http://student-friendly.blogspot.com/2013/07/advanced-algorithms-mtech-2nd-sem-cs.html

Satya narayana

Volume 2, Issue 7, July 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Various Most Common Encryption Techniques

E. Thambiraja
Dept. of Maths,
Dr. Pauls Engineering College,
Vanur, Tamilnadu
India

G. Ramesh
Research Scholar,
Research and Development Centre,
Bharathiyar University,Coimbatore,
India

Dr. R. Umarani
Associate Professor
Dept. in Computer Science,
Sri Sarada college for women,
Salem -16

Abstract- **This talk will present a perspective on the current state of play in the field of encryption algorithms, in particular on private key block ciphers which are widely used for bulk data and link encryption. we have initially survey some of the more popular and interesting algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available encryption techniques. Also focuses on image encryption techniques, information encryption techniques. This study extends to the performance parameters used in encryption processes and analyzing on their security issues.**

Keywords: **UR5, UMARAM, Survey, Encryption Algorithm, DES, AES**

I. INTRODUCTION

The high growth in the networking technology leads a common culture for interchanging of the data very drastically. Hence it is more vulnerable of duplicating of data and re-distributed by hackers. Therefore the information has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of wireless communication, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the wireless. Different encryption techniques are used to protect the confidential data from unauthorized use. Encryption is a very common technique for promoting the information security. The evolution of encryption is moving towards a future of endless possibilities. Everyday new methods of encryption techniques are discovered. This paper holds some of those recent existing encryption techniques and their security issues. The performance of all those encryption techniques are studied and discussed including UMARAM and UR5 in later chapters of the paper.

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.

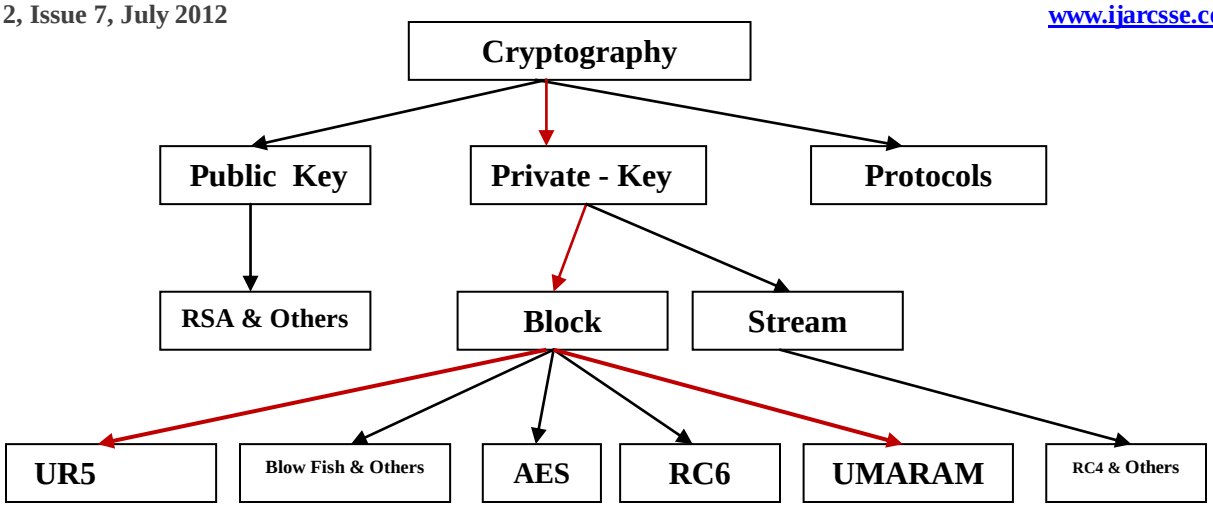

Fig.1.1 Overview of Most Common encryption algorithm

- 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].

II PREVIOUS RELATED WORKS

This subsection 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.

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 with out 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.

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.

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].

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].

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].

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].
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].

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.

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].

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].

Shashi Mehrotra Seth and her collegue Rajan Mishra(2011) jointly has done a Comparative Analysis Of Encryption Algorithms For Data Communication.The authors analyse the performance of encryption algorithm is evaluated considering the following parameters like Computation Time, Memory usage and Output Bytes. The experimental results shows the comparison of three algorithm AES, DES and RSA using same text file for five experiment, output byte for AES and DES is same for different sizes of files. The authors noticed the RSA has very smaller output byte compare to AES and DES algorithm. Time taken by RSA algorithm is much higher compare to the time taken by AES and DES algorithm. Finally the authors concludes, Based on the text files used and the experimental result it was concluded that DES algorithm consumes least encryption time and AES algorithm has least memory usage while encryption time difference is very minor in case of AES algorithm and DES algorithm. RSA consume longest encryption time and memory usage is also very high but output byte is least in case of RSA algorithm[17].

Diaa Salama Abd Elminaam etal.,(2010) [18]eavaluate the Performance of Symmetric Encryption Algorithms like AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. For the experiment, the authors use a laptop IV 2.4 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 321 K byte to 7.139Mega Byte139MegaBytes for text data, from 33 Kbytes to 8262 Kbytes for audio data, and from 4006 Kbytes to 5073 Kbytes for video files. By the authors, several points can be concluded from the Experimental results. The RC6 requires less time than all algorithms except Blowfish. The AES has an advantage over other 3DES, DES and RC2 in terms of time consumption and throughput. 3DES has low performance in terms of power consumption and throughput when compared with DES. It always requires more time than DES because of its triple phase encryption characteristics. Finally, it is found that RC2 has low performance and low throughput when compared with other five algorithms in spite of the small key size used.

Diaa Salama et.al jointly done a research work in the title “Wireless Network Security Still Has no Clothes ”[19]. The above research work evaluate the performanace of most common symmetrical encryption algorithms like AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6. The authors illustrates the key concepts of security, wireless networks, and security over wireless networks. Wireless security is demonstrated by applying the common security standards like (802.11 WEP and 802.11i WPA,WPA2) and provides evaluation of six of the most common encryption algorithms on power consumption for wireless devices namely: AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6.

A comparison is conducted between the results of selected different encryption algorithms using different setting such as different and data types, different packet size, different key size · In case of changing packet size, (throughput, power consumption in µJoule/Byte and power consumption by calculating difference in battery percentage were calculated) in case of encryption processes to calculate the performance of each encryption algorithms. · In case of changing data types such as audio, ,(throughput ,power consumption in µJoule/Byte and power consumption by calculating difference in battery percentage were calculated)in case of encryption processes to calculate the performance of each encryption algorithms.

Ruangchaijatupon.P and his collogue Krishnamurthy.P(2001)[20] has done a research work on "Encryption and Power Consumption in Wireless LANs”. This research was shown in that energy consumption of different common symmetric key encryptions on handheld devices. It is found that after only 600 encryptions of a 5 MB file using Triple-DES the remaining battery power is 45% and subsequent encryptions are not possible as the battery dies rapidly. It was concluded in that AES is faster and more efficient than other encryption algorithms. When the transmission of data is considered there is insignificant difference in performance of different symmetric key schemes. Increasing the key size by 64 bits of AES leads to increase in energy consumption about 8% without any data transfer. The difference is not noticeable.

Prasithsangaree.P and Krishnamurthy.P(2003),“ [21] has done the analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs. A study is conducted for different secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows 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.

Idrus.S.Z, Aljunid.S.A, Asi.S.M(2008), done the research [22]work in the different browsers for evaluate the Performance Analysis of Encryption Algorithms Text Length Size. The authors study of security measure level has been proposed for a web programming language to analyze four Web browsers. This study consider of measuring the performances of encryption process at the programming language’s script with the Web browsers.

Gast.M.S (2002),"802.11 Wireless Network: The Definitive Guide,[23]" A study is conducted for different popular secret key algorithms such as RC4, AES, and XOR. They were implemented, and their performance was compared by encrypting for real time video streaming of varying contents. The results showed; encryption delay overhead using AES is less than the overhead using RC4 and XOR algorithm. Therefore, AES is a feasible solution to secure real time video transmissions.

Monika Agrawal et al. 2012 gives a detailed study[24] of the popular symmetric key encryption algorithms such as DES, TRIPLE DES, AES, and Blowfish. Symmetric Key algorithms run faster than Asymmetric Key algorithms such as RSA etc and the memory requirement of Symmetric algorithms is lesser than Asymmetric encryption algorithms. Further, the security aspect of Symmetric key encryption is superior than Asymmetric key encryption.

Ezedin Barka and his collegue Mohammed Boulmalf conducting two experiments[25] scenarios that were conducted for the purpose of establishing a baseline and for understanding the impact of adding encryptions, with different key sizes, used by WEP and WPA security protocols on UDP and TCP WLAN traffic. While the first experiment was for measuring the throughput under normal conditions (No encryption applied), the second experiment was to analyze the variation of traffic throughputs over an Infrastructure network when encryption is applied. the general observations taken from these experiments are: Throughput decreases when security, WEP and WPA are enabled. This is due to the fact that encryption operations performed by these protocols increase the amount of data transmitted and slow down the rate of data being sent or received.

For WEP, when the key size increases the throughput slightly decreases, which is due to the fact that WEP adds the Initial Value of its symmetric encryption key to the data sent and it uses the rest of the key bits to initiate a key scheduling algorithm that generates a stream key for the streamed data to be XORed with. This normal process of the RC4 encryption algorithm can impose some delay to the data to be sent after encryption then received and decrypted.

In the wireless to wireless environment, the throughput suffered more degradation than that in the wireless to wired environment. This is due to the fact that in the wireless to wireless environment, there are double encryptions which result from having two air interfaces with one access point. In the ad hoc communication, the throughput is already low due to the fact that, in addition to the degradation caused by the encryption, there are no access points involved in the communication process. Finally, general observation from all experiments conducted here indicate that there is some degradation in throughput resulted from applying encryption, however, this degradation is moderate, in comparison to the benefits provided by applying encryption, thus, we recommend that WEP or WPA encryptions be enabled in WLANs communications[26].

D. S. Abdul. Elminaam etal., (2009) analysed the Performance Evaluation of Symmetric Encryption Algorithms. The authors use a laptop IV 2.4 GHz CPU, in which performance data is collected. In the experiments, the laptop encrypts a different file size ranges from 321 K byte to 7.139Mega Byte. Several performance metrics are collected: encryption time, CPU process time, and CPU clock cycles and battery power.

The following tasks that will be performed are shown as follows:
- A comparison is conducted between the results of the selected different encryption and decryption schemes in terms of the encryption time at two different encoding bases namely; hexadecimal base encoding and in base 64 encoding.
- A study is performed on the effect of changing packet size at power consumption during throughput for each selected cryptography algorithm.
-A study is performed on the effect of changing data types - such as text or document and images- for each cryptography selected algorithm on power consumption.
- A study is performed on the effect of changing key size for cryptography selected algorithm on power consumption.

The selected algorithms are AES, DES, 3DES, RC6, Blowfish and RC2. Several points can be concluded from the simulation results. First; there is no significant difference when the results are displayed either in hexadecimal base encoding or in base 64 encoding.

G. Ramesh et.al designed al algorithm in the year 2010 named as UMARAM[27]. The UMARAM is a Symmetrical encryption algorithm. The key generation generates 16-keys during 16-rounds.One key of them is used in one round of the encryption or decryption process. The new algorithm uses a key size of 512-bits to encrypt a plaintext of 512-bits during the 16-rounds. In this Algorithm, a series of transformations have been used depending on S-BOX, different shift processes, XOR-Gate, and AND-Gate. The S-Box is used to map the input code to another code at the output. It is a matrix of16×16×16 .The S-Box consists of 16-slides, and each slide having 2-D of16×16 . The numbers from 0 to 255 are arranged in random positions in each slide.

G. Ramesh et.al designed al algorithm in the year 2010 named as UR5[28]: A block encryption algorithm is proposed in this approach. In this Algorithm, a series of transformations have been used depending on S-BOX, XOR Gate, and AND Gate. The proposed algorithm encrypts a plaintext of size 64-bits by a key size of 64-bits. It uses eight rounds for encryption or decryption process. It overcomes some drawbacks of the other algorithms.

III. CONCLUSION

In this wireless world nowadays, the security for the data has become highly important since the communication by transmitting of digital products over the open network occur very frequently. 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.

[22] Idrus.S.Z, Aljunid.S.A, Asi.S.M(2008), 'Performance Analysis of Encryption Algorithms Text Length Size on Web Browsers," IJCSNS International Journal of Computer Science and Network Security,
VOL.8 No.1, PP 20-25.

[23] Gast.M.S (2002),"802.11 Wireless Network: The Definitive Guide," O'REILLY.

[24] Monika Agrawal, Pradeep Mishra," A Comparative Survey on Symmetric Key Encryption Techniques", International Journal on Computer Science and Engineering (IJCSE), Vol. 4 No. 05 May 2012, PP877-882.

[25] Ezedin Barka, Mohammed Boulmalf," On The Impact of Security on the Performance of WLANs", JOURNAL OF COMMUNICATIONS, VOL. 2, NO. 4, JUNE 2007,pp.10-17.

[26] D. S. Abdul. Elminaam et.al," Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009 ISSN: 1943-7765,pp.58-64.

[27] Ramesh, G. Umarani, R. ,UMARAM: A novel fast encryption algorithm for data security in local area network http://ieeexplore.ieee.org /xpl/ freeabs_all.jsp? arnumber=5670740

[28] G. Ramesh, R. Umarani," UR5: A Novel Symmetrical Encryption Algorithm with Fast Flexible and High Security Based on Key Updation", European Journal of Scientific Research ISSN 1450-216X Vol.77 No.2 (2012), pp.275-292.

[29] Ramesh G, Umarani. R, " UR5:A Novel Symmetrical Encryption Algorithm With Fast Flexible and High Security Based On Key Updation", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4, April 2012 Page 16-22. 2010.

