Peformance Analysis Of Data Encryption Algorithms

O P Verma, Ritu Agarwal, Dhiraj Dafouti, Shobha Tyagi
Information Technology
Delhi Technological University,
New Delhi, India
e-mail: opverma@dce.ac.in, ritu.jeea@gmail.com, ddafouti100@gmail.com, shobhadtu@ieee.org

Abstract—**The principal goal guiding the design of any encryption algorithm must be security against unauthorized attacks. However, for all practical applications, performance and speed are also important concerns. These are the two main characteristics that differentiate one encryption algorithm from another. This paper provides the performance comparison between four of the most commonly used encryption algorithms: DES(Data Encryption Standard), 3DES(Triple DES), BLOWFISH and AES (Rijndael).The comparison has been conducted by running several setting to process different sizes of data blocks to evaluate the algorithms encryption and decryption speed. Based on the performance analysis of these algorithms under different hardware and software platform, it has been concluded that the Blowfish is the best performing algorithm among the algorithms under the security against unauthorized attack and the speed is taken into consideration.**

Keywords-Encryption Algorithms, Performance Analysis, AES, DES, Blowfish, Triple DES, Cryptography.

I. INTRODUCTION

As the importance and the value of exchanged data over the internet or other media types are increasing, the search for the best solution to offer the necessary protection against the data thieves' attacks along with providing the services under timely manner is one of the most active subjects in the security related communities.

This paper tries to present a fair comparison between the most common and used algorithms in the data encryption field. Since our main concern here is the performance and speed of these algorithms under different settings, the presented comparison takes into consideration the behavior and the performance of the algorithm when different data loads are used. Section 2 will give an overview of the cryptography and its usages in daily life; in addition to that it will explain some of the most used terms in cryptography. Section 3 gives the background to understand the key difference between the compared algorithms we have chosen. Section 4 will show the performance results of algorithms under different settings. Section 5 will walk through the conclusion of the paper and the relatively the advantages of the Blowfish algorithm and the further scope. 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. Different Hardware and Software platforms are taken and the like languages C# and the Java, showing the capability of the different algorithms. The results are presented in the two modes such as the Block Cipher mode and the Stream Cipher modes.

II. CRYPTOGRAPHY: OVERVIEW

An overview of the main goals behind using cryptography will be discussed in this section along with the common term used in this field.

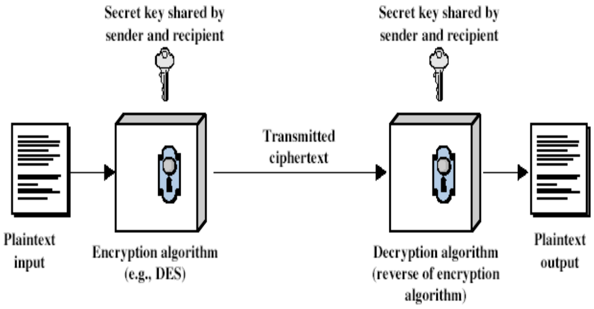
Secret key shared by sender and recipient
Secret key shared by sender and recipient
Transmitted ciphertext
Plaintext input
Encryption algorithm (e.g., DES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

Figure 1. Encrption / Decryption

Cryptography is usually referred to as "the study of secret", while nowadays is most attached to the definition of encryption. Encryption is the process of converting plain text "unhidded" to a cryptic text "hidded" 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 in figure 1.

A. Cryptography Goals

This section explains the six main goals behind using Cryptography. Every security system must provide a bundle of security function that can assure the secrecy of the system. These functions are usually referred to as the security system.

1. CONFIDENTIALLY- Information in computer transmitted information is accessible only for reading by authorized parties.
2. AUTHENTICATION- Origin of message is correctly identified with an assurance that identity is not false.
3. INTERGRITY- Only authorized parties are able to modify transmitted or stored information.
4. NON REPUDIATION- Requires that neither the sender, nor the receiver of message be able to deny the transmission.

978-1-4244-8679-3/11/$26.00 ©2011 IEEE

5. ACCESS CONTROL- Requires access may be controlled by or for the target system.
6. AVAILIBILITY- Computer system assets are available to authorized parties when needed.

B. Block Cipher and Stream Cipher

One of the main categorization methods for encryption technique commonly used is based on the form of input data they operate on. The two types are Stream and Block Cipher. The definition of the cipher presented. “A Cipher is an algorithm for performing encryption (reverse decryption).

Block Cipher- In this method data is encrypted and decrypted if data is in form of blocks. In its simplest mode, you divide the plain text into blocks which are fed into the cipher system to produce blocks of cipher text. ECB (Electronic Codebook Mode) is the basic form of block cipher where data blocks are encrypted directly to generate its corresponding cipher blocks.

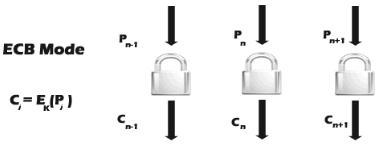

Figure 2. BLOCKS CIPHER (ECB MODE)

Stream Cipher- Stream cipher functions on a stream of data by operating on it by bits. Stream cipher consists of two major components: a key stream generator, and a mixing function. Mixing function is usually just an XOR function, while key stream generator is the main unit in stream cipher encryption technique. For example, if the key stream generator produces series of zeroes, the outputted ciphered stream will be identical to the original plain text.

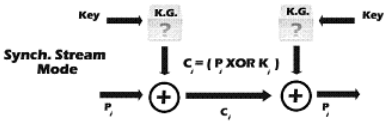

Figure 3. STREAM CIPHER (SIMPLE MODE)

C. Mode of operation

There are many variance of cipher, where different techniques are used to strengthen the security of the system. The most common methods are ECB(Electronic Code book).CBC(Chain Block Chaining mode)and OFB(Output Feedback mode).There are many other modes like CTR(Counter mode). CFB(Cipher feedback mode) or 3 DES. In this paper the main concentration will be on ECB and CFB.

III. INTRODUCTION TO ALGORITHMS

The following Secret key algorithms were chosen for the survey.

DES- Data Encryption Standard DES[1] is a block cipher (a form of secret key encryption that was selected by the National Bureaus of Standard as an official Federal Information Processing Standard (FIPS) for United States in 1976 and which has subsequently enjoyed widespread use internationally. It is based on symmetric key algorithm that uses a 56 bit key. The algorithm was initially controversial with classified design elements, a relatively short key length. Many attacks and methods recorded that exploit the weakness of DES, which made it insecure block cipher.

TRIPLE DES- As an enhancement of DES[2] , the 3DES(Triple DES) encryption standard was proposed based on the existing DES , and was standard in ANSI X9.17 and ISO 8732 and in PEM for key management .The 3DES algorithm uses either two or three 56 bit key. Thus the effective key length is up to 168 bits. But it was fact that 3DES is slower than the other block cipher method.

AES (Advanced Encryption Standard)- AES[3][4][5] is the new encryption recommended by NIST to replace DES. Rijndael(pronounced Rain Doll) algorithm was selected in 1997 after a competition to select the best encryption standard .Brute Force attack is only effective attack known against it, in which attacker tries to test all characters combinations to unlock the encryption. The AES candidates are the latest generation block cipher, and have a significant increase in the block size from the old standard of 64 bits up to 128 bits; and key from 128 to 256 bits. It is an iterative rather than a Fiesta cipher (like IDEA).

BLOWFISH-Blowfish[6][7][8][9][10] is a keyed symmetric block cipher designed in 1993 by Bruce Schneier and included a large number of cipher suites and encryption products. Blowfish provides a good encryption rate in software and no effective crypt analyzing it has been found till date. Blowfish has a 64 bit block size and variable key length from 32 up to 448 bits.It is a 16 round Fiestel cipher and uses a large key dependent S-boxes. This algorithm can be optimized in hardware application though it is mostly used in software. It is best among other block cipher.

IV. PERFORMANCE RESULTS

To give more prospective about the performance of the compared algorithms, this section discusses the results. All were coded in C++, compiled with Microsoft Visual C++[11] .NET 2003(whole program optimization, optimize for speed, P-4 code generation), and ran on a Pentium- 4 , 2.1 GHz processor under Windows XP SP1.386 assembly routines were used for multiple precision addition and subtraction SSE2 intrinsic were used for multiple precision multiplication . The algorithm setting for the performance comparisons is shown in Table I.

TABLE I. ALGORITHM SETTINGS

Algorithm	Key Size (Bits)	Block Size (Bits)
DES	**64**	**64**

3DES	192	64
Rijndael	256	128
Blowfish	448	64

TABLE II. COMPARISON RESULTS USING CRYPTO++

Algorithm	Megabytes(2^20 bytes) Processed	Time Taken	MB/Second
Blowfish	256	3.976	64.386
Rijndael (128-bit key)	256	4.196	61.010
Rijndael (192-bit key)	256	4.817	53.145
Rijndael (256-bit key)	256	5.308	48.229
Rijndael (128) CTR	256	4.436	57.710
Rijndael (128) OFB	256	4.837	52.925
Rijndael (128) CFB	256	5.378	47.601
Rijndael (128) CBC	256	4.617	55.447
DES	128	5.998	21.340
(3DES)DES-XEX3	128	6.159	20.783
(3DES)DES-EDE3	64	6.499	9.848

This section also describes the simulation environment and the used system components. As mentioned this simulation uses the provided classes in the .NET[12][16] environment to simulate the performance of DES, 3DES and AES (Rijndael).This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithms.. Long key length means more effort must be put forwarded to break the encrypted data security.

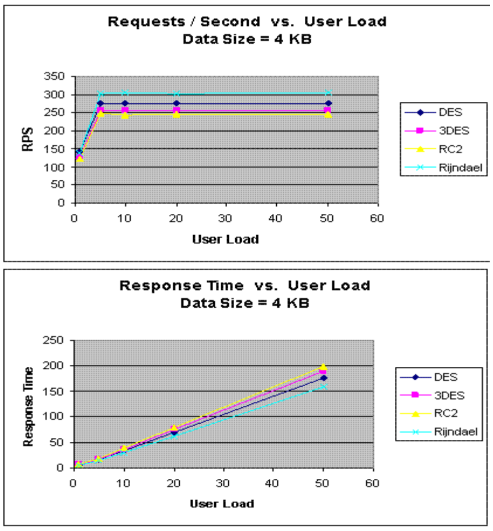

Figure 4. Comparision results using .NET Implementation

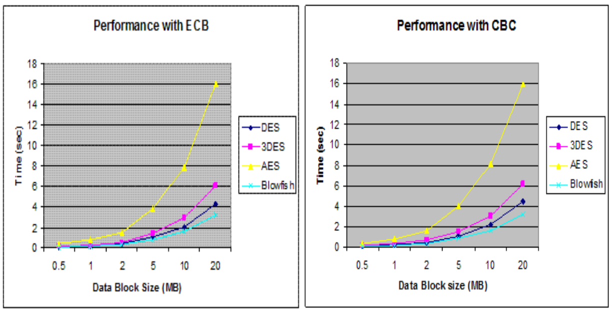

Figure 5. Performance Results with CBC and ECB Mode

The first set of experiment were conducted using ECB mode, the result are shown in figure 5. The results show the superiority of Blowfish algorithm over other algorithm in terms of the processing time. It shows also that AES consumes more resources when the data block size is relatively big. The results shown here are different from the results obtained as discussed in the figure 4 under .NET implementation. Since the data blocks used here are much larger. Another point can be noticed there that 3DES require always more time than DES, because of its triple phase encryption characteristics. Blowfish, although it has a long key (448 bit), outperformed other encryption algorithm .DES and 3DES are known to have worm holes in their security mechanism. Blowfish and AES on the other hand, do not have any so far.

As expected CBC requires more processing time than ECB because of its key chaining nature. The result shown in figure 5 indicates also that the extra time added is not significant for many applications, knowing that CBC is much better than ECB in terms of protection. The difference between the two modes is hard to see by naked eye, the results showed that the Average difference between ECB and CBC is 0.059896 second which is relatively small.

A. *Performance Result For Block Cipher*

The execution results of secret key algorithm in ECB (electronic code book) modes are presented first. These results are shown in Table III and IV, for execution of code on a P-II 266 MHz machine and P-4 2.4 GHZ machine respectively. The algorithms are implemented in a uniform language (java), using their standard specification. An obvious way to compare the performance of these algorithms is to take average of execution times for each algorithm.

TABLE III. COMPARATIVE EXECUTION TIMES (IN SECONDS) OF ENCRYPTION ALGORITHMS IN ECB MODE ON A P-II 266 MHZ MACHINE

Input Size (bytes)	DES	3DES	AES	BF
20,527	2	7	4	2
36,002	4	13	6	3

45,911	5	17	8	4
59,852	7	23	11	6
69,545	9	26	13	7
137,325	17	51	26	14
158,959	20	60	30	16
166,364	21	62	31	17
191,383	24	72	36	19
232,398	30	87	44	24
Average Time	14	42	21	11
Bytes/sec	7,988	2,663	5,320	10176

B. Performance Results of Stream Cipher

In this section[13][14], the results of execution of the secret key algorithm in the CFB mode are presented. This section, the results of execution of the secret key algorithm in CFB mode are presented. Table IV and Table V give execution times of these algorithms on Pentium –II 266MHZ, and Pentium-4, 2.4 GHZ platform respectively.

As with block cipher, the performance of a stream cipher also varies with the block size and the key size, but the effect of a larger block size is reversed. The larger block size , the slower will be the algorithm ,because with a larger block size , the algorithm will have to do more work for the same amount of input data(a bit or a byte) in a single execution cycle of the algorithm. With a smaller block size, the same size of the input data would be encrypted more efficiently, thus decreasing the overall encryption time other thing being equal. The effect of a larger key in a stream cipher is the same in the block cipher, i.e. it slows down the encryption, because in general, all bits of the key are involved in an execution cycle of the algorithm. With a smaller key, a lower number of key bits are involved, thus reducing the time to complete one execution cycle.

TABLE IV. COMPARATIVE EXECUTION TIMES (IN SECONDS) OF ENCRYPTION ALGORITHMS IN ECB MODE ON A P-4 2.4 GHZ MACHINE

Input Size (bytes)	DES	3DES	AES	BF
20,527	24	72	39	19
36,002	48	123	74	35
45,911	57	158	94	46
59,852	74	202	125	58
69,545	83	243	143	67
137,325	160	461	285	136
158,959	190	543	324	158
166,364	198	569	355	162
191,383	227	655	378	176
232,398	276	799	460	219
Average Time	134	383	228	108
Bytes/sec	835	292	491	1,036

From the result shows that Blowfish [15][16][17] has a very good performance compared to other algorithm. Also it showed that AES has a better performance than 3DES and DES. Amazingly it shows also that 3 DES has almost 1/3 through put of DES, or in other words it needs 3 times than 3DES to process the same amount of data.

It has also done experimentally for comparing the performance of the different encryption algorithm inside .NET Framework. Their result are closer as shown in the above discussion .The result shows that AES outperformed other algorithm in both the number of requests processed per second in different user loads, and in the response time in different user load situation.

Using this criterion it is apparent from Table III, IV, V and VI that four symmetric key algorithm are in the following order, as regards to their performance

1. BLOWFISH (FASTEST)
2. DES or 3DES
3. AES
4. TRIPLE DES (SLOWEST)

TABLE V. COMPARATIVE EXECUTION TIMES OF SECRET KEY ALGORITHMS IN CFB MODE ON A PENTIUM-IL 266 MHZ

Input Size (bytes)	DES	3DES	AES	BF
20,527	17	56	62	18
36,002	30	99	94	23
45,911	41	130	125	33
59,852	52	181	174	46
69,545	69	201	200	53
137,325	129	401	409	104
158,959	151	472	473	122
166,364	159	488	489	130
191,383	185	568	567	148
232,398	229	681	687	184
Average Time	106	328	328	86
Bytes/sec	1055	341	341	1300

TABLE VI. COMPARATIVE EXECUTION TIMES (IN SECONDS) OF ENCRYPTION ALGORITHMS IN CFB MODE ON A P-4 2.4 GHZ MACHINE

Input Size (bytes)	DES	3DES	AES	BF
20,527	188	498	596	141
36,002	362	934	1123	271
45,911	431	1174	1484	352
59,852	570	1532	1932	433
69,545	629	1894	2251	518

137,325	**1203**	**3622**	**4419**	**992**
158,959	**1405**	**4240**	**5044**	**1175**
166,364	**1511**	**4424**	**5501**	**1216**
191,383	**1714**	**5128**	**5923**	**1369**
232,398	**2139**	**6238**	**7231**	**1649**
Average Time	**1015**	**2969**	**3551**	**812**
Bytes/sec	**110**	**38**	**31**	**138**

V. CONCLUSION AND FUTURE WORK

This paper presented the fair comparisons among the four commonly used algorithms and the simulated results showed the capability of each of the algorithms. Through the presented results under different hardware setting and using different languages, it has being concluded that the Blowfish is the best performing algorithm under the speed and the security was taken into the consideration. Blowfish is not only the fastest but also provides the great security through the strong key size which enables it to be used in many applications like Bulk Encryption, Random Bit Generation , Internet Based Security (network security) , Packet Encryption and so many of applications. Though having so many advantages and application it is still suffered from the Weak Key problem which yet to be rectified and explored.

REFERENCES

[1] National Bureau of Standards – Data Encryption Standard, FIPS Publication 46, 1977.

[2] National Bureau of Standards – 3-Data Encryption Standard ,FIPS Publication 46, 1977.

[3] NIST,"Advanced Encryption Standard Call", NIST,1997. http://www.nist.gov/aes/

[4] NIST Advanced Encryption Standard (AES) Development Effort web site. http://csrs.nist.gov/encryption/aes/aes-home.html

[5] Daemen, J., Rijmen, V:: "AES Proposal: Rijndael", "Banksys /Katholieke Universiteit Leuven", Belgium, submission, Jun 1998.

[6] Schneier, B.: "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings(Dec. 1993), Lecture Notes in Computer Science(LNCS) Springler verlag Vol. 809, pp. 191-204, 1993, ISBN 3- 540-58108-1.

[7] Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall,,and Ferguson ,N.:"Performance Comparison of the AES Submissions", Counterpane Systems, Dec 1998. http://www.counterpane.com/AESperformance.html

[8] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", *Fast Software* Encryption, Cambridge Security Workshop proceedings *December 1993*, Springer-Verlag, 1994, pp. 191-204 .

[9] B.Schneier, Applied Cryptography: Protocols,Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons, 1995.

[10] W. Stallings, Cryptography and Network Security:Principles and Practices, 2nd ed., Prentice Hall, 1999.

[11] .Net Media Framework:http://dotnet.com/products/dot-media/jmf

[12] Crypto++ libraries in dot net 2003, http://dotnet.com/products/dot-media/crypto++

[13] Java Media Framework (JMF): http://java.sun.com/products/java-media/jmf

[14] Schulzrinne, H, Casner, S., Frederick, R., Jacobson, V. (Audio-video Transport working group) "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, January, 1996.

[15] Schneier B. "Description of a New Variable-length Key 64- Bit Block Cipher (*Blowfish*).", *Cambridge Security* Workshop Proceedings Springer-Verlag, 1994

[16] Cryptix: open-source cryptographic software libraries: http://www.cryptix.org/

[17] McCanne, S., and Jacobson, V. "VIC: A Flexible Framework for Packet Video". ACM Multimedia 95 –Electronic Proceedings November 5-9, 1995 San.

[18] Blowfish open source code: http://www.counterpane.com/blowfish-download.html