Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 72 (2014) 25218-25219

ISSN: 2229-712X

A comparative study of AES, Blowfish, Two fish and serpent cryptography algorithms

Debasish Roy, Saptarshi Paul and Sanju Das
Computer Science Department, Assam University, Silchar, India.

ARTICLE INFO

Article history:
Received: 25 February 2014;
Received in revised form:
19 June 2014;
Accepted: 29 June 2014;

Keywords
Encryption Algorithm,
Performance Analysis,
AES,
Blowfish,
Twofish,
Serpent,
Cryptography.

ABSTRACT
This paper provides a performance comparison between four of the most common symmetric key cryptography algorithms: AES(Rijndael), Blowfish, Twofish and Serpent. The comparison has been conducted by running four encryption algorithms to process different sizes of data blocks with any extension of files to evaluate the algorithm's encryption/decryption speed. Simulation has been conducted using java language

Introduction

This paper tries to present a fair comparison between the four most commonly used symmetric key cryptography algorithms in the data encryption field. Since our main concern here is the performance of these algorithms for different sizes of data blocks with different bytes of files, the presented paper takes into consideration the performance of the algorithms when different data blocks are used with different file extensions.

Table 1: Theoretical Comparison of AES,Blowfish, Twofish and Serpent

FACTORS	AES	Blowfish	Twofish	Serpent
Key Length	128, 192, or 256 bits	1 bit up to 448 bits	128, 192 or 256 bits	128, 192 or 256 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block Size	128, 192, or 256 bits	64-bit block size	Block size of 128 bits	Block size of 128 bits
published	1998	1993	1998	1998
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and Square attacks	granted natural protection against brute-force attacks, weak against differential	Truncated differential cryptanalysis, Impossible differential attack	Strong against differential cryptanalysis attacks
Security	Considered secure	weak as it suffers from weak key problem	Higher Security margin	Higher Security margin
Possible Keys	2^{128}, 2^{192}or 2^{256}	1-2^{448}	1-2^{256}	2^{128}, 2^{192}, or 2^{256}
Structure	Substitution-permutation network	Feistel network	Feistel network	Substitution-permutation network
Rounds	10, 12 or 14	16	16	32
Derived from	Square	Square	Blowfish, SAFER, Square	Square

Table 2: Encryption time (in milliseconds) for various file sizes (in kb) and bytes

File Name	File Size (in kb)	AES (128bit key)	Blowfish (128bit key)	Twofish (128bit key)	Serpent (128bit key)
GATE.ppt	199	32	62	234	454
BSNL.jpg	406	34	78	375	594
Digital.doc	1117	78	172	922	1203
Prog.pdf	2247	125	250	1765	2000
Book1.xlsx	2698	157	281	2110	2281
Aptitude.pdf	4464	234	469	3359	3610
Jai ho.mp3	4994	265	453	3750	4015
No promise.3gp	6231	312	531	4734	4875
3_Idiot.mp4	8381	422	656	6219	6531
Simple.txt	18381	875	1594	13640	14110
Total Average Time(in milliseconds)		253.4	454.6	3710.8	3967.3

Encryption is the process of converting ordinary information (plaintext) into unintelligible cipher text. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext.

Comparative Analysis

The following table summarizes the comparison of *AES, Blowfish, Twofish and Serpent* Encryption algorithms with some key factors:

Tele:
E-mail addresses: sanjudasp@gmail.com

Comparative Analysis for encryption and decryption time as performance metrics:

Encryption time for various file sizes and types:

The simulation was done on Intel Pentium 4 CPU 3.06 GHz, 512MB of RAM, OS-Windows XP SP-2. Encryption was done on files of varying types and sizes, for which the following facts were observed:

Decryption time for various file sizes and types:

Decryption was done on the same environment on the Encrypted files and the following facts were observed:

Table 3 : Decryption time (in milliseconds) for various files

File Name	File Size (in kb)	AES (128bit key)	Blowfish (128bit key)	Twofish (128bit key)	Serpent (128bit key)
GATE.ppt	199	63	484	1828	2063
BSNL.jpg	406	67	500	1937	2171
Digital.doc	1117	125	672	2375	2609
Prog.pdf	2247	172	718	3078	3312
Book1.xlsx	2698	203	750	3328	3578
Aptitude.pdf	4464	391	937	4375	4687
Jai ho.mp3	4994	343	938	4734	5000
No promise.3gp	6231	406	1140	5500	5734
3_Idiot.mp4	8381	531	1171	6750	7125
Simple.txt	18381	1406	1875	12922	13172
Total Average Time(in milliseconds)		370.7	918.5	4682.7	4945.1

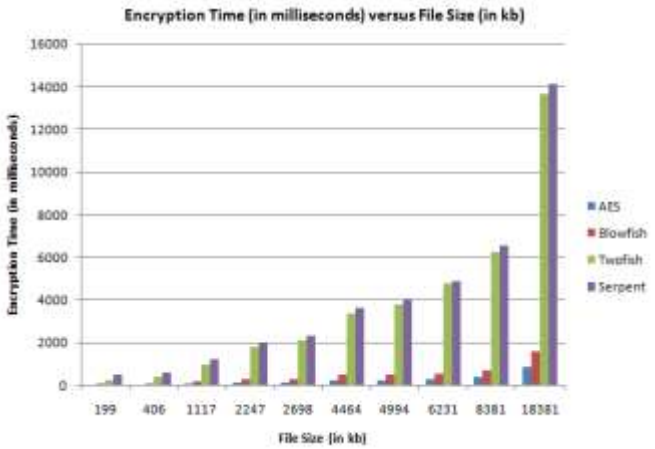

Fig 1: Encryption Time

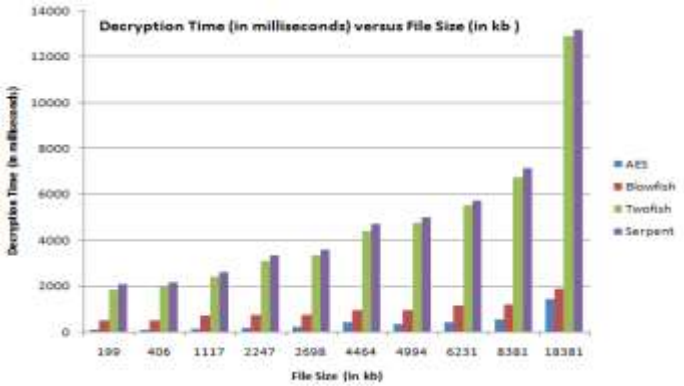

Fig 2: Decryption Time

Conclusion

It has been observed that for 128 bit key size AES is much faster than Serpent. But the Encryption and Decryption time will vary in certain environment (i.e. it depends on the processor) and the amount of data needed to be Encrypt/Decrypt. In very high speed processor the Encryption and Decryption time will be less than that of the slower one. It also depends on the Programming language used for implementation.

The presented simulation result shows that AES has better performance in Encryption/Decryption time than other algorithms used, it is a very secure encryption algorithms because it has a strong key. Blowfish shows poor performance result compared to AES since it requires more processing power but Blowfish has a better performance than Serpent and Twofish. Unfortunately Blowfish suffers the same problem as DES. The security guaranteed by the Blowfish algorithm is weak because it suffers from weak key problem. Compared to AES Serpent and Twofish is not suitable because of its high Encryption/decryption time taken, but in some condition where the security is more important rather than Encryption/Decryption time, in that case Serpent is more secure than other Encryption algorithms.

References:

[1.] CRYPTOGRAPHIC STANDARDS AND GUIDELINES: A STATUS REPORT, By Elaine Barker, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

[2] PERFORMANCE ANALYSIS OF DATA ENCRYPTION ALGORITHMS, By Abdul Karim Al Tamimi, aa7@wustl.edu

[3] AES Proposal: Rinjndael ,By John Daeman ,Vincent Rijmen.

[4] The Internet Protocol Journal - Volume 4, Number 2Goodbye DES, Welcome AES, By Edgar Danielyan.

[5] Atul Kahate ,Cryptography and Network Security ,Tata Mc Graw Hill ,2008

[6] William Stallings ,Cryptography and Network Security : principles and practice, 4th edition Prentice Hall ,2006

[7]Herbert Schildt, Java: The Complete Reference,Mc Graw Hill ,Seventh edition , 2009

[8.]www.encryptionanddecryption.com/encryption/symmetric_encryption.html

[9]www.topbits.com/symmetric-and-asymmetric-ciphers.html

[10]http://paper.ijcsns.org/07_book/201001/20100139.pdf

[11]www.ibm.com/developerworks/library/s-crypt02.html

[12]*www.schneier.com/paper-aes-performance.pdf*

[13]http://www.schneier.com/blowfish.html

[14]http://pocketbrief.net/related/BlowfishEncryption.pdf

[15]www.schneier.com/paper-twofish-paper.pdf

[16]csrc.nist.gov/archive/aes/round1/conf1/twofish-slides.pdf

[17]www.schneier.com/paper-serpent-aes.ps.gz