Through Put Analysis of Various Encryption Algorithms

[1]Gurjeevan Singh, [2]Ashwani Kumar Singla, [3]K.S. Sandha
[1]S.B.S.C.E.T. (Polywing), Ferozepur, Punjab, INDIA
[2]G.T.B.K.I.E.T. Chappianwali, Malout, Punjab, INDIA
[3]Thapar University, Patiala, Punjab, INDIA

Abstract
In today's world of networks, communication without security is not reliable. Encryption Algorithm provides the security to the users in the network the main goal of this research is to provide the fair performance comparison of various Encryption Algorithms at different text data packets. This paper presents the comparison of various Algorithms or different text file sizes to evaluate the average speed of Encryption and Decryption process. Experimental results in visual basic language shows the superiority of blowfish Algorithm over the other Algorithm in terms of throughput.

Keywords
AES, Blowfish, Cryptography, Network Security.

I. Introduction

In recent years internet applications are exploring day by day such as online banking, online shopping, stock market and bill payments etc. Without security these applications are impossible, Encryption Algorithms provides the security to the information which is exchange over internet. The encryption algorithms are usually summarized into two popular types: Symmetric key encryption and Asymmetric key encryption. In Symmetric key encryption, only one key is used to encrypt and decrypt data. The key is distributed before transmission between entities. Therefore, key plays an important role in Symmetric key encryption. Strength of Symmetric key encryption depends on the size of key used. For the same algorithm, encryption using longer key is harder to break than the one done using shorter key. The representative Symmetric key cryptography algorithms include RC2, DES, 3DES, RC5, Blowfish, and AES, which use certain- or variable-length key. Asymmetric key encryption is used to solve the problem of key distribution. In Asymmetric key encryption, private key and public key are used. Public key is used for encryption and private key is used for decryption. However, public key encryption is based on mathematical functions, and is not very efficient for small mobile devices [9]. All the algorithms are extensively used for security of wireless networks. It is essential to evaluate their performance to ensure their domain applications. It is also significant to facilitate the process of the encryption algorithm.

II. Related Work

In this section, we have studied a number of articles that make comparison in terms of performance between the common encryption algorithms like AES, 3DES, DES and Blowfish. It was shown in [2] 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 [3] 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 (most of the resources are consumed for data transmission rather than computation). Even under the scenario of data transfer it would be advisable to use AES scheme in case the encrypted data is stored at the other end and decrypted multiple times. 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. Reducing the number of rounds leads to power savings but it makes the protocol insecure for AES and should be avoided. Seven or more rounds can be considered fairly secure and could be used to save energy in some cases. In [5], the author compares the various encryption algorithms with different settings for each algorithm such as different sizes of data blocks, different data types and battery power encryption / decryption speed. This paper organized as follow: Introduction in section I, related work in section II, experimental setup design in section III, results in section IV and last section V explains the conclusion and future scope of present study.

III. Experimental Set-Up Design

For our 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.

IV. Experimental Results

All the four Encryption Algorithms have been tested with different text size files. The fig. 1 shows the screen shot of software using which the user firstly select derive then folder after this particular file and at last the type of algorithm.

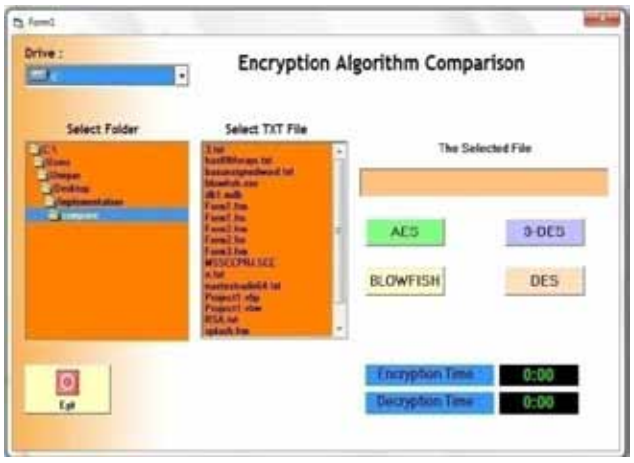

Fig. 1 : Screen shot of the Software

Screen shot of software shows that all the four encryption algorithms can be implemented to different file sizes. Comparison of throughput has been explained in the following table 1 and also the execution time of various encryption algorithms on different text file sizes.

Table 1: Comparative Throughput (Mb/sec) of various algorithms with different packet size

Text File Size in Kbytes	AES	3DES	Blowfish	DES
20	42	34	25	20
48	55	55	37	30
108	40	48	45	35
241	91	82	46	51
322	115	115	48	47
780	165	170	65	85
910	213	230	68	145
5501	260	310	120	250
7200	210	286	109	260
7838	1240	1470	122	1280
22335	1370	1800	155	1720
42000	1530	2300	165	2100
99000	1720	2750	190	2600
Average Time	542.38	742.31	91.92	663.31
Throughput (Mb/sec.)	25.80	18.85	152.25	21.09

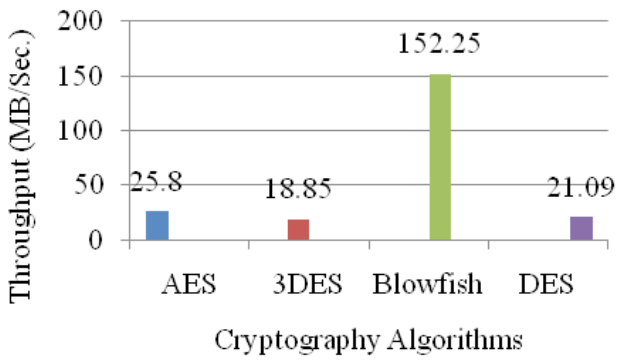

Fig. 2 : Throughput (Mb/Sec.) of Encryption Process

The simulation results for this comparison shown in fig 2 and table 1. The result shows the superiority of Blowfish algorithm over the other algorithms in terms of the throughput of encryption process. Because more the throughput; more the speed of the algorithm & less will be the power consumption. Second point can be noticed here that AES has advantage over the other 3DES and DES in terms of throughput & encryption time except Blowfish. In third point we say can that DES has better performance than 3DES. Fourth point which has been concluded that 3DES has least performance. Hence Blowfish is the best of all.

Table 2: Comparative Throughput (Mb/sec) of various algorithms with different packet size"

Text File Size in Kbytes	AES	3DES	Blowfish	DES
20	45	40	28	34
48	63	53	37	50
108	57	50	29	47
241	61	78	53	72
322	77	88	67	75
780	150	151	95	122
910	144	173	90	160
5501	172	180	102	168
7200	165	1108	85	988
7838	660	1507	150	1052
22335	885	1708	140	1200
42000	998	2030	190	1800
99000	1208	2730	210	2200
Average Time	360.38	761.23	98.15	612.92
Throughput (Mb/sec.)	38.83	18.38	142.58	22.83

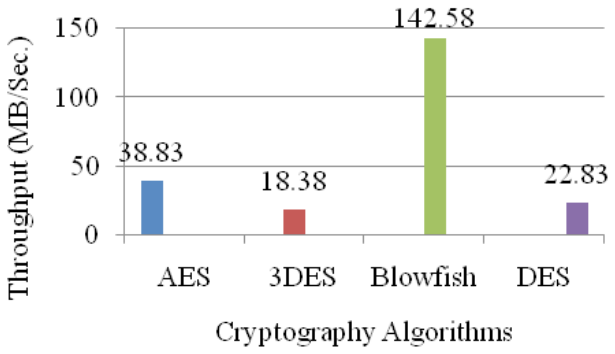

Fig. 3 : Throughput (Mb/Sec.) of Decryption Process

The simulation results for this comparison shown in fig 3 and table 2. The result shows the superiority of Blowfish algorithm over the other algorithms in terms of the throughput of Decryption process. Because more the throughput; more the speed of the algorithm & less will be the power consumption. Second point can be noticed here that AES has advantage over the other 3DES and DES in terms of throughput & decryption time except Blowfish. In third point we say can that DES has better performance than 3DES. Fourth point which has been concluded that 3DES has least performance. Finally it is concluded that Blowfish is the best of all.

V. Conclusion and Future Scope

This paper 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. In future we can perform same experiments on image, audio & video as well. With the improved results we can design a more efficient intrusion detection system.

References

[1] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks." IBM Journal of Research and Development, May 1994, pp. 243-250.

[2] Ruangchaijatupon, P. Krishnamurthy, ''Encryption and Power Consumption in Wireless LANs-N,'' The Third IEEE Workshop on Wireless LANs -September 27-28, 2001- Newton, Massachusetts.
[3] S.Hirani, ''Energy Consumption of Encryption Schemes in Wireless Devices Thesis,'' university of Pittsburgh, April 9, 2003.
[4] R.Chandramouli, "Battery power-aware encryption - ACM Transactions on Information and System Security (TISSEC),'' Vol. 9 Issue 2, May 2006.
[5] Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader, Mohie Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", International Journal of Computer Science and Network Security, Dec 2008.
[6] A.Sindhuja, R. Logeshwari, K. Thirunadana Sikamani, "A Secure PMS based on Fingerprint Authentication and Blowfish Cryptographic Algorithm", Proceedings of 2010 IEEE International conference on Signal and Image Processing (ICSIP-2010), 15-17 Dec. 2010, pp 424-429.
[7] Shish Ahmad, Mohd. Rizwan beg, Qamar Abbas, "Energy Efficient Sensor Network Security Using Stream Cipher Mode of Operation", Proceedings of 2010 IEEE International Conference on Computer & Communication Technology (ICCCT-2010), pp 348-354.
[8] Hardjono, ''Security in Wireless LANS and MANS,'' Artech House Publishers 2005.
[9] W.Stallings, ''Cryptography and Network Security 4th Ed,'' Prentice Hall, 2005, pp. 58-309.

Gurjeevan Singh was born in Punjab, INDIA in 1985. He has done his B-Tech. from P.T.U. Jalandhar. He has published various papers in internationals journals. Presently, he is pursuing M-Tech. from PTU and he is the Deptt. In charge ECE at SBSCET (Polywing) Ferozepur. His main Research interests are Network Security, wireless communications and VLSI design.

Ashwani Kumar Singla was born in Punjab, INDIA in 1975. He has received his B-Tech. from G.N.D.U. Amritsar and M-Tech. from PTU, Jalandhar. He has 12 years of experience of teaching and research and published various papers in national and international journals. Presently he is working as Asst. Prof & HOD of ECE Deptt in GTBKIET, Chappianwali (Malout).

K.S. Sandha was born in Punjab, INDIA. He has received his M-Tech from PTU, Jalandhar and B-Tech from Amravati University. He has presented various papers in conferences and papers in various international journals. He has 12 years of experience of teaching and research. His research interests are embedded systems and VLSI interconnects. Presently he is working Asst. Prof. in ECE Deptt in Thapar University, Patiala.