International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

Analogy of Most Common Data Encryption Algorithms

Kinshuk Dudeja & Aishwarya Kharbanda
6th Semester, Electronics and Computer Science Department,
dudejakinshuk@gmail.com; aishwarya.kharbanda58@gmail.com

ABSTRACT:
This paper tries to present a fair comparison between the most common and used algorithms in the data encryption field. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. This paper provides a performance comparison between four of the most common encryption algorithms: DES, 3DES, Blowfish and AES.
The comparison has been conducted by running several encryption settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. Since our main concern here is the performance of these algorithms under different settings, the presented comparison takes into consideration the behavior and performance of the algorithm when different data loads are used.

Keywords:
Encryption Algorithms; Cryptography; AES; DES; Blowfish; Triple DES

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].

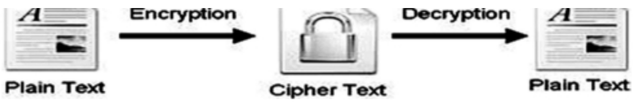


Fig.1: Encryption-Decryption Flow

II. DATA ENCRYPTION ALGORITHMS

DES: (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer.

DES became a standard in 1974. Since that time, many attacks and methods recorded that exploit weaknesses of DES, which made it an insecure block cipher.

3DES: As an enhancement of DES, the3DES (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods.

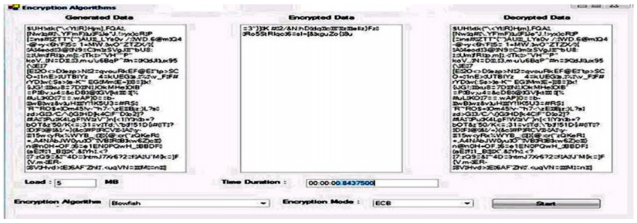
AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. It was originally called Rijndael(pronounced Rain Doll). It was selected in 1997 after a competition to select the best encryption standard. It has variable key length of 128, 192, or 256 bits; default 256. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devicesBrute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers.

Blowfish: It is one of the most common public domain encryption algorithms provided by Bruce Schneier – one of the world's leading cryptologists, and the president of Counterpane Systems, a consulting firm specializing in cryptography and computer security. It takes a variable length key, ranging from 32 bits to 448 bits; default 128 bits. Blowfish is unpatented, license-free, and is available free for all uses.

III. SIMULATION PROCEDURE

Here, our goal is to measure the Encryption and Decryption speed of each algorithm for different packet sizes. Encryption time is used to calculate the throughput of an encryption scheme. It indicates the speed of encryption. The throughput of the encryption

scheme is calculated by dividing the total plaintext in Megabytes encrypted on the total encryption time for each algorithm
in. As the throughput value is increased, the power consumption of this encryption technique is decreased. By considering different sizes of data blocks (0.5MB to 20MB) the algorithms were evaluated in terms of the time required to encrypt and decrypt the data block. All the implementations were exact to make sure that the results will be relatively fair and accurate.
The Simulation program (shown in Fig. 2) accepts three inputs: Algorithm, Cipher Mode and data block size.
After a successful execution, the data generated, encrypted and decrypted are shown. Another comparison is made after the successful encryption/decryption process to make sure that all the data are processed in the right way by comparing the generated data (the original data blocks) and the decrypted data block generated from the process.



Load : 5 MB

Time Duration : 00:00:00.8437500

Encryption Algorithm Blowfish

Encryption Mode : ECB

Fig. 2: GUI of the Simulation Program

IV. SIMULATION RESULTS

Simulation results for this compassion point are
shown Fig. 3 and Table 1 at encryption stage. The results show the superiority of Blowfish algorithm over other algorithms in terms of the processing time. It can also be noticed here; that 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics.

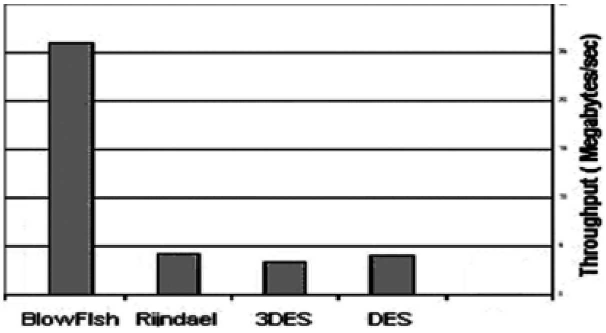


Fig. 3: Throughput of each encryption algorithm (Megabyte/Sec)

Input size in (Kbytes)	*AES*	*3DES*	*DES*	*Blow Fish*
49	56	54	29	36
59	38	48	33	36
100	90	81	49	37
247	112	111	47	45
321	164	167	82	45
694	210	226	144	46
899	258	299	240	64
963	208	283	250	66
5345.28	1237	1466	1296	122
7310.336	1366	1786	1695	107
Average Time	374	452	389	60.3
Through put (Mega-byt es/sec)	4.174	3.45	4.01	25.892

Table 1.
Comparative Execution Times (in Milliseconds) of Encryption Algorithms with Different Packet Size.

Simulation results for this compassion point are shown Fig. 4 and Table 2 decryption stage. We can find in decryption that Blowfish is the better than other algorithms in throughput and power consumption. Finally, Triple DES (3DES) still requires more time than DES.

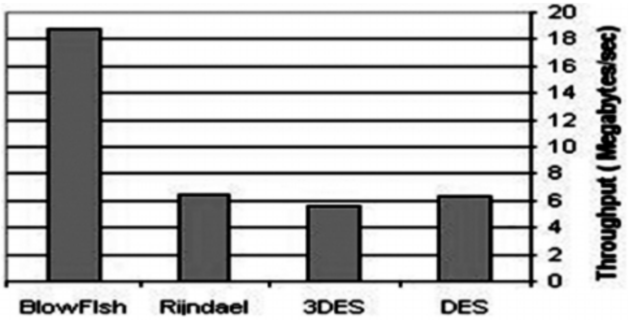
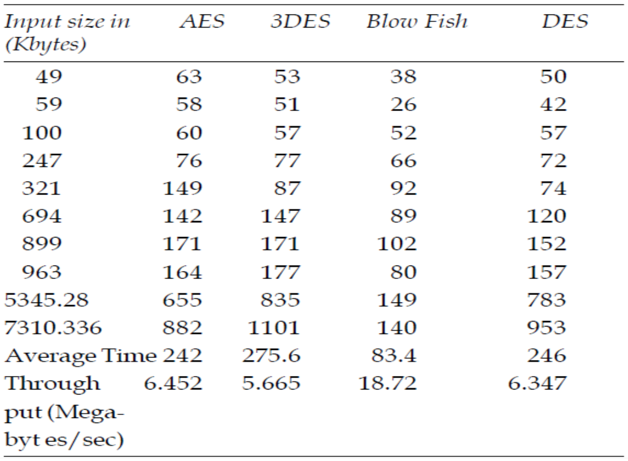


Fig. 4: Throughput of Each Decryption Algorithm (Megabyte/Sec)



Input size in (Kbytes)	*AES*	*3DES*	*Blow Fish*	*DES*
49	63	53	38	50
59	58	51	26	42
100	60	57	52	57
247	76	77	66	72
321	149	87	92	74
694	142	147	89	120
899	171	171	102	152
963	164	177	80	157
5345.28	655	835	149	783
7310.336	882	1101	140	953
Average Time	242	275.6	83.4	246
Through put (Mega-byt es/sec)	6.452	5.665	18.72	6.347

Table 2.
Comparative Execution Times (in Milliseconds) of Decryption Algorithms with Different Packet Size

5. CONCLUSION

The simulation results showed that Blowfish has better performance than other commonly used encryptionalgorithms. Since Blowfish has not any known security weak points so far, it can be considered as an excellent standard encryption algorithm. AES showed poor performance results compared to other algorithms, since it requires more processing power.

6. REFERENCES

[1] Aamer Nadeem, "A Performance Comparison of Data Encryption Algo". IEEE 2005.

[2] "Wireless Security Handbook", Auerbach Publications 2005.

[3] Bruce Schneier, "Applied Cryptography", *John Wiley and Sons*, Inc 1996.

[4] Ferguson, N., Schneier, B., and Kohno T., (2010). "Cryptography Engineering: Design Principles and Practical Applications". New York : John Wiley and Sons.

[5] Electronic Frontier Foundation. (1998). Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design. Sebastopol, CA: O'Reilly and Associates.

[6] F.I.P. Standard, Advanced Encryption Standard (AES), National Institute of Standards and Technology (NIST), 2001.

[7] Bruce Schneier. "The Blowfish Encryption Algorithm Retrieved", October 25, 2008.

[8] A.A. Tamimi, '"Performance Analysis of Data Encryption Algorithms". Retrieved October 1, 2008.

[9] W. Stallings, "Cryptography and Network Security", *Prentice Hall*, 4th Ed., 2005.