Performance Analysis of AES and TwoFish Encryption Schemes

Dr. S.A.M Rizvi , Associate Professor,Department of Computer Science, Jamia Millia Islamia,New Delhi, samsam_rizvi@yahoo.com

Dr. Syed Zeeshan Hussain, Assistant Professor, Deptt. of Computer Science, Jamia Millia Islamia, New Delhi, szhussain@rediffmail.com

Neeta Wadhwa, Research Scholar, Deptt. of Computer Science, Jamia Millia Islamia, New Delhi, neeta.088@gmail.com

***Abstract*- The two main characteristics of a good encryption algorithm are: Security and Speed. Usually security algorithms have to be embedded in a variety of applications like e-banking, online shopping, mails etc. So they should be fast as well as secure in different environments. In this paper, we do security v/s performance analysis of two algorithms Twofish and AES. First, we will discuss security issues of both algorithms by considering their safety factor. Then we study encryption speed of both algorithms by encrypting different type of data (text, image, audio) and analyze their performance in terms of throughput of every algorithm on different size of RAMs. The results show the relationship between performance of algorithms and size of RAM and type of data.**

Keywords: Twofish, AES, Encryption Schemes.

I. Introduction

From mails to money when everything is getting digital, Internet becomes the one and main medium of communications in all aspects of our life. Meanwhile sniffing, intrusion, denial of service like threats to information are also increasing day by day. Thus encryption becomes the necessity of the hour.

Encryption means the art and science of secret writing. It stores and transmits the information safely over the insecure medium like Internet by encoding plain text into cipher text with the the help of various encryption algorithms. The encryption algorithms are generally categorized into two popular types: Symmetric key encryption and Asymmetric key encryption. In Symmetric key encryption, same key is used to encrypt and decrypt data. The key has to be shared before transmission to sender and receiver. Length of Key has an important place in Symmetric key encryption. For the same algorithm, encryption using longer key is hard to cryptanalyze means more secure as compared to the one using shorter key. The main Symmetric key cryptography algorithms include 3DES, RC5, Blowfish, Towfish, Cast, AES. In Asymmetric key encryption, a key-pair, private key and public key are used. Public key is used for encryption and private key is used for decryption like RSA[1]. In any secure communication system, Symmetric Encryption Schemes perform the real part of encrypting data as they are very fast and Asymmetric Encryption Schemes take the responsibility of distributing keys.

When DES(Data Encryption Standard) got cracked, there was a need of a new strong Encryption Standard, NIST announced the Advanced Encryption Standard (AES) program in 1997. NIST's call requested a block cipher with the specified criteria: a longer key length, larger block size, faster speed, and greater flexibility respect to the previous standard DES. Twofish and Rijndael are two algorithms out of 5, selected as finalists of the competition in second round, **TwoFish** has been designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner and **Rijndael** by J. Daemen & V. Rijmen. Rijndael won the competition and became the Advanced Encryption Standard (AES). Both the algorithms perform on a wide range of hardware from smart card microprocessor to large microprocessors.

The rest of the paper is organized as : section II gives the brief review of the two algorithms and discuss their security issues; section III outlines the related work ; section IV describes the implementation details ; section V shows the simulation results; finally, the conclusions and future work is followed in section VI .

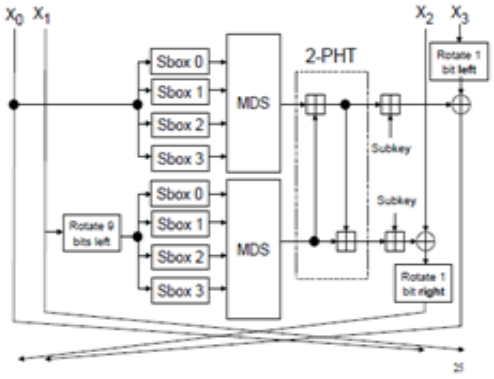
978-0-7695-4437-3/11 $26.00 © 2011 IEEE
DOI 10.1109/CSNT.2011.160

II. Overview of two algorithms

A. TwoFish

Twofish is an algorithm from Counterpane Internet Security, it is highly suited for large microprocessors and also for smart card microprocessors. A brief overview of the concepts and considerations relevant to the Twofish design procedure is given in [2].

Fig 1 :Twofish Encryption Scheme

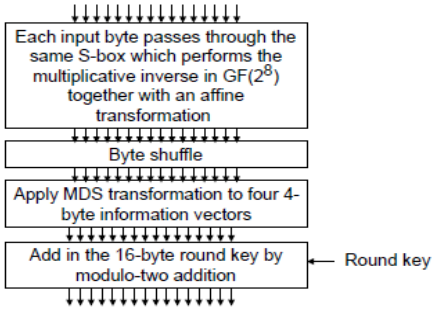


Currently the best attacks on Twofish use different versions of differential cryptanalysis, None of them succeeds on the full number of rounds with the present computational power.

B. AES

AES has Non-Feistel structure, based on a sophisticated mathematical design. It's simple structure attracts cryptographers and cryptanalysts. It encrypts 128 bit block size with 128/192/256 bit key for 10/12/14 rounds.

FIG 2 : AES Encryption Scheme



The complete specification and the above structure of AES encryption scheme is given in [3].

Eli Biham in [4] compared the AES candidates by calculating the "minimal secure rounds" .On the basis of this, he defined a measure of security called ' Safety Factor' .

The safety factor **σ ,** is defined as **σ** = *n/b*.

Where n : number of rounds of the full cipher,

b *:* be the largest number of rounds that has been broken.

A broken cipher has a safety factor of 1. A safety factor of 2 means a cipher for which a version with half the rounds has been broken.

AES	1.11/1.33/1.56
Twofish	2.67
18-round AES	2.00
24-round AES	2.67

Lars Knudsen also compared the AES candidates in [5] by using this factor as a measure of security.AES has a safety factor less than 2, it implies that it is somewhat more delicate for the advancements of cryptanalysis. To make the safety factor of AES equivalent to Twofish would require 24 rounds of AES. An increase in the number of rounds may reduce its performance.

III. Related Work

A research of [6] was performed for different common secret key algorithms including DES, 3DES, AES, and Blowfish in two different modes ECB(Electronic Codebook) and CFB(Cipher Feedback). Their performance was compared by encrypting input files of varying contents and sizes. They concluded that Blowfish is the fastest encryption algorithm. It also showed that AES is better than 3DES and DES. Also, it confirms that DES is 3 times faster than 3DES.

Krishnamurthy in [7] demonstrated the energy consumption of different common symmetric key encryptions on hand-held devices.

Diaa in [8] evaluated several symmetric encryption algorithms such as AES, DES, 3DES, RC6, Blowfish and RC2.They concluded: there is no significant difference when the results are displayed either in hexadecimal base encoding or

in base 64 encoding; Blowfish has better performance than other common encryption algorithms used, followed by RC6; In the case of changing data type such as image, RC2, RC6 and Blowfish become slower; Higher key size leads to significant change in the battery and time consumption.

The study in [9] proves that AES is faster and more efficient than others. Hirani showed in his experiment that reducing the number of rounds leads to power savings but it makes the algorithm prone to cryptanalysis so should be avoided. Seven or more rounds can be considered fairly secure and could be used to save energy in some cases.

Most of above parallel research focused on the analysis of encryption algorithms for different parameters like encryption speed and battery consumption , encryption/decryption time for varying key lengths, for different modes. In this paper we are analyzing Twofish and AES for text, image and audio encryption on different size of RAM, and derive the correlation between these parameters : encryption speed for different types of plaintext and size of RAM.

IV. Experimental Design

For our experiment, we use two PCs

1. Intel Pentium® Dual Core 2.50GHz CPU with 2GB and 4GB RAM (DDR2 DRAM frequency 399.0MHz) .
2. Intel Pentium® Dual Core 2.50GHz CPU with 1GB RAM (DDR2 DRAM frequency 399.0MHz).

We implemented the algorithms according to their standard specifications in .Net environment using C#, on Windows XP OS. In the experiment we encrypt the pdf and text files of different size ranges between 100KB to 13 MB, the images ranges 10-200KB,the audio files ranges 3-4.5 MB on 1GB, 2GB,4GB RAM and calculate their mean encryption time.

A. Text Encryption

Table 1: Encryption time(in milliseconds) of Twofish & AES

	1GB RAM		2 GB RAM		4 GB RAM	
PlainText size in Mbytes	TwoFish	AES	TwoFish	AES	TwoFish	AES
1.31	109	120	89	118	76	117
1.52	172	183	152	182	134	179
2.03	204	222	194	219	174	218
2.79	232	245	202	243	187	241
3.01	282	301	252	299	242	298
7.13	532	539	492	537	465	535
13.50	756	764	686	761	665	759
Average time	2487	2374	2067	2359	1953	2347
Execution speed (MegaBytes/sec)	12.58	13.1803	15.18	13.264	16.046	13.33

B. Image Encryption

Table 2. Encryption time(in milliseconds) of Twofish & AES

	1GB RAM		2 GB RAM		4 GB RAM	
Image size(KB)	TwoFish	AES	TwoFish	AES	TwoFish	AES
19.4	93	89	87	84	79	80
23.4	110	98	100	93	89	90
52.9	171	165	164	159	156	152
114	324	302	311	298	299	296
170	363	323	352	319	320	317
193	377	345	363	338	339	334
Average time	239	220	229	215	214	211
Execution speed(KiloBytes/sec	3.98	4.33	4.16	4.43	4.46	4.51

C. Audio Encryption

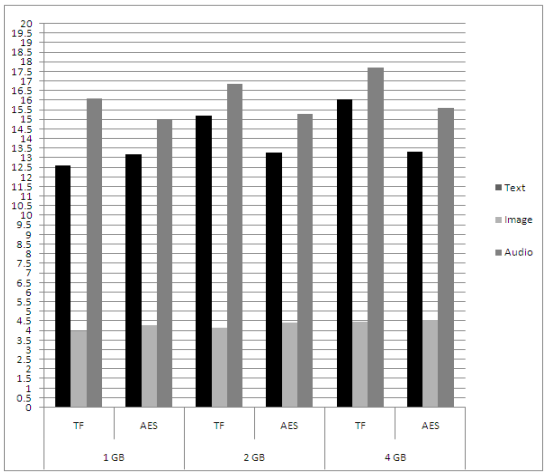
Table 3. Encryption time(in ms) of Twofish & AES

	1GB RAM		2 GB RAM		4 GB RAM	
Audio file size (KB)	TwoFish	AES	TwoFish	AES	TwoFish	AES
3723	178	194	165	191	153	189
3920	183	201	179	198	167	195
4089	234	256	229	251	218	247
4150	249	266	238	260	224	257
4685	327	341	311	335	297	328
5222	396	419	372	401	359	394
Average time	261	279	249	274	236	268
Execution speed(KiloBytes/sec)	16.07	15.0	16.856	15.3	17.7	15.6

V. Simulation Results

The following graph based on the data collected illustrates how the Encryption Speed varies with the RAM size for AES and TwoFish Algorithms:

Fig 3: Graph between Encryption Speed and RAM Size of AES and TwoFish(TF) for Text , Image and Audio Files



On the basis of data collected , we calculated the correlation Coefficient between encryption speed and system's RAM for every type of data as :

Let Encryption Speed (X) and System's RAM (Y):

Then Correlation r_{xy} predicts how encryption speed varies with the change in size of RAM.

Correlation coefficient r_{xy}	**Twofish**	**AES**
r_{xy} (Text Encryption)	**0.95**	**0.78**
r_{xy}(Image Encryption)	**0.89**	**0.62**
r_{xy}(Audio Encryption)	**0.98**	**0.54**

VI. Conclusion

In this paper, we analyzed two popular encryption algorithms: AES and Twofish.

We discussed the basic design and the security issues of the two algorithms.

It has been found that both of them have the equivalent safety factor.

From the simulation results we conclude that

For Text Encryption

AES is faster than Twofish, but with increasing RAM Twofish become faster than AES.

For Image Encryption

AES is faster but with increasing RAM Twofish performs at same speed.

For Sound Encryption

Twofish performs better and with more RAM , its speed increases even more.

So RAM size affects more the performance of Twofish. In future we intend to conduct the experiments in varying hardware and software environment to evaluate the performances of these algorithms .

References

[1] W. Mano, Modern Cyptography Tbeory &Practice, Prentice Hall, Upper Saddle River**,** New Jersey, 2004

[2] B. Schneier, J. Kelsey, D. Whiting, D. Wagner,C. Hall, and N. Ferguson, "TwoFish: A 128-bit Block Cipher", AES submission, june 1998, http://www.counterpane.com/twofish.html.

[3] J. Daemen and V. Rijmen. AES Proposal: Rijndael. 1999.

[4] E. Biham, "A Note Comparing the AES Candidates," revised ver-sion, comment submitted to NIST, 1999.

[5] L. Knudsen, "Some Thoughts on the AES Process," comment submitted to NIST, Apr 1999.

[6]. A. Nadeem and M. Y. Javed, "A performance comparison of data encryption algorithms", Information and Communication Technologies, ICICT 2005, pp.84-89, 2005.

[7]. N. Ruangchaijatupon and P. Krishnamurthy, "Encryption and power consumption in wireless LANs-N," The Third IEEE Workshop on Wireless LANs, pp. 148-152, Newton, Massachusetts, Sep. 27-28,2001.

[8]. Diaa Salama Abdul. Elminaam , Hatem Mohamed Abdul Kader and Mohiy Mohamed Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms," in IJCSNS International Journal of Computer Science and Network Security, vol.8 No.12, December2008, pp. 280-286.

[9]. S.Hirani, "Energy consumption of Encryption Schemes in Wireless Devices Theses," university of Pittsburg, April 9,2003. Retrieved October 1, 2008.