I.J. Information Technology and Computer Science, **2012, 12, 60-66**
Published Online November 2012 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2012.12.06

Performance Analysis of Most Common Encryption Algorithms on Different Web Browsers

G. Ramesh
Research Scholar, Research and Development Centre, Bharathiyar University, Coimbatore
mgrameshmca@yahoo.com

R. Umarani, Dr.
Associate Professor in Computer Science, Sri Saradha college for women, Salem -16
umainweb@gmail.com

Abstract— The hacking is the greatest problem in the wireless local area network (WLAN). Many algorithms like DES, 3DES, AES,UMARAM, RC6 and UR5 have been used to prevent the outside attacks to eavesdrop or prevent the data to be transferred to the end-user correctly. We have proposed a Web programming language to be analyzed with five Web browsers in term of their performances to process the encryption of the programming language’s script with the Web browsers. This is followed by conducting tests simulation in order to obtain the best encryption algorithm versus Web browser. The results of the experimental analysis are presented in the form of graphs. We finally conclude on the findings that different algorithms perform differently to different Web browsers like Internet Explorer, Mozilla Firefox, Opera and Netscape Navigator. Hence, we now determine which algorithm works best and most compatible with which Web browser. A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as encryption/decryption speed in the different web Browsers. Experimental results are given to demonstrate the effectiveness of each algorithm.

Index Terms— Ur5, Encryption, Algorithms, Web Browsers, Data Security

I. Introduction

Encryption is the process of converting plain text “unhidden” to a cryptic text “hidden” to secure it against data thieves. This process has another part where cryptic text needs to be decrypted on the other end to be understood. Fig.1 shows the simple flow of commonly used encryption algorithms [1].

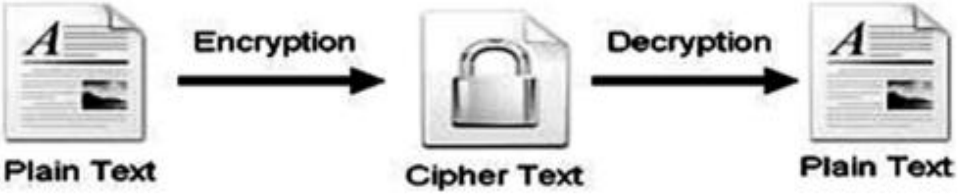


Fig. 1: Encryption-Decryption Flow

Wireless Local Area Network (WLAN) is one of the fastest-growing technologies. The demand for connecting devices without the use of cables is increasing everywhere. WLAN is found in the office buildings, and in many other public areas. The security in WLAN is based on cryptography, the science and art of transforming messages to make them secure and immune to attacks by authenticating the sender to receiver within the WLAN.

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, such as DES [2], TDES [3], AES [4], and RC6 [5],UMARAM[7], and UR5[8]. 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.

II. Conceptual Framework

In this study, we have proposed only one Web programming language script to be analyzed with five

Web browsers in order to determine which type of algorithm is suitable to which type of Web browser in terms of their performance and compatibility. Active Server Pages (ASP), has been selected and six different types of encryption algorithms have been chosen to be analyzed to observe their performance. The encryption algorithms selected are DES, 3DES, AES,UMARAM, RC6 and UR5. These encryption algorithms are known to be able to support 128-bit key size. Furthermore, the six types of algorithms will be co-analyzed with the five selected Web browsers that are able to process its scripts effectively and in an efficient manner.

Fig. 2: Different web browsers available in the market.

There are quite a number of Web browsers that are available in the market, but these five are known to be among the top and most popular. They are Internet Explorer, Mozilla Firefox, Opera, Netscape Navigator and Google Chrome. From the analysis, we hope to find out the most perfect web browsers that can match in the best possible way with the encryption algorithms for ASP scripts[9].

III. Methodology

Before implementing an encryption algorithm, we need to understand the principle behind the encryption i.e. to secure data held within a message or file and to ensure that the data is unreadable to others. The unencrypted message or file is often referred to as Plaintext, and the encrypted message or file is referred as Cipher text. In encryption, it consists of key length in number of bits. A key is a long sequence of bits used by encryption algorithms. Thus, the length of the key determines the probabilities if one ought to figure it out all its possible key values.

The commencement of the encryption process begins after the authorization to use the system has been obtained, only then that the information inputted be submitted. In order not to be intercepted by offender along the way, the text must first be encrypted prior to storage using the encryption secret codes along with its key known only to the sender and the receiver. For the receiver to be able to read it, the data has to be decrypted simply by reversing the process using the given key.

Asymmetric encryption techniques are almost 1000 times slower than Symmetric techniques, because they require more computational processing power.

The most common encryption algorithms are listed below:

AES: AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications[4].

DES: The 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 [2].

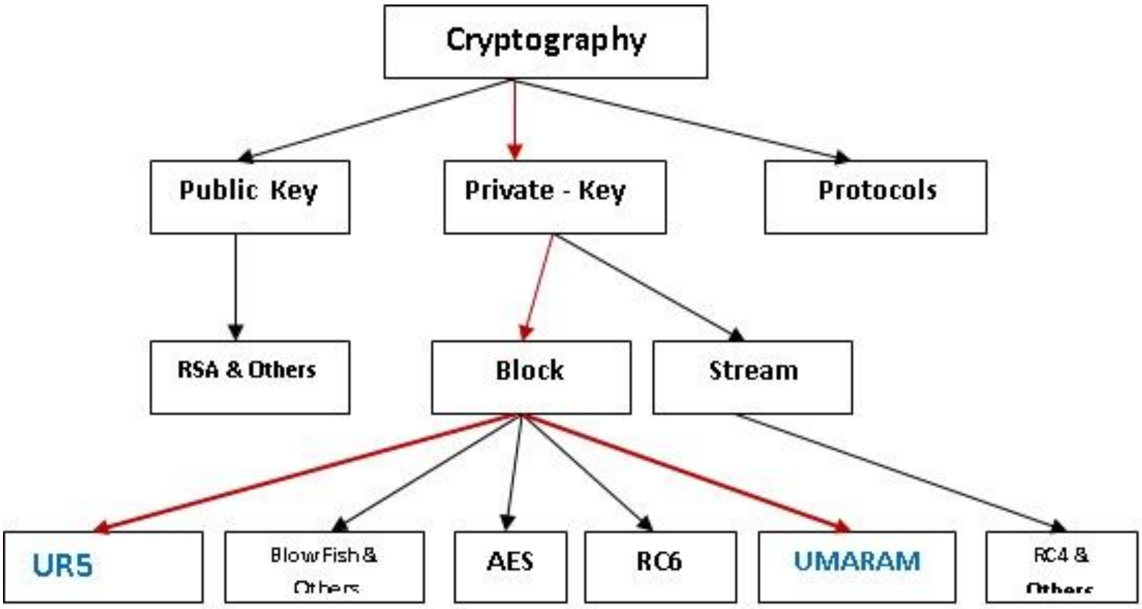


Fig. 3: Overview of the field of Cryptography

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 [3].

UMARAM: The UMARAM was designed by Ramesh G and R.Umarani in the year 2010. This 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 of 16 X 16 X 16. The S-Box consists of 16-slides, and each slide having 2-D of 16 x16. The numbers from 0 to 255 are arranged in random positions in each slide[7].

UR5:This algorithm was designed by G.Ramesh and Dr. R. Umarani in the end of the year 2010. 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 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. It is more efficient and useable for the Wireless Local Area Network because it avoids the using of the same key with other packets within a message. The algorithm is simple and helpful in avoiding the hackers. S-BOX generation is the backbone of this algorithm. It has eight columns and 256 rows; each element consists of 8-bits. It replaces the input by another code to the output.[8].

IV. Comparison of Desktop Web Browser Speed Test

We tend to find that different browsers (like different and latest versions like Chrome 17 vs Firefox 10 vs IE9 vs Opera 11 and Netscape Navigator) have different strong advantages and disadvantages over one another, but as with a lot of things in life; one of the key characteristics of a good browser is pure unadulterated speed. Different latest version of web browsers used in this research.

Google Chrome 17 has recently been released which features a new pre-rendering feature for faster page loading as well as integrating increased malware detection which checks every file downloaded to our machine for pestilence. The Firefox and Opera browsers have also recently launched new versions which have dramatically increased page loading times with Firefox 10 being publicly released and then version 11 entering beta not long after.

The first test focuses on how long it takes each browser to launch from the time the user decides to open it until it appears on our display, ready for action. The test had been slightly changed from previous versions, and is only timed up until it is ready for user communication. The graphics show that Chrome was unquestionably faster with Internet Explorer in second place followed by Opera and finally Firefox which lagged behind by approximately one second.

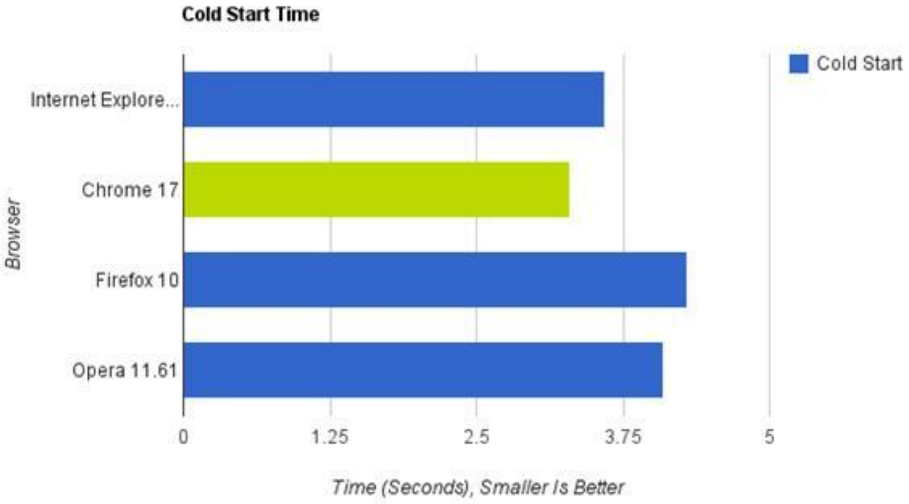


Fig. (3a): Browsers Cold Start time comparison

The second test was all about how quickly each browser could open up with ten tabs enabled with each tab containing a different URL with varying content ranging from the LifeHacker website to Facebook and Hulu. Having nine tabs open from the beginning will obviously place an increased load on the browser but Opera seemed to have no problems at all as it finished the processing task miles ahead of the competition with IE and Firefox achieving the objective at the same rate and Chrome surprisingly being a distant fifth place[13].

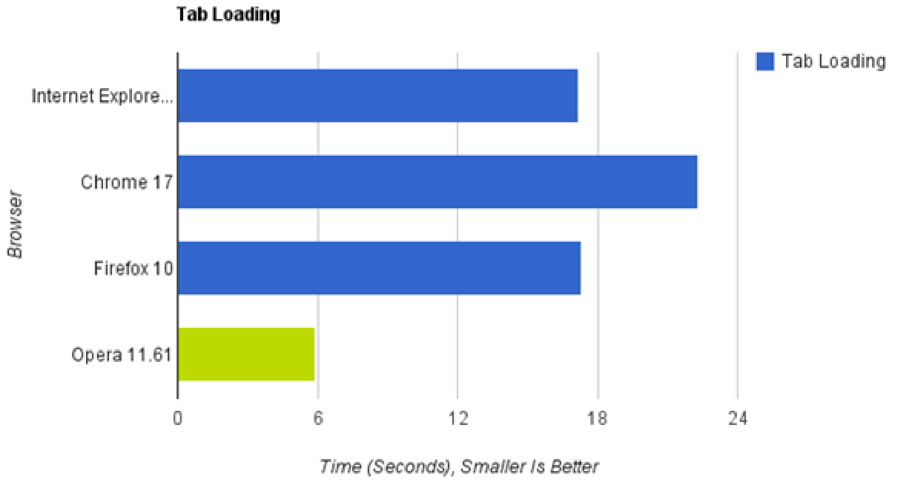
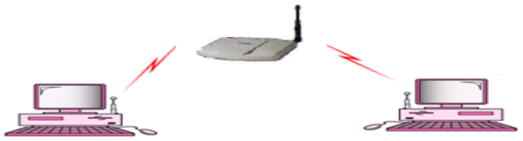


Fig. (3b): Browser tab Loading Comparison

This paper is organized as follows. Related work is described in Section 4. The proposed experimental design is described in section 5. Performance analysis are shown in section 6. Results are shown in 7.Finally the conclusions are in section 8.

V. Experimental Design

For our experiment, we use two Desktop system IV 2.4 GHz CPU, in which performance data is collected. The two Desktop computers (sender and receiver) had windows XP professional installed on it. The two Desktop Computer (sender and receiver) is connected to a router. See fig 3c.



PC1: Intel(R) Pentium(R) 4 CPU 2.8GHz, and 1GB of RAM with a 54M Wireless USB Adapter of BELKIN

PC2: Intel(R) Pentium(R) 4 CPU 2GHz, and 128MB of RAM with a 54M Wireless USB Adapter of BELKIN

Fig. (3c): Wireless LAN (infrastructure mode)

In the experiments, the laptop encrypts a different file size ranges from 20 K byte to 100.06 Mega Byte. The encryption time is considered the time that an encryption algorithm takes to produce a cipher text from a plaintext. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption.

In this study, we have proposed only one Web programming language script to be analyzed with five Web browsers in order to determine which type of algorithm is suitable to which type of Web browser in terms of their performance and compatibility. Active Server Pages (ASP), has been selected and six different types of encryption algorithms have been chosen to be analyzed to observe their performance.

There are quite a number of Web browsers that are available in the market, but these five are known to be among the top and most popular. They are Internet Explorer, Mozilla Firebox, Opera and Netscape Navigator and Google Chrome. From analysis, we hope to find out the most perfect web browsers that can match in the best possible way with the encryption algorithms for ASP scripts [9].

VI. Performance Analysis

In order to verify which of the six encryption algorithms perform better to the five Web browsers mentioned earlier, a test have been conducted using two desktop computers that have been setup and dedicated as Client and Server via a router. Encryption testing is to test the performance of six encryption algorithms in encrypting a set of text and key via Web browsers for ASP scripts. Thus, the text length starting at 10 will be increasing five times its initial characters, whereas the key length for each text length remains unchanged.

VII. Experimental Results

The outcome of the testing will project the response time i.e. the encryption process and the time taken of the five Web browsers namely Internet Explorer, Mozilla Firefox, Opera and Netscape Navigator and Google Chrome after performing the encrypting scripts timed in millisecond onto the computer screen. Fig. 4 to Fig. 8 were the test results after having increased the text length for each encryption algorithms for the five Web browsers by 10 characters, where it had been observed and noted of their performance results. Fig. 4 illustrates the result of Internet Explorer and its Text Length versus Response Time. From the analysis, UMARAM performs better compared to others and sustain almost lower response time. The RC6 is better than 3DES algorithm.

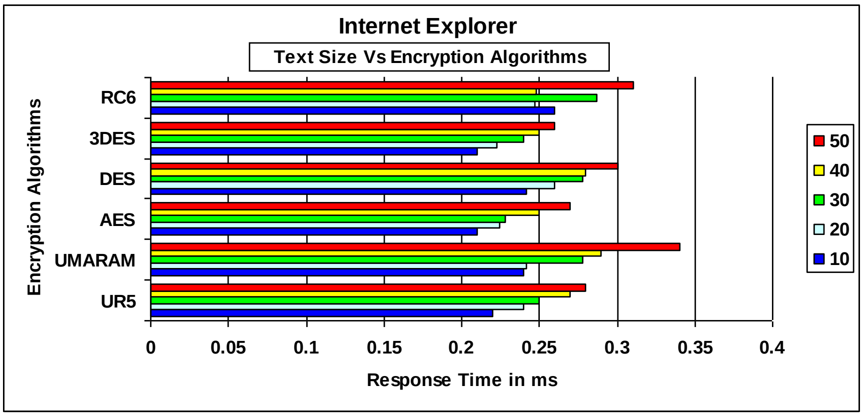


Fig. 4 Internet Explorer's Text Length vs. Response Time

Fig. 5 illustrates the result of Mozilla Firefox and its Text Length versus Response Time. From the analysis, UR5 yet again performs better compared to others and just about sustaining lower response time. It does however perform less at 20 and 40 Text Length with a couple of algorithm namely RC6 and AES.

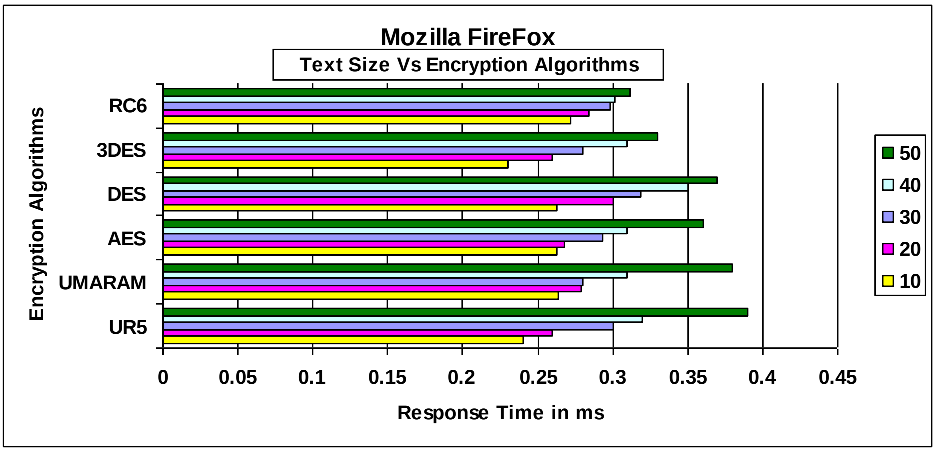


Fig. 5: Mozilla Firefox's Text Length vs. Response Time

Fig. 6 illustrates the result of Opera and its Text Length versus Response Time. From the analysis, DES performs slightly less than AES at the start. But nonetheless, it performs better for the remaining text lengths compared to others in its response time.

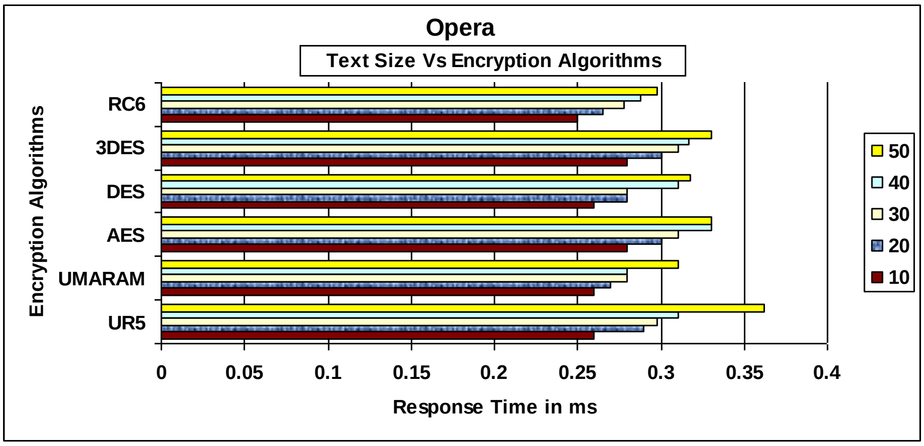


Fig. 6: Opera's Text Length vs. Response Time

Fig. 7 illustrates the result of Netscape Navigator and its Text Length versus Response Time. From the analysis, UMARAM had a good start and performs better compared to others up until 30 Text Length. Unfortunately, it failed to sustain its lower response time, whereby AES and DES had outperform in the last two text lengths.

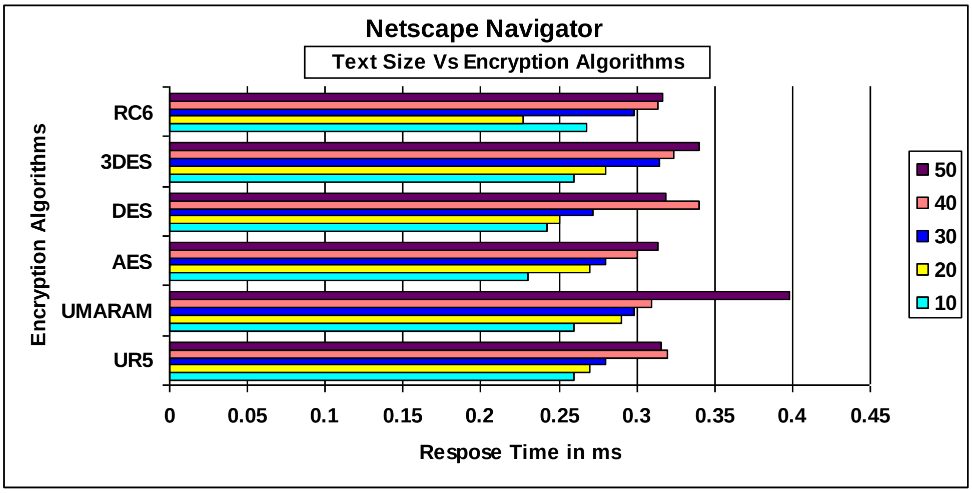


Fig. 7: Netscape Navigator’s Text Length vs. Response Time

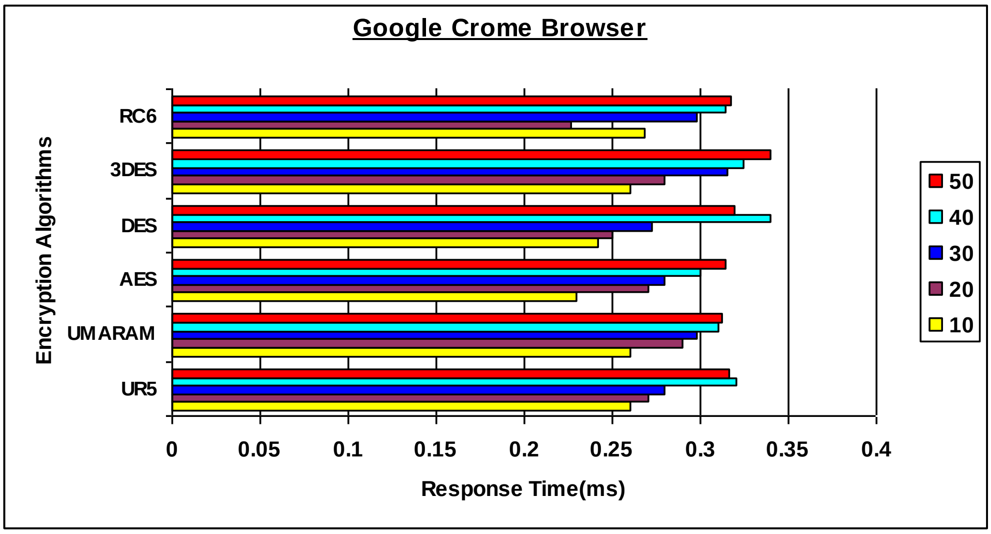


Fig. 8: Google Chrome’s Text Length vs. Response Time

Fig. 8 illustrates the result of Google Chrome and its Text Length versus Response Time. From the analysis, UR5 had a good start and performs better compared to others up until 30 Text Length. Unfortunately, it failed to sustain its lower response time, whereby AES and DES had outperform in the last two text lengths.

The following factors are affected the response time of web browsers.

1. Web Browser’s version.
2. Depends the operating system installed in the computer.
3. Depends the Computer configuration.

VIII. Conclusion

In an actual observation, the response time sometimes fluctuates when we ought to run the test twice with an encryption algorithm on the same Web browser using the same text length. This could be due to the network traffic or even the heavy usage of the Server. But in this case, there is only one Client and a Server, hence there should not be any traffic at all as only one Client accessing the Server. Thus, we can safely conclude that it must been caused by the time it takes for the Server to process the ASP script of an algorithm on the Web browser, along with many other processes running at the same time within the Server. This can cause the Central Processing Unit (CPU) usage amounting high, hence slows down the encryption process.

Therefore, apart from the network conditions that we are aware of from using Local Area Network (LAN), Wide Area Network (WAN) and Internet, Server also plays an important role for better performance. From our findings, we came to the conclusion that for a one-time run simulation test of an algorithm that performs best on Web browser are as follows: -

(i) Internet Explorer Web browser suited for DES encryption algorithms.

(ii) Mozilla Firefox Web browser suited for RC6 encryption algorithms.

(iii) Opera Web browser suited for UR5 encryption algorithms.

(iv) Netscape Navigator Web browser suited for DES encryption algorithms.

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

[4] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[5] 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.

[6] Syed Zulkarnain Syed Idrus1, Syed Alwee Aljunid, Salina Mohd Asi, Suhizaz Sudin, and R. Badlishah Ahmad" Performance Analysis of Encryption Algorithms' Text Length Size on Web Browsers" IJCSNS International Journal of Computer Science 20 and Network Security, VOL.8 No.1, January 2008 pp.22-25.

[7] 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

[8] Ramesh, G. Umarani, R," 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.

[9] Paul Morris "Desktop Web Browser Speed Test: Chrome 17 vs Firefox 10 vs IE9 vs Opera 11" February 15th, 2012 http://www.redmondpie.com/ desktop-web-browser-speed-test-chrome-17-vs-firefox-10-vs-ie9-vs-opera-11/

[10] 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.

[11] 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

[12] G. Ramesh and R. Umarani , Data Security in Local Area Network Based on Fast Encryption Algorithm, Communications in Computer and Information Science, 2010, Volume 89, Part 1, 11-26,http://www.springerlink.com/content/m330150 8219h7g66/

[13] Paul Morris ,Desktop Web Browser Speed Test: Chrome 17 vs Firefox 10 vs IE9 vs Opera 11, http://www.redmondpie.com/desktop-web-browser-speed-test-chrome-17-vs-firefox-10-vs-ie9-vs-opera-11/

Dr. **R. Umarani**:- Received her Ph.D., Degree from Periyar University, Salem in the year 2006. She is a rank holder in M.C.A., from NIT, Trichy. She has published around 40 papers in reputed journals and national and international conferences. She has received the best paper award from VIT, Vellore , Tamil Nadu in an international conference. She has done one MRP funded by UGC. She has acted as resource person in various national and international conferences. Her areas of interest include information security, data mining, fuzzy logic and mobile computing.

G. Ramesh:- He is working as Scholar in Research and development Centre, Bharathiyar University, Coimbatore,India. He has 12 years of experience in both Industrial and academic fields. He has published 21 Papers in International and national journals and 23 papers presented in national and international conferences. His area of Interest includes information security and Wireless Networks.