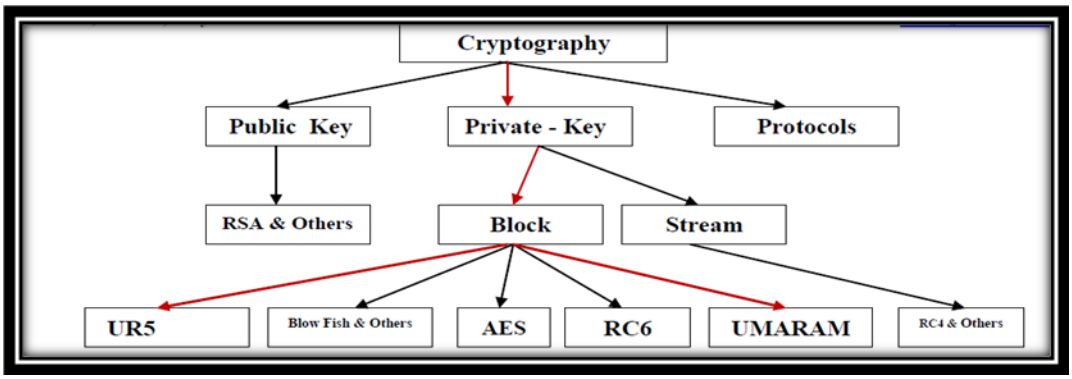
In the recent years, with the development of network and multimedia technology, multimedia data, especially image, audio and video data, is used more and more widely in human society. Some multimedia data, including entertainment, politics, economics, militaries, industries, education etc, are necessary to be protected by providing confidentiality, integrity, and ownership or identity. In this regard, to protect multimedia contents, cryptology, which appears to be an effective way for information security, has been employed in many practical applications. However, number theory or algebraic concepts based traditional ciphers, such as Data Encryption Standard (DES) (Tuchman, 1997), Advanced Encryption Standard (AES) (Zeghid et al., 1996), International Data Encryption Algorithm (IDEA) (Dang & Chau, 2000), and the algorithm developed by Rivest, Shamir and Adleman (RSA) (Cormen et al., 2001), most of which are used for text or binary data, appear not to be ideal for multimedia applications.

Keywords: Image encryption, Shuffling, Simplified AES, Chaos, Baker's map, S-box

1. Introduction

Encryption is a process of converting in formation in "hidden" form. So that it is intelligible only to some one who knows how to decrypt it. For encryption and decryption there are two aspects: algorithm and key used. Key is similar to one time pad used in vernal cipher. If same key is used for encryption and decryption then this is called secret key cryptography. And if different keys are used for encryption and decryption we call this public key cryptography. In secret key cryptography single key is used. So as before distributing the data between entities the key must be transferred. Secret key cryptography includes DES, AES, 3DES, IDEA, Blowfish algorithms etc. and public key cryptography includes RSA, Digital Signature and Message Digest algorithms.[3,4]

For each algorithm there are two key aspects used: Algorithm type (define size of plain text should be encrypted per step) and algorithm mode (define cryptographic algorithm mode).Algorithm mode is combination of series of the basic algorithm and some block cipher and some feedback from previous steps.



A. Basic Terms Used in Cryptography

❖ *Plain Text*

The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.

❖ *Cipher Text*

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".

❖ *Encryption*

A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.

❖ *Decryption*

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

❖ *Key*

A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of

encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

B. Purpose of Cryptography

Cryptography provides a number of security goals to ensure the privacy of data, non alteration of data and so
on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

- *Confidentiality*

Information in computer is transmitted and has to be accessed only by the authorized party 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 a authorized person or a false identity.

- *Integrity*

Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.

- *Non Repudiation*

Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.

- *Access Control*

Only the authorized parties are able to access the given information.

C. Classification of Cryptography

Encryption algorithms can be classified into two broad categories- Symmetric and Asymmetric key encryption.

- Symmetric Encryption

In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6,BLOWFISH[2].

2. Requirements of multimedia encryption

Due to special characteristics of multimedia data, such as large data volumes, high redundancy, interactive operations, and requires real-time responses, sometimes multimedia applications have their own requirements like security, invariance of compression ratio, format compliance, transmission error tolerance, demand of real-time. In this section, some special requirements of multimedia encryption are summarized.

2.1 Security

For multimedia encryption, security is the primary requirement, thus the usage of chaotic maps should guarantee the security of a multimedia datum. Generally speaking, an encryption algorithm is regarded as secure if the cost for cracking it is no smaller than the one paid for the authorization of video content. For example, in broadcasting, the news may be of no value after an hour. Thus, if the attacker can not break the encryption algorithm during an hour, then the encryption algorithm may be regarded as secure in this application (Lian et al., 2008). Security of an encryption usually consists of its perceptual security, its key space, key sensitivity, and its ability against potential attacks. (1) Perceptual security: when we use a method to encrypt a multimedia datum, for example an image, if the encrypted image is not perceptual recognized, the encryption is secure in perception. (2) Key space: it is generally defined as the number of encryption keys that are available in the cryptosystem. Assume *ki* denotes a key and *K* represents a finite set of possible keys, the key space can be expressed as $K = \{k1, k2, ..., kr\}$, where *r* is the number of key. For chaos-based encryptions, the chaotic sequence generator should produce chaotic ciphers with good randomness, which can be tested by long period, large linear complexity, randomness and proper order of correlation immunity (Rueppel, 1986).

(3) Key sensitivity: an ideal multimedia encryption should be sensitive with respect to the secret key i.e. the change of a single bit in the secret key should produce a completely different encrypted result, which is called key sensitivity. Generally, key sensitivity of a chaotic cipher refers to the initial states sensitivity and control parameters sensitivity of chaotic map.

(4) Potential attacks: here, we just introduce the common used attacks as following:

• Ciphertext-only attack: it is an attack with an attempt to decrypt ciphertext when only the ciphertext itself is available. The opponent attempts to recover the corresponding plaintext or the encryption key.

• Known-plaintext attack: when having access to the ciphertext and an associated piece of plaintext, the opponent attempts to recover the key.

• Chosen-plaintext attack: it is an attack where the cryptanalyst is able to choose his own plaintext, feed it into the cipher, and analyze the corresponding ciphertext.

• Brute-force attack: it is a form of attack in which each possible key is tried until the success key is obtained. To make brute-force attack infeasible, the size of key space should be large enough.

• Differential attack: it is a chosen-plaintext attack relying on the analysis of the evolution of the differences between two plaintexts.

Therefore, a secure encryption algorithm should be secure in perception, have large key space, high key sensitivity, and resist potential attacks.

Review of Related Works

In this section describes and examines previous work on most common algorithm implementation for both software and hardware approaches. The metrics taken into consideration are processing speed, throughput, power consumption, packet size and data types.

1. Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul. Elminaam et.al., (2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results. First; in the case of changing packet size with and without transmission of data using different architectures and different WLANs protocols, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Second; in case of changing data type such as audio and video files, it is found the result as the same as in text and document. In the case of image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption. He is found that 3DES still has low performance compared to algorithm DES. Third point;[5]when the trans mission of data is considered there was insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). There is insignificant difference between open key authentications and shared key authentication in ad hoc Wireless LAN connection with excellent signals. In case of poor signal it is found that, transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod. Finally -in the case of changing key size – it can be seen that higher key size leads to clear change in the battery and time consumption.
2. Comparison Of Data Encryption Algorithms has done by Simar Preet Singh, and Raman Maini -The simulation results showed that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results compared to other algorithms, since it requires more processing power. The first set of experiments were conducted using ECB Mode. The results show the superiority of Blowfish algorithm over other algorithms in terms of processing time. It shows also that AES consumes more resources when data block size is relatively big. Another point can be noticed here that 3DES requires always more time than DES because of its triple phase encryption characteristic. Blowfish, which has a long key (448 bit), outperformed other encryption algorithms. DES and 3DES are known to have worm holes in their security mechanism, Blowfish and AES do not have any so far[6]. As expected, CBC requires more processing time than ECB because of its key-chaining nature. The results indicates also that the extra time added is not significant for many applications, knowing that CBC is much better than ECB in terms of protection.
3. Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files designed by challa Narasimham and Jayaram Pradhan(2008)- They performed the performance comparison for variable sized text files as input. An analysis on computational running times results in significant difference among the methods. He believe in that the performance of DES, especially in decryption method is very high than the alternatives. Despite the key distribution, DES is more suitable to the application, which has the decryption as the highest priority.He has proposed and performed the test cases on the two PKCS methods i.e., RSA and NTRU Though the encryption, decryption and complexity are high in NTRU, the RSA provides the highest security to the business application. He presented all these parameters with computational running times for all the methods, so as to select the appropriate method[7].
4. Abdel-Karim and his colleague Al Tamimi presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm? AES showed poor performance results compared to other algorithms since it requires more processing power. Using CBC mode has added extra

processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks.

The results showed that Blowfish has a very good performance compared to other algorithms. Also it showed that AES has a better performance than 3DES and DES. Amazingly it shows also that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data[8].

5. P. Prasithsangaree and his collegeue P. Krishnamurthy have analyzed the Energy Consumption of RC4 and AES Algorithms in Wireless LANs in the year 2003.They have evaluated the performance of RC4 and AES encryption algorithms. The performance metrics were encryption throughput, CPU work load, energy cost and key size variation. Experiments show that the RC4 is fast and energy efficient for encrypting large packets. However, AES was more efficient than RC4 for a smaller packet size. From the results, it appears that we can save energy by using a combination of RC4 and AES to provide encryption for any packet size. The tradeoffs with security are not completely clear[9].

6. Comparative Analysis of AES and RC4 Algorithms for Better Utilization has designed by Nidhi Singhal, J.P.S.Raina in the year (2011).The performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments show that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of the research, RC4 is better than AES.we compare the encryption time of AES and RC4 algorithm over different packet size. RC4 takes less time to encrypt files w.r.t. AES. In AES, CFB and CBC takes nearly similar time but ECB takes less time then both of these[10]. Another performance comparison point is the changing key size. The three different key sizes used are 128 bit, 192 bit and 256 bits. As the key size vary from 128 bits to 192 bits to 256 bits, encryption time for RC4 is almost constant and is less then AES. Hence it consumes less power w.r.t AES. But for different modes of AES, encryption time increases as key size increases.

The result shows the superiority of RC4 over AES. With different key sizes RC4 gives almost the same result. But for different modes of AES, throughput decreases as key size increases because of more usage of computational power and encryption characteristics. Thus RC4 is fast in nature and consume less power w.r.t its counterparts. Better results were obtaining in decryption w.r.t. encryption

Efficiency and Security of Some Image Encryption Algorithms Marwa Abd El-Wahed et.al (2008) – worked in this paper, four image encryption algorithms have been studied by means of measuring the encryption quality, the memory requirement, and the execution time of the encryption. In addition, the security analysis of these schemes is investigated from cryptographic viewpoint; statistical and differential attacks. The results are compared, focusing on those portions where each scheme is performed differently. Based on the experimental results, it can be concluded that:

1) Permutation techniques achieve efficient schemes (minimum encryption time and memory requirement) compared with substitution techniques.

2) Permutation techniques are attractive due to their efficiency. But the drawbacks of these techniques are evident in terms of generated key and security.

3) Techniques that based on SCAN methodology achieve the highest security.

4) The chaos-based encryption scheme still need further study to achieve a reasonable degree of security and acceptable efficiency.

5) A security defect exists in the schemes that generated key based on random number sequence compared with these techniques that based on scan methodology. If a solution requires random numbers it is important to evaluate the efficiency and implicating the security will be considered.
6) When permutation technique combined with substitution technique in intertwined manner and iteratively, it leads to design complex, but secure and efficient techniques when variable key size and key number is used (according to plain-image size).
7) The schemes implementation using the computational approach for selecting random permutations performs slower time.
8) If the key used to encrypt plaint-image is random and the length of the key exceeds the amount of plaint image to be encrypted, then the cipher-image is unbreakable.
From these results, it appears that there are three main criteria should be considered at the same level of importance to evaluate new cryptosystems: how much it eases implementation, level of security, and efficiency. To identify an optimal security level, it is necessary to compare carefully the cost of the multimedia information to be protected and the cost of the protection itself[11].

7. A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms *designed by* S.A.M Rizvi1 et.al., All algorithms run faster on Windows XP. The CAST runs slower than AES for text. Blowfish encrypts images most efficiently on all 3 platforms, even CAST runs faster on Windows XP for image data. But on Windows Vista and Windows7, AES and CAST perform at the similar speed .CAST performs better than BLOWFISH and AES on Windows XP for encrypting audio files, but on Windows Vista and Windows7, there is no significant difference in performance of CAST and AES, however BLOWFISH encrypts audio files at less speed for audio files[12].

8. Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems Turki Al-Somani et.al.,. They presented an implementation of three symmetric block encryption algorithms using Java and JCA. The main objective was to evaluate the performance of these algorithms in terms of CPU execution time. The measurements were performed on two platforms; SunOS and Linux. 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 has over the DES algorithm.

9. ThroughPut Analysis of Various Encryption Algorithms presented by Gurjeevan Singh et al.,(2011)- For experiment a Laptop with 2.20 GHz C.P.U., 4GB RAM Core-2-Dou Processor and Windows 7 Home Premium (32-Bit) is used in which the performance data are collected. In this experiment software encrypts the text file size that ranges from 20 Kb to 99000 Kb. Their implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm. The performance matrices are throughput. The throughput of encryption as well as decryption schemes is calculated but one by one. In the case of Encryption scheme throughput is calculated as the average of total plain text in k bytes divided by the average Encryption time and in the case of Decryption scheme throughput is calculated as the average of total cipher text is divided by the average Decryption time. This work presents the performance evaluation of selected symmetric algorithms. The selected algorithms are AES, 3DES, Blowfish and DES. The presented simulation results show the numerous points. Firstly it was concluded that Blowfish has better performance than other algorithms followed by AES in terms of throughput. Secondly 3DES has least efficient of all the studied algorithms[15].

10. R. Chandramouli et.al., investigated battery power-aware Encryption algorithms. The main conclusions they reached was that the power consumption changes linearly with the number of rounds of several popular cryptographic algorithms. Their experimental test bed had a laptop connected to a power supply. The power supply was connected to a computer running the Lab VIEW software to graph changes in voltage and current from the power supply. These changes were graphed during the life of the encryption algorithms[16].

DATA ENCRYPTION ALGORITHMS

Data Encryption Standard (DES): An encryption algorithm that encrypts data with a 56-bit, randomly generated symmetric key. DES is not a secure encryption algorithm and it was cracked many times. Data Encryption Standard (DES) was developed by IBM and the U.S. Government together. DES is a block encryption algorithm.

Data Encryption Standard XORed (DESX): DESX is a stronger variation of the DES encryption algorithm. In DESX, the input plaintext is bitwise XORed with 64 bits of additional key material before encryption with DES and the output is also bitwise XORed with another 64 bits of key material.

Triple DES (3DES): Triple DES was developed from DES, uses a 64-bit key consisting of 56 effective key bits and 8 parity bits. In 3DES, DES encryption is applied three times to the plaintext. The plaintext is encrypted with key A, decrypted with key B, and encrypted again with key C. 3DES is a block encryption algorithm.

RC2 and RC5: Ronald Rivest (RSA Labs), developed these algorithms. They are block encryption algorithms with variable block and key sizes. It is difficult to break if the attacker does not know the original sizes when attempting to decrypt captured data.

RC4: A variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation and is commonly used for the encryption of traffic to and from secure Web sites using the SSL protocol.

Advanced Encryption Standard (AES): Advanced Encryption Standard (AES) is a newer and stronger encryption standard, which uses the Rijndael (pronounced Rhine-doll) algorithm. This algorithm was developed by Joan Daemen and Vincent Rijmen of Belgium. AES will eventually displace DESX and 3DES. AES is capable to use 128-bit, 192-bit, and 256-bit keys.

International Data Encryption Algorithm (IDEA): IDEA encryption algorithm is the European counterpart to the DES encryption algorithm. IDEA is a block cipher, designed by Dr. X. Lai and Professor J. Massey. It operates on a 64-bit plaintext block and uses a 128-bit key. IDEA uses a total of eight rounds in which it XOR's, adds and multiplies four sub-blocks with each other, as well as six 16-bit sub-blocks of key material.

Blowfish: Blowfish is a symmetric block cipher, designed by Bruce Schneier. Blowfish has a 64-bit block size and a variable key length from 32 up to 448 bits. Bruce Schneier later created Twofish, which performs a similar function on 128-bit blocks.

CAST: CAST is an algorithm developed by Carlisle Adams and Stafford Tavares. It's used in some products offered by Microsoft and IBM. CAST uses a 40-bit to 128-bit key, and it's very fast and efficient.

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
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	Substitution permutation	Yes	Good Security
IDEA	James Massey	1991	128 bits	64 bits	8.5	Substitution Permutation	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

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 analyzed to promote the performance of the encryption methods also to ensure the security proceedings.

In this paper, it has been surveyed that the existing works on the encryption techniques. Those encryption techniques are studied and analyzed well to promote the performance of the encryption methods also to ensure the security proceedings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security.

References

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
[2] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.
[3] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[4] Ramesh G, Umarani. R, " Data Security In Local Area Network Based On Fast Encryption Algorithm",International Journal of Computing Communication and Information System(JCCIS) Journal Page 85-90. 2010.
[5] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept.
[6] Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127
[7] Challa Narasimham, Jayaram Pradhan," EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILES" Journal of Theoretical and Applied Information Technology,pp55-59 2008.
[8] Abdel-Karim Al Tamimi," Performance Analysis of Data Encryption Algorithms "
[9] Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the
IEEE GLOBECOM 2003, pp. 1445-1449.
[10] Nidhi Singhal1, J.P.S.Raina2, Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011 pp177-181.
[11] Marwa Abd El-Wahed, Saleh Mesbah, and Amin Shoukry," Efficiency and Security of Some Image Encryption Algorithms", Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.
[12] Dr. S.A.M Rizvi1 ,Dr. Syed Zeeshan Hussain2 and Neeta Wadhwa" A Comparative Study Of Two Symmetric Encryption Algorithms Across Different Platforms",
[13] Turki Al-Somani ,Khalid Al-Zamil "Performance Evaluation of Three Encryption/Decryption Algorithms on the SunOS and Linux Operating Systems", Theses
[14] 1Gurjeevan Singh, 2Ashwani Kumar Singla, 3K.S. Sandha," Through Put Analysis of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011
[15] Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, "Through Put Analysis Of Various Encryption Algorithms", IJCST Vol. 2, Issue 3, September 2011.
[16] R.Chandramouli, "Battery power-aware encryption – ACM Transactions on Information and System Security (TISSEC),'' Vol. 9 Issue 2, May 2006.
[17] 1Shashi Mehrotra Seth, 2Rajan Mishra," Comparative Analysis Of Encryption Algorithms For Data Communication", IJCST Vol. 2, Iss ue 2, June 2011 pp.192-192.
[18] Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2," Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vol.10, No.3, PP.213{219, May 2010.
[19] Diaa Salama1, Hatem Abdual Kader2, and Mohiy Hadhoud2" Wireless Network Security Still Has no Clothes", International Arab Journal of e-Technology, Vol. 2, No. 2, June 2011 pp.112-123.
[20].N.Ruangchaijatupon and P. Krishnamurthy, "Encryption and power consumption in wireless LANs-N,"The Third IEEE Workshop on Wireless LANs, pp. 148-152,Newton, Massachusetts, Sep. 27-28,2001.
[21] Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.

