ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 10, October 2015

Performance Comparison of Symmetric Algorithms for SMS Communication

Amardeep Kaur[1], Rohit Dhadwal[2]

Assistant Professor, Punjabi University Regional Centre for Information Technology and Management, Mohali, India[1]

M.Tech Student, Punjabi University Regional Centre for Information Technology and Management, Mohali, India[2]

Abstract: A popular way for mobile phone users to send and receive simple text messages is Short Message Service (SMS). A secure communication channel and environment for confidential data transmission is missing in the literature for SMS; therefore it is desirable to secure SMS by additional encryption. Encryption algorithms differ from one another by their ability to identify &prevent the valuable data against data hack attacks and their speed and efficiency in doing securing data. This study provides a performance comparison between the best symmetric encryption algorithms for usage in SMS communication: Blowfish and RC4 (Rivest Cipher 4)). The comparison analysis ran on parameters: size of text data, encryption time, decryption time, encryption throughput, decryption throughput, average encryption time and average decryption time. Based on analysing the criteria's for efficient way of securing SMS, performance analysis of these algorithms under different parameters and input features is provided in the conclusion section.

Keywords: Cryptography, Decryption, Encryption, Blowfish, RC4.

I. INTRODUCTION

Many encryption algorithms are widely available and used in information security [2, 3, and 4]. The capacity, value and importance of exchanged information over the internet or other media types is increasing day by day. Thus,to offer the best solution and necessary protection against the data hackers along with providing the data security services under timely manner is most active research subject in the security related communities. This study presents a comparison between the most suitable algorithms in the data encryption field for making Short Message Service (SMS) communication most effective. Our main concern is with the performance and the speed of theses algorithms under test for use in low storage, fast processing and mobile devices. The comparison presented takes into consideration the performance of the algorithms for different size of text input. In the second section of this paper we briefly mention two best Cryptography Algorithms. Section III will show the simulation results of all analysed algorithms under different settings and performance of each algorithm based on performance metrics displayed in form of graphs. Section IV will walk through the conclusion of the paper and the relatively the advantages the algorithms and Section V will hint you through the work which can be carried out in future.

II. CRYPTOGRAPHIC ALGORITHMS

This section provides the readers with the necessary information for the algorithms in comparison.

A. Blowfish

Introduced in 1993 [5], a symmetric key block cipher technique [12 and 13]. Provided by Bruce Schneier – one of the world's leading cryptologists. He is the president of Counterpane Systems, which is a consulting firm specializing in cryptography and computer security [18]. Blowfish a variable length key from 32 bits to 448 bits [6]. It uses Feistal cipher network and uses large key dependent S-boxes. This algorithm can be optimized in hardware applications though it is mostly used in software applications. The algorithm operates with two parts: a key expansion part and a data encryption part [8]. The role of key expansion part is to convert a key of at most 448 bits into several sub key arrays totalling 4168 bytes [8]. A 16-round Feistel network is used for data encryption [7]. It is suitable for application where the key does not change often, like an automatic file encryption application and a communications link [12].

B. RC4

Developed by Ronald Rivest of RSA in 1987, this symmetric key Stream Cipher algorithm has variable key 256-bits to initialize a 256-bit state table [9, 10 and 14]. Suitable state size is 1684 bits. RC4 encryption algorithm normally uses 64 bit & 128 bit key sizes [1]. Pseudo-random bits are generated from a State Table. These Pseudo-random bits are XOR with the plain text to generate the cipher text. It consists of 2 parts: Key Scheduling Algorithm (KSA) & Pseudo-Random Generation Algorithm (PRGA) [15]. Due to its weaknesses, in 2014, Ronald Rivest gave a talk and published a paper on updated redesign called Spritz [17].

III. RESULT OF PERFORMANCE COMPARISON

These results are carried out using simulation developed by Java language on Eclipse IDE. The methodology is tested on simple plain text input and the results are calculated for encryption time, decryption time, encryption throughput, decryption throughput, average encryption time and average decryption time for variable text size less. Using these simulations Encryption and Decryption time, throughput and average encryption and decryption time can be determined.

DOI 10.17148/IJARCCE.2015.41013

The Encryption time with varying text sizes is displayed in this Table I. The encryption time is calculated in nanoseconds and text size in bytes. Average encryption time is calculated as the total encryption time divided by total bytes encrypted. The throughput of the encryption scheme is calculated as the total plaintext in bytes encrypted divided by the encryption time. More the throughput, more the speed of the algorithm & less will be the power consumption [16].

TABLE I ENCRYPTION TIME FOR SMALL TEXT SIZE

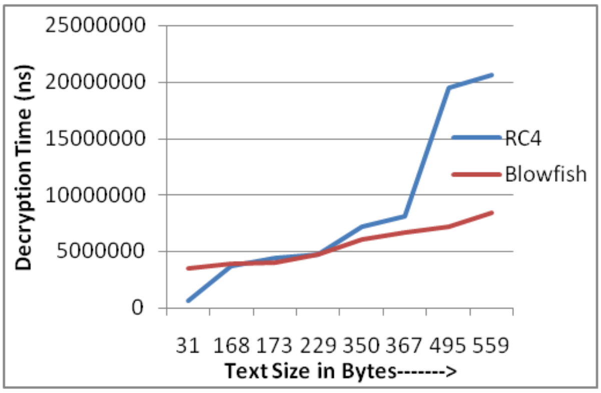
Text Size (Bytes)	RC4 (nanoseconds)	Blowfish (nanoseconds)
31	643571	57168759
168	3346141	65575803
173	3439362	70425890
229	5569347	44302474
350	7688640	60763776
367	7961035	43408316
495	21720195	61697273
559	22733230	58143309

The Decryption time with varying text sizes is displayed in the Table II. Decryption time can be determined by calculating the total cipher text decrypted over the decryption time. Average decryption time is calculated as the total decryption time divided by total bytes. The throughput of the decryption scheme is calculated as the total bytes decrypted divided by the decryption time.

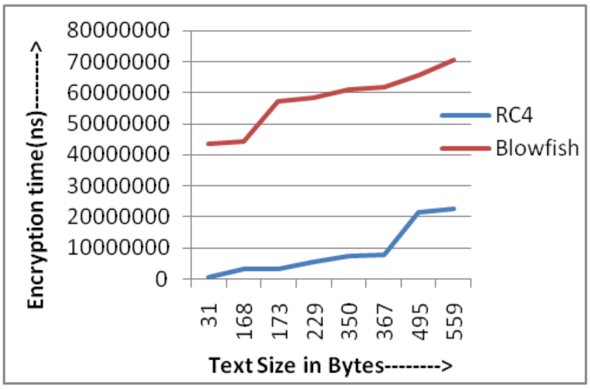
TABLE II DECRYPTION TIME FOR SMALL TEXT SIZE

Text Size (Bytes)	RC4 (nanoseconds)	Blowfish (nanoseconds)
31	623473	3496236
168	3696363	6676886
173	4709399	40745088
229	4447694	7135725
350	7148981	3939253
367	8086756	8412604
495	19538468	4036323
559	20616503	6047855

Graphical Comparison for Encryption and Decryption with varying text sizes.

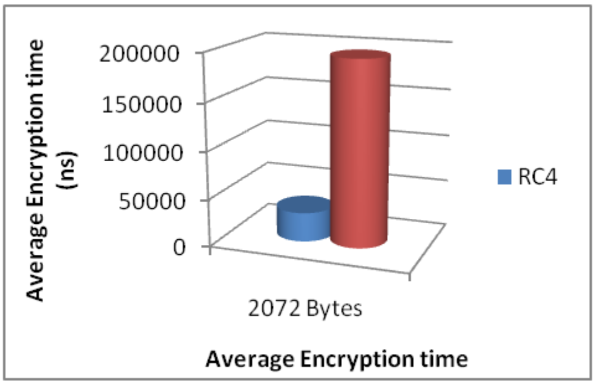


(a)

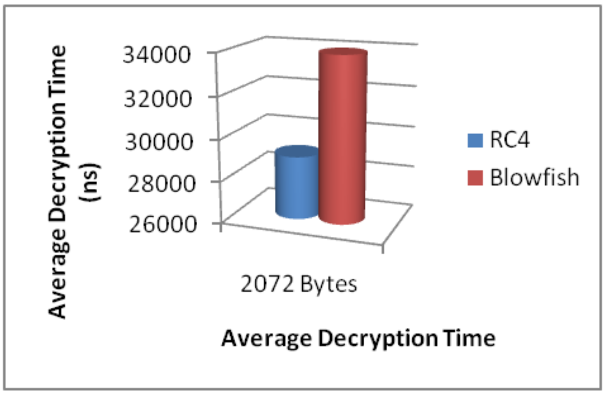


(b)

Figure (a) and (b) showing Encryption Time and Decryption Time for different text sizes.

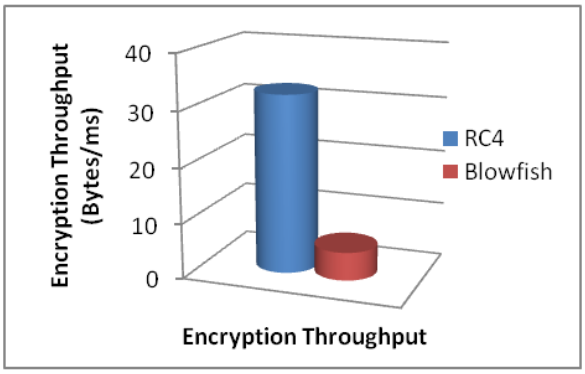


(c)



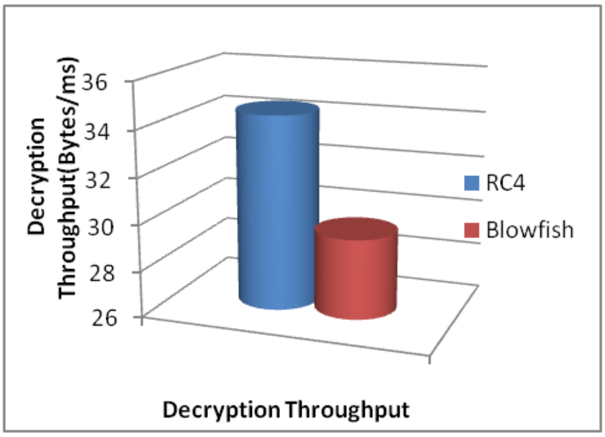
(d)

Figure (c) and (d) showing Average Encryption Time and Average Decryption Time for different text sizes.



(e)

DOI 10.17148/IJARCCE.2015.41013



(f)

Figure (e) and (f) showing Encryption Throughput and Decryption Throughput for different text sizes.

IV. CONCLUSION AND FUTURE SCOPE

The proposed methodology compared the symmetric cryptographic algorithms RC4 stream cipher and Blowfish block cipher on different setting of text sizes for Short Messages Services (SMS) of 160 characters. Analysis found that for small text size like SMS message size, performance of RC4 stream cipher is better than Blowfish Block Cipher. Encryption time of RC4 symmetric encryption algorithm is less than Blowfish symmetric encryption algorithms and decryption time of Blowfish is less than RC4 decryption algorithm. So, RC4 has better encryption performance and Blowfish has better decryption performance for small message texts. The Average Encryption time and Average Decryption time for both algorithms is greater for Blowfish algorithm which implies that Performance of RC4 is greater than Blowfish algorithm. Also, throughput value of Blowfish is greater than RC4 symmetric algorithms that imply RC4 has better performance and efficiency than Blowfish algorithm that further implies that Power consumption for RC4 algorithm is less than Blowfish algorithm. This study encourages beginners to work in the RC4 and Blowfish algorithms for their efficient software Implementation in SMS message communication. An extension to this research work can be an android application based implementation of the best algorithm for SMS encryption. Comparative analysis of Encryption and Decryption speed with varying key sizes for Encryption and decryption can also be carried out. Also, the performance analysis of these two algorithms for power utilization and memory utilization for SMS can be done.

REFERENCES

[1] A. Fenyi and J. G. Davis, "Comparative Analysis of Advanced Encryption Standard, Blowfish and Rivest Cipher 4 Algorithms Abstract :," vol. 3, no. 11, pp. 384–392, 2014.
[2] K. Acharya, "Analysis of Cryptographic Algorithms for Network Security," vol. 3, no. 2, pp. 130–135, 2014.
[3] A. Gupta and N. K. Walia, "Cryptography Algorithms : A Review," vol. 2, no. 2, pp. 1667–1672, 2014.
[4] R. Masram, V. Shahare, J. Abraham, and R. Moona, "Analysis and Comparison of Symmetric Key Cryptographic Algorithms Based on Various File Features," Int. J. Netw. Secur. Its Appl., vol. 6, no. 4, pp. 43–52, 2014.
[5] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (Blowfish)," Int. J., vol. 1, no. 4, Fast Softw. Encryption, pp. 191–204, 1994.
[6] R. Singh, R. Misra, and V. Kumar, "analysis the impact of symmetric cryptographic algorithms," 2013.
[7] C. H. Meyer, "Ibm frg," pp. 150–154, 1989.
[8] R. Arora and S. Sharma, "Performance Analysis of Cryptography Algorithms," Int. J. Comput. Appl., vol. 48, no. 21, pp. 35–39, 2012.
[9] W. Stallings, "the Rc4 Stream Encryption Algorithm," p. 7, 2005.
[10] A. Mousa and A. Hamad, "Evaluation of the RC4 Algorithm for Data Encryption," Int. J. Comput. Sci. Appl., vol. 3, no. 1, pp. 44–56, 2006.
[11] D. Salama, A. Elminaam, H. M. A. Kader, and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms on Power Consumption for Wireless Devices," Int. J., vol. 1, no. 4, pp. 343–351, 2009.
[12] Cryptanalysis and Design of Symmetric Cryptographic Algorithms, no. March. 2011.
[13] Blowfish Algorithm available at <http://iitd.vlab.co.in/index.php>
[14] W. Stallings, "the Rc4 Stream Encryption Algorithm," p. 7, 2005.
[15] A D. I. Amd, "SHA1 Encryption Algorithm ARM - DSP Group," New York, pp. 14228–14228, 2003.
[16] C. Haldankar and S. Kuwelkar, "Implementation Of AES And Blowfish Algorithm," pp. 2319–2322, 2014.
[17] RC4 algorithm available at <http://www.tempusfugit.ca/sitewatch/rc4.html>
[18] Blowfish algorithm available at <http://www.ece.ualberta.ca/~elliott/ee552/studentAppNotes/1998f/blowfish_encryption/>

DOI 10.17148/IJARCCE.2015.41013