A Comparative Study of Six Most Common Symmetric Encryption Algorithms across Different Platforms

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

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

ABSTRACT

The hacking is the greatest problem in the wireless local area network (WLAN). Many algorithms like RC6,UMARAM,DES,3DES,RC2 and UR5 have been used to prevent the outside attacks to eavesdrop or prevent the data to be transferred to the end-user correctly. In this paper, we study the six most common and popular symmetric cryptographic algorithms like RC6,UMARAM,DES,3DES,RC2 and UR5. We analyze their security issues and then compare their efficiency for encrypting text and image across different widely used Operating Systems like Windows XP, Windows Vista and Windows 7. The simulation results concluded the performance of most common encryption across the different platforms . Which algorithm performs better on which operating system for encrypting what kind of data.

Keywords

DES,3DES,DES,UMARAM,UR5,Symmetric Encryption.

1. INTRODUCTION

The cryptography algorithms are divided into two groups: symmetric-encryption algorithms and asymmetric-encryption algorithms. There are a lot of symmetric-encryption algorithms used in WLAN[19], such as DES[3], 3DES,RC6[8],UMARAM[12],RC2 and UR5[6]. In all these algorithms, both sender and receiver have used the same key for encryption and decryption processes respectively. The outside attackers use the fixed plaintext and encrypted text to obtain the key used in the WLAN. Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power [5]. This paper examines a method for evaluating performance of most common symmetric encryption of various algorithms on Encryption speed for wireless devices. In this paper we do the comparative analysis of *RC6,UMARAM,DES,3DES,RC2 and UR5* on different latest platforms like Windows XP, Windows Vista and Windows7. This analysis shows which algorithm is best suited in which environment.

2. OVERVIEW OF ALGORITHMS

Brief definitions of the most common encryption techniques are given as follows:

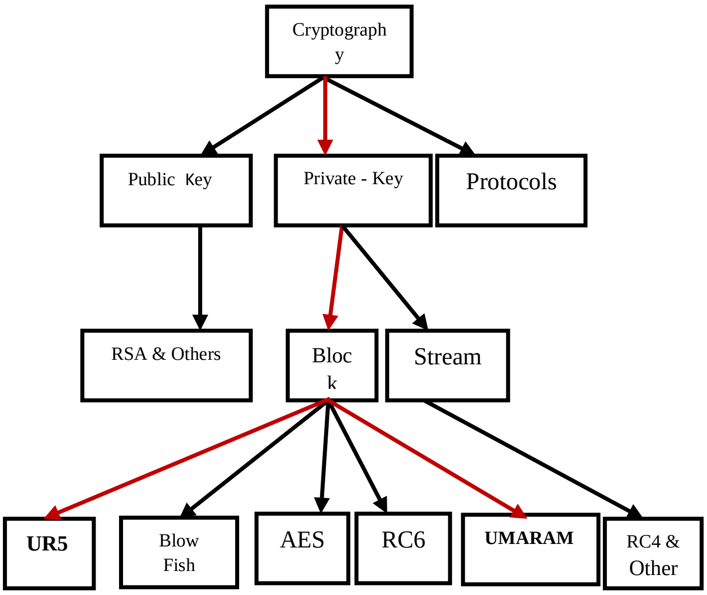

Figure 1: Overview of the field of Cryptography

2.1 DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).DES is (64 bits key size with 64 bits block size) .Since that time, many attacks and methods recorded the weaknesses of DES, which made it an insecure block cipher [3].

2.2 Triple DES: 3DES is an enhancement of DES; it is 64 bit block size with 192 bits key size. In this standard the encryption method is similar to the one in the original DES but applied 3 times to increase the encryption level and the average safe time. It is a known fact that 3DES is slower than other block cipher methods[1]

2.3 RC2: RC2 is a block cipher with a 64-bits block cipher with a variable key size that range from 8 to128 bits. RC2 is vulnerable to a related-key attack using 234 chosen plaintexts [2].

2.4 RC6: RC6 is block cipher derived from RC5. It was designed to meet the requirements of the Advanced Encryption Standard competition. RC6 proper has a block size of 128 bits and supports key sizes of 128, 192 and 256 bits. Some references consider RC6 as Advanced Encryption Standard [8].

2.5 UMARAM: The UMARAM Algorithm[12] is a new symmetrical encryption algorithm was designed by G.Ramesh and R. Umarani in the year 2010. 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.

2.6 UR5: The UR5 Algorithm[6] is a new symmetrical encryption algorithm was designed by Ramesh and Umarani in the year 2011. .A block encryption algorithm is UR5 in this approach. In this Algorithm, a series of transformations have been used depending on S-BOX, XOR Gate, and AND Gate. The UR5 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.

This paper is organized as follows. Section 2 gives overview of Symmetrical Algorithm; Section 3 gives related works. Section 4 gives experimental design of symmetrical encryption algorithm across different platforms. Section 5 gives experimental results of UR5.Conclusions are presented in section 5.

3. RELATED WORK

In research of CAST ciphers with random S-boxes are proposed. It is shown that when randomly generated S-boxes are used, the resulting cipher is resistant to both differential and linear attack . A Crypto++ Library [14] analyze some common encryption algorithms. It showed that Blowfish and AES have the best performance compared with other encryption algorithms.

Nadeem and Kader, did performance evaluation of few symmetric encryption algorithms like AES, DES, and 3DES, RC6, Blowfish and RC2. They concluded from the simulation results that Blowfish has better performance as compared to other encryption algorithms for different file size, followed by RC6. AES has better performance than RC2, DES, and 3DES. 3DES still has low performance compared to algorithm DES. RC2 is the slowest. However they conducted the experiments on only one platform: Windows OS.
Krishnamurthy in [16] demonstrated the energy consumption of different common symmetric key encryptions on hand-held devices.
Salama and Elminaam have done a comparison between encryption algorithms (AES, DES, and 3DES, RC2,Blowfish, and RC6) at different settings like different sizes of data blocks, different data types, CPU time, and different key size. The algorithms were tested on two different hardware platforms. The results indicated that the Blowfish had more efficient compared to other algorithms. And AES had a better performance than 3DES and DES[5].
The study in[15] tested the encryption algorithms such as RC4, AES and XOR to find out the overall performance of real time video streaming. The results showed that AES has less time overhead than the overhead using RC4 and XOR algorithm. So, AES is more efficient to secure real time video transmissions.

Most of the above parallel research focus on performance analysis of different symmetric encryption algorithms on different settings for various kinds of input data with different modes. In this paper , we are analyzing ,UMARAM,DES,3DES,RC2 and UR5 on three different Operating Systems for encrypting three kinds of data :text ,image and sound.

4. EXPERIMENTAL DESIGN

We implemented the algorithms according to their standard specifications in Microsoft Visual Basic 6.0 and a tool has designed, which calculates the encryption time in ms(milliseconds) of each algorithm .The no. of different types of files like text file and image files have been encrypted with the designed tool and their execution time is calculated.

For our experiment, we use three laptops of 32bit configuration: 1. Intel Pentium® Dual Core with Windows XP. 2. Intel Pentium® Dual Core with Windows Vista. 3. Intel Pentium® Dual Core with Windows 7.

The tool’s front end look like as:

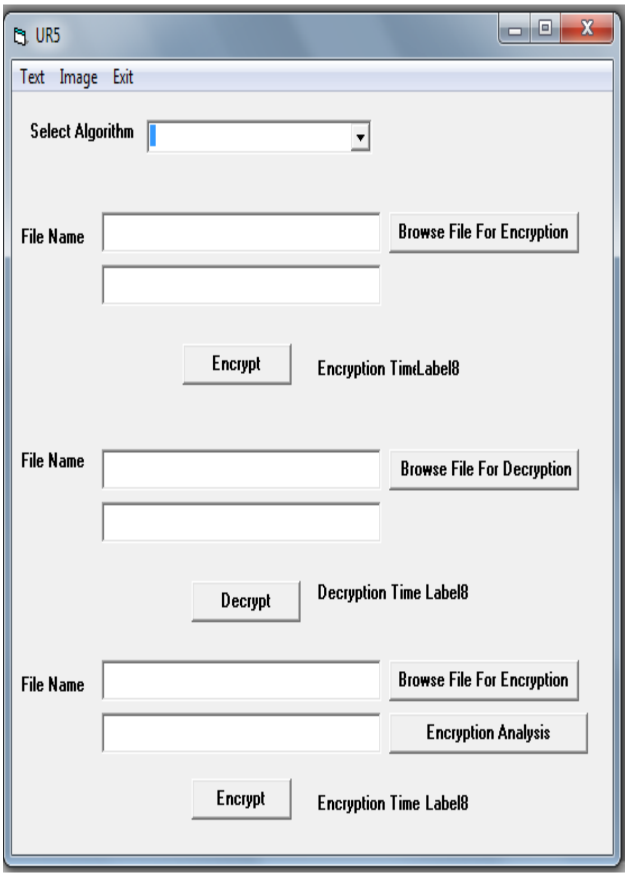

Figure.2. Experimental design of Most common encryption algorithm

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 three different windows platforms like Windows XP, Vista and Windows 7.

-A study is performed on the effect of changing data types such as text or document, and image file for each cryptography selected algorithm.

5. EXPERIMENTAL RESULTS

The front end tools are installed in all three laptops. We encrypt 40 text files of size ranges between 500KB to 50MB and 40 images ranges between 20 KB to 200KB. First we tabulated their encryption time in ms(milli seconds) and then calculated their mean execution speed in MB/sec (MegaBytes per second) .

Table 1: Encryption Speed (in MB/sec) of Most Common Algorithms on different OS for text data

OS Encryption	Windows XP	Windows Vista	Windows 7
RC6	11.6	11.44	10.74
UMARAM	13.76	13.11	13.10
DES	14.38	15.02	15.11
3DES	15.12	14.65	15.11
RC2	18.84	16.40	14.56
UR5	10.58	10.28	10.12

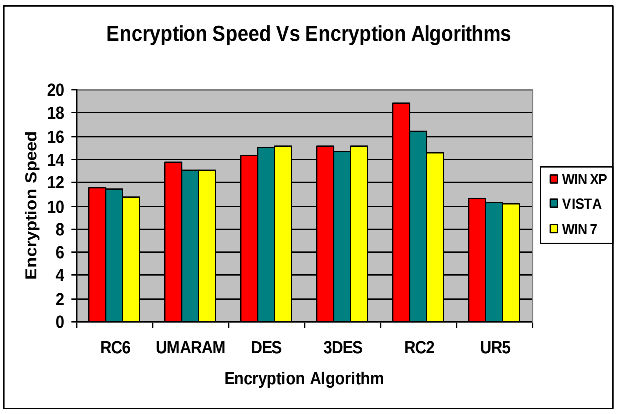

Figure 3: Execution speed for encrypting text data: Comparison between different OS

Figure 2 show the superiority of UR5 algorithm over other algorithms in terms of encryption speed. Another point can be noticed here; that RC2 requires more time than all algorithms. A third point can be noticed here; that RC6 has an advantage over other 3DES, DES and RC2 in terms of throughput especially in small size file. A fourth point can be noticed here; that 3DES has low performance in terms of encryption when compared with RC6. Compare the RC6 and 3DES, the RC6 has high performance. Another point is, the Windows 7 has better performance compare with other two platforms. Finally, it is found that RC2 has low performance and low throughput when compared with other five algorithms.

Table 2: Encryption Speed (in KB/sec) of Most Common Algorithms on different OS for image data

OS Encryption	Windows XP	Windows Vista	Windows 7
RC6	55.42	55.12	54.84
UMARAM	50.15	50.04	50.00
DES	56.32	55.25	55.05
3DES	60.42	59.88	58.52
RC2	58.54	58.54	58.50
UR5	51.25	51.12	51.03

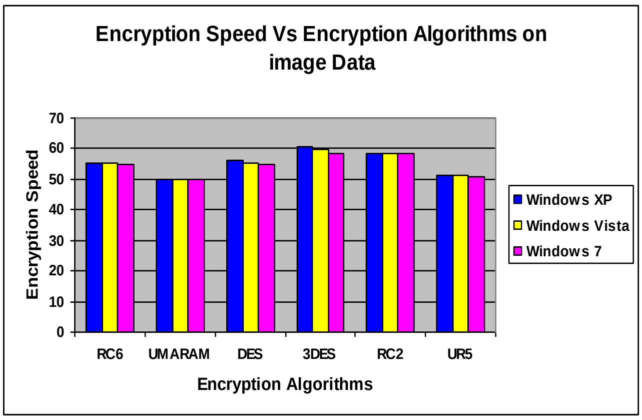

Figure 4: Execution speed for encrypting image data: Comparison between different OS

Experimental results for image data type (JPEG images) are shown (Table 2, and Figure 2) respectively.
From those results, it is easy to observe that RC2 still has disadvantage in encryption process over other algorithms in terms of encryption speed. On the other hand, it is easy to observe that RC2 and 3DES have disadvantage in encryption process over other algorithms in terms of time consumption. It is found that 3DES still has low performance when compared to DES. It is found that there is insignificant difference in performance of different symmetric key schemes in case of data transmission. The encryption of image data, the Windows7 operating system is better performance. The Windows XP platforms has low performance compare with other two platforms like Wndows7 and Vista.

6. CONCLUSION

This paper presents a performance evaluation of most common encryption algorithm on encryption speed. The most common algorithm are *RC6,UMARAM,DES,3DES,RC2 and UR5. Several points concluded from the experimental results.*

All algorithms run faster on Windows XP , but UR5 is the most efficient and UMARAM runs slower than DES and 3DES for Text data. UR5 encrypts images most efficiently on all 3 platforms. The UMARAM runs faster on Windows XP than 3DES.But on Windows Vista and Windows7, UR5 and UMARAM perform at the similar speed for Image data. In future , we try to incorporate good features of UMARAM and UR5 in a single algorithm, which can perform well on all latest platforms for all types of data.

7. REFERENCES

[1] William Stallings " Network Security Essentials (Applications and Standards)", Pearson Education, 2004.

[2] B.Schneier, *Practical Cryptography,*Wiley, 2003.

[3] National Bureau of Standards, " Data Encryption Standard," FIPS Publication 46, 1977.

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

[5] D. Salama, A. Elminaam and etal, "Evaluating The Performance of Symmetric Encryption Algorithms", International Journal of Network Security, Vo1.10, No.3, PP.216-222, May2010.

[6] 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.

[7] 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.

[8] S. Contini, R.L. Rivest, M.J.B. Robshaw and Y.L. Yin. "The Security of the RC6 Block Cipher. Version 1.0 ". August 20, 1998.

[9] Aamer Nadeem, Dr M. Younus Javed, " A Performance Comparison of Data Encryption Algorithms ", IEEE International Conference on Networking, 2009.

[10]A. A. Tamimi, Performance Analysis of Data Encryption Algorithms, Retrieved Oct. 1, 2008. (http://www.cs.wustl.edu/»jain/cse567-06/ftp/encryption perf/index.html)

[11] 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.

[12]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

[13] G. Ramesh, Dr. R. Umarani "A Novel Symmetrical Encryption Algorithm with High Security Based on Key Updating" gopalax Journals , International Journal of Computer Network and Security (IJCNS) Vol. 3 No. 1 pp 57-69, http://www.ijcns.com/pdf/207.pdf

[14]. Results of Comparing Tens of Encryption Algorithms Using Different SettingsCrypto++ Benchmark, Retrieved Oct. 1, 2008. (http://www.eskimo.com/weidailbenchmarks.html).

[15] W.S.Elkilani, "H.m.Abdul-Kader, "Performance of Encryption Techniques forReal Time Video Streaming, BIMAConference, Jan 2009, PP 1846- 1850.

[16]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.

[17] Jose J. Amador, Robert W.Green, " Symmetric-Key Block Ciphers for Image and Text Cryptography", International Journal of Imaging

[18] ANSI3.106, "American National Standard for Information Systems—Data Encryption Algorithm—Modes of Operation," American National Standards Institute, 1983.

[19] Institute of Electrical and Electronics Engineers, "Local and Metropolitan Area Networks: Overview and Architecture", IEEE Standard 802,1990.