Performance Evaluation of Encryption Algorithms' Key Length Size on Web Browsers

Syed Zulkarnain Syed Idrus[1], Syed Alwee Aljunid[2], Salina Mohd Asi[3], Suhizaz Sudin[4]

Universiti Malaysia Perlis (UniMAP), Perlis, Malaysia

Summary
In this article, the research correlates to our previous study done on encryption algorithms' "text length size". However, in this study, the evaluation is analysed on a different means instead, which is the encryption algorithms' "key length size", but by imposing the same method and programming language over the same Web browsers in order to signify their performance differences. The performance is based on the encryption process of the programming language's script with the Web browsers. We had performed the simulation test by observing their performances as to which algorithm works best and most suited to which Web browser. The results were obtained and concluded in our findings.

Key words:
Data Security, Encryption Method, Encryption Algorithms, Web Browser, ASP.

1. Introduction

In today's technology advancement era, where computers are no longer the needs, but has become a nutrient of necessity to comply with and serve all activities [1,2]. In many organisations, they craved for secure, reliable, simple and flexible system. Thus, there is no security system that has been said to be foolproofed. However, researchers throughout the world are in search to strengthen the security systems and continue to make improvements to the ones that are existed in order to combat against the attackers.
In this study, similarly to the ones in our previous research article on encryption, we made a study on another aspect that is the key length size as opposed the previous ones of the text length size. In [3], the text length size was increased and the key length size remains unchanged, where we had monitored its performances and obtained a set of results. Here, is the reverse, whereby we had increased the key length size instead, but restrained the size of the text length.

2. Conceptual Framework

In our study, we have imposed a Web programming language script namely the Active Server Pages (ASP) that will be used to analyse with four Web browsers, which are Internet Explorer, Mozilla Firefox, Opera and Netscape Navigator as the ones that were utilised in [3]. This study will be conducted in order to determine which type of algorithm is suitable to which type of Web browser in terms of their performance and compatibility.
There are five types of encryption algorithms that were selected to be utilised, which will be used for the analysis namely Blowfish, International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES), Tiny Encryption Algorithm (TEA) and Twofish [1,3]. These encryption algorithms are known to be able to support 128-bit key size [4]. Subsequently, the five types of algorithm will be co-analysed with the four Web browsers mentioned earlier, which are able to process its scripts effectively and in an efficient manner.

3. Methodology

As stated in [1,3], the idea of an encryption is basically to secure the 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* (raw data), and the encrypted message or file is referred as *Ciphertext*. Figure 1 illustrates the process of data encryption from an unencrypted data into an encrypted data.

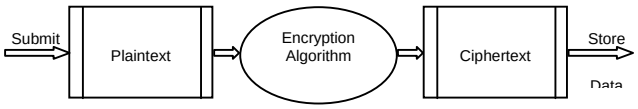

Figure 1: Data Encryption

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 key determines the probabilities if one ought to figure it out all its possible key values [1].
Figure 2 exemplifies the data before and after it is encrypted, then stored in a database. The two data are of the same values, where the one circled in blue is the unencrypted data (in English it stands for "School of Computer and Communication Engineering") and the encrypted data (funny characters) circled in red is

Manuscript received May 5, 2012
Manuscript revised May 20, 2012

encrypted using the Blowfish encryption algorithm.

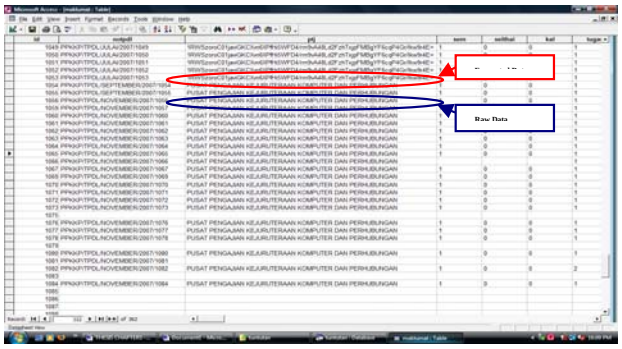

Figure 2: Encrypted Data vs. Raw Data Stored in the Database Using Blowfish Encryption Algorithm

4. Performance Analysis

A test was conducted by using two computers that have been setup and dedicated as Client and Server via a router in order to determine which of the five encryption algorithms perform better over the four Web browsers stated in Section 2. By performing the encryption testing, we would like to test the performance of the five encryption algorithms by encrypting a set of text and key via Web browsers on an ASP scripts. Thus, the key length starting at 10 will be increase four times its initial characters, whereas the text length for each key length remains static.

5. Simulation Test

The encryption test involves in testing the performance of the encryption algorithms and to perceive which of the algorithms have the best performance in attaining or able to sustain lower response time.

Figure 3 shows a sample of how a fifty-character text i.e. MalaysiannMalaysiannMalaysiannMalaysiannMalaysiann will be encrypted using a six-character key or password i.e. UniMAP by using AES encryption algorithm on Mozilla Firefox Web browser.

Figure 3: Encrypt Fifty Characters Using Six Characters Key (or Password)

Figure 4 illustrates the output as a result of the fifty-character that was encrypted by using the UniMAP key or password on AES encryption algorithm and projected the response time that it took to process the encryption. Hence, it took 0.3047 milliseconds on Mozilla Firefox.

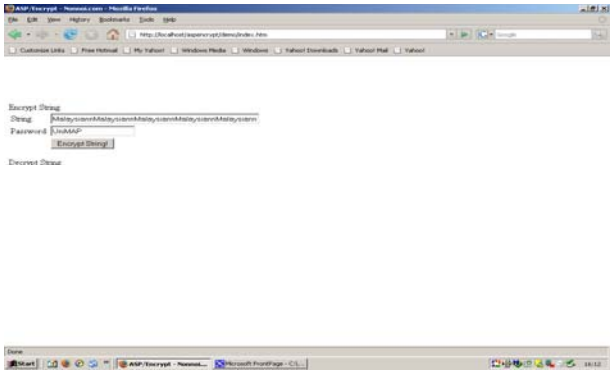

Figure 4: Encryption Outcome of Fifty Characters Using Six Characters Key (or Password)

6. Results

The outcome of the testing will project the response time i.e. the encryption process and the time taken for the four Web browsers namely Internet Explorer, Mozilla Firefox, Opera and Netscape Navigator after performing the encrypting scripts timed in *milliseconds* onto the computer screen. Figure 5 shows how we performed the timing calculations on ASP to obtain the response time. Figure 6 to 9 were the test results after having increased the key length for each encryption algorithms for the four Web browsers by 10 characters, where it had been observed and noted of their performance results.

```
Dim StartTime : StartTime = Timer() [variable]

… Encryption Script (i.e. Listings … [encryption script]

Response.Write(Timer() – StartTime) [time calculation script]
```

Figure 5: Response Time in ASP

Figure 6 illustrates the result of Internet Explorer and its Key Length versus Response Time. From the analysis, Twofish had performed better compared to others and sustained lower response time.

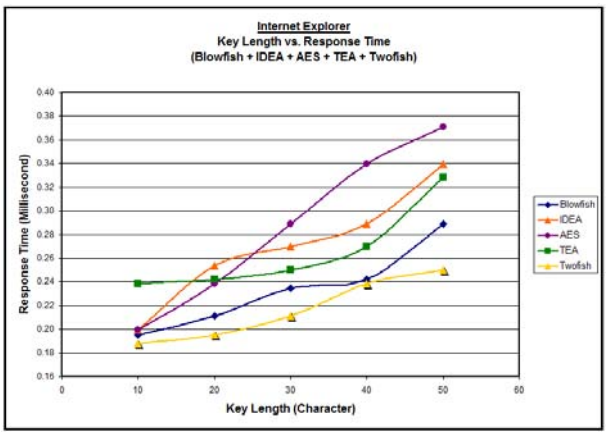

Figure 6: Internet Explorer's Key Length vs. Response Time

Figure 7 illustrates the result of Mozilla Firefox and its Key Length versus Response Time. From the analysis, AES had performed better compared to others and lower response time at the beginning and end. It does however, perform slightly less in between 30-40 Key Length than a couple of algorithm namely IDEA and Twofish.

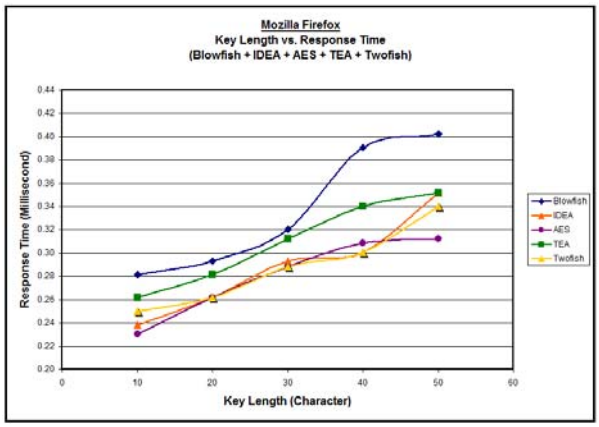

Figure 7: Mozilla Firefox's Key Length vs. Response Time

Figure 8 illustrates the result of Opera and its Key Length versus Response Time. From the analysis, Twofish had performed better compared to its rival Blowfish for the first two Key Length i.e. 10 and 20. Nonetheless, Blowfish had improved all the way through and far better at the end compared to others in its response time.

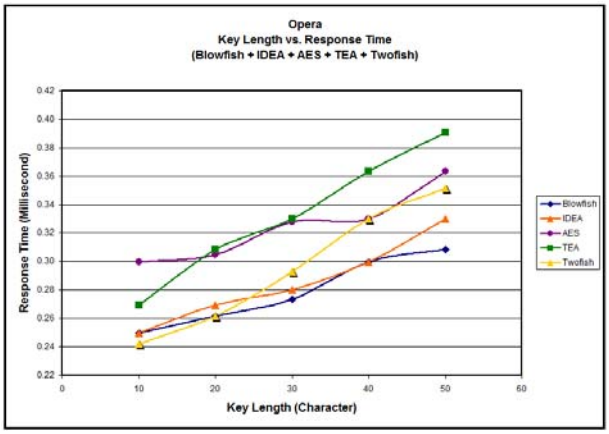

Figure 8: Opera's Key Length vs. Response Time

Figure 9 illustrates the result of Netscape Navigator and its Key Length versus Response Time. From the analysis, Blowfish had performed better compared to IDEA and also its rival Twofish for the first two Key Length i.e. 10 and 20. Instead, none of them had sustained lower response time, whereas IDEA, which initially had a bad start has outperforms the others at the last three i.e. 30, 40 and 50 Key Length.

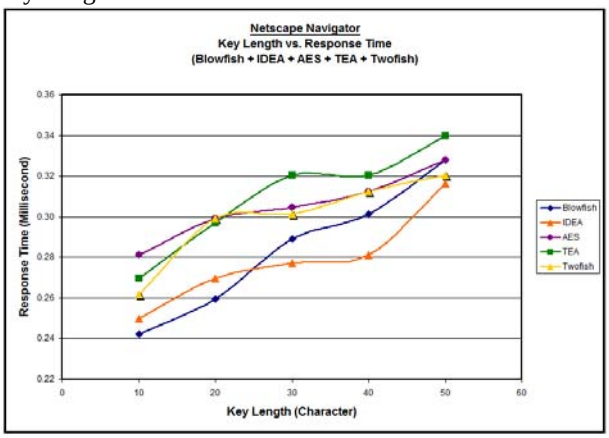

Figure 9: Netscape Navigator's Key Length vs. Response Time

7. Conclusions

From the analysis, different encryption algorithms obviously perform better with different Web browsers. But, the testing was conducted on a one-time run for all encryption algorithms.

Based on our observation during the simulation, the response time may vary when we run the test twice with an encryption algorithm on the same Web browser using the same key length. The reason could be because of the

network traffic or perhaps on the Server heavy usage. But in our case, we tested it solely on a Client and Server machines.
Thus, in our findings, we came to the conclusion that for a one-time run test of an algorithm that performs best on Web browser by increasing the key length size are as follows: -

(a) Internet Explorer Web browser suited for Twofish encryption algorithms.
(b) Mozilla Firefox Web browser suited for AES encryption algorithms.
(c) Opera Web browser suited for Blowfish encryption algorithms.
(d) Netscape Navigator Web browser suited for IDEA encryption algorithms.

Acknowledgments

The authors would also like to express their cordial thanks to the Research, Management and Innovation Centre, Universiti Malaysia Perlis (UniMAP), Perlis, Malaysia for the support and had made this paper possible for publication.

References

[1] S. Z. Syed Idrus. Database encryption for a web-based claims system. Master's thesis, School of Computer and Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia, 2008.
[2] S. Z. Syed Idrus, A. Z. Rozali, and H. Desa. The development of a web-based claims system. In *Proceedings of the 2009 International Conference on Computer Technology and Development*, volume 1, pages 317 – 321, Sabah, Malaysia, 13-15 November 2009. IEEE Computer Society.
[3] S. Z. Syed Idrus, S. A. Aljunid, S. M. Asi, S. Sudin, and R. B. Ahmad. Performance analysis of encryption algorithms text length size on web browsers. *International Journal of Computer Science and Network Security*, 8(1):20–25, 2008.
[4] http://en.wikipedia.org/wiki/… (cipher)

Syed Zulkarnain Syed Idrus received the B.Sc. degree in Information Systems Engineering from University of Manchester Institute of Science and Technology (UMIST), United Kingdom and M.Sc. degree in Computer Engineering from Universiti Malaysia Perlis (UniMAP), Malaysia in 2001 and 2008, respectively. He started his career as an IT Support Executive cum Trainer (from 2002) in Cosmopoint College of Technology Penang, Malaysia and Information Systems Officer (from 2005) at the Universiti Sains Malaysia (USM), Malaysia. He is a lecturer at UniMAP (from 2009) and currently on study leave. He is pursuing a Ph.D. degree in Computer Science and Applications at University of Caen Lower-Normandy, France specialising in biometrics. His research interest includes information systems, systems development, biometrics, pattern recognition, encryption and information security. He was also members of The British Computer Society and International Association of Computer Science and Information Technology (IACSIT) in 2001 and 2009, respectively.

Syed Alwee Aljunid Syed Junid received the B.Eng. degree in Computer and Communication System (First Class Honours) and Ph.D. in Communication and Network Engineering from University Putra Malaysia (UPM), Malaysia in 2001 and 2005, respectively. He is a Full Professor at the School of Computer and Communication Engineering and currently the Dean of Research, Management and Innovation Centre, Universiti Malaysia Perlis (UniMAP), Malaysia.

Salina Mohd Asi completed her B.CompSc. degree at Universiti Teknologi Malaysia (UTM), Malaysia in 1995. After working for about a year, she pursued her study in M.Sc. degree in Real-Time Software Engineering at UTM. After she had completed her Master's degree, she worked in industry for 6 years before joining the Universiti Malaysia Perlis (UniMAP), Malaysia as a lecturer. Her research interest includes artificial intelligence in embedded system, artificial neural network, image processing, bioinformatic (protein analysis) and parallel computing.

Suhizaz Sudin received the B.IT. (Hons.) degree, from University Utara Malaysia (UUM), Malaysia in 1998. After his graduation, he had been working with several organizations before he pursued a M.Sc. degree in Computer Science from University Putra Malaysia (UPM), Malaysia. He then joined Legenda Group of Colleges as a lecturer until 2004. Later, he became a lecturer and also had been appointed as a Deputy Director of Centre for Industrial Collaboration in Universiti Malaysia Perlis (UniMAP), Malaysia. Now, he is a Senior Lecturer at UniMAP. His research interest includes computer networks (network security, network modeling, network performance study), ubiquitous computing, distributed, parallel and GRID computing and information systems. Currently, he is pursuing a Ph.D. and in his final year, researching on Network Performance at Massey University, New Zealand.