ISBN : 978-81-945631-7-4

FAI-Conference Proceedings

(VOL: 2, 2020)

International Conference on Engineering , Mathematical and Computational Intelligence

(ICEMCI 2019)

DEC, 21 - 23 | 2019

Jabalpur, Madhya Pradesh, India

Editors

Pankaj Srivastava

C.C. Tan

An informative analysis of Encryption algorithms using quantitative Fitness Function

Rajeev Chourey[1], Chhayansh Purohit[2], Vanshita Bansal[3], Shivam Pratap Singh[4]

[1234] Computer Science and Engineering, Jabalpur Engineering College, Jabalpur, India
rajeevchourey786@gmail.com

Abstract. Today, we are using an enormous amount of data and applications in our day to day life. But not every information is shareable and hence need to be prevented from illegitimate access. Any vulnerability can lead to exploitation and therefore requires security. This can be achieved by encrypting the data and then the information can be passed on safely. Encryption is the process of converting data or information into a coded form so that only the authorized user has access.

To make information more secure Cryptography has come into the picture. Cryptography is the most common method to provide security in the virtual world. There are various Cryptographic algorithms (means of altering data by converting plaintext to ciphertext) such as AES, DES, 3DES, BLOWFISH, and TWOFISH that have been compared below. These algorithms can be efficient depending on the type of field they are used in. In this paper, we are focusing on comparing every aspect of these algorithms. Based on the overall performance analysis of the algorithms we give the best-suited technique for use. The performance criteria are the Fitness Function which is the implementation of the weighted sum model of the multicriteria decision analysis methods, that is computed by taking values such as encryption time, decryption time, etc. Higher the value of Fitness Function better is the performance of algorithm.

Keywords: AES, DES, 3DES, BLOWFISH, TWOFISH, Fitness Function, Avalanche Effect, Encryption Algorithms

1 Related Work

This section gives us a brief overview of studies done in the past that are related to the comparative analysis of data encryption algorithms. A thorough reading of papers published on the above-mentioned topic has helped us to propose a unique and reliable way for the analysis of cryptographic algorithms.

Authors of [1], have done a comparative analysis of three algorithms: RSA, DES, and AES based on parameters like computation time, memory usage, output byte. These are three prime parameters that give us a measure of the performance of any encryption

ISBN :978-81-945631-7-4

algorithm. The paper shows that DES takes the least encryption time among other algorithms under study. RSA consumes the longest time to encrypt raw data.

There is a subtle difference between the encryption time of DES and AES algorithm. From memory usage aspect AES outperforms the other two (RSA and DES) algorithms. RSA has high memory usage but when it comes to output byte it gives ciphertext of shorter length than the other two algorithms.

In [2], Alanazi and his other co-authors did a comparative analysis of three encryption algorithms (DES, 3DES, and AES). Factors under consideration were the key length, block size, possible keys, cipher type, security, possible ASCII printable character keys and time required to check all probable keys at a rate of 50 billion keys per second, etc. The authors came out with the result that AES is better than DES and 3DES.

In[3], Authors have focused their study on five data encryption algorithms (DES, 3DES, AES, RSA, and MD5) and done a thorough analysis of them by taking various factors such as block size, key size, and encryption time/decryption time, possible keys, etc. The paper concludes that AES has a greater edge over other algorithms under consideration in terms of execution speed, time to break the algorithm and security.

The content in, [4] is based on performance analysis of various encryption techniques used to implement multistage encryption and decryption of data being stored on a cloud. Authors of this paper have tried different combinations of encryption algorithms such as RSA & DES, RSA & AES, RSA & IDEA for multistage encryption and they evaluated above-cited combinations in terms of encryption time performance. Experimental results of the paper suggested that RSA & IDEA gave higher performance than other combinations.

Unlike any other theoretical comparisons [5], it has proposed a method of comparing different cryptographic algorithms by analyzing trade-offs in their strength, weakness, cost, and performance and then recommending the best algorithm which meets the user requirements best. The authors took five algorithms: DES, 3DES, RSA, AES, and BLOWFISH for their study. Various evaluation parameters considered in this paper are encryption time, decryption time, memory used, Avalanche effect, entropy, number of bits required for encoding optimally. Experimental results showed that BLOWFISH has less memory requirement whereas RSA requires the largest memory among considered algorithms. RSA took the longest time to encrypt and decrypt while BLOWFISH consumed the least time amongst all. When the evaluation was done on the avalanche effect parameter it was observed that AES shows the highest avalanche effect which makes it more reliable in applications where confidentiality is of paramount concern. Results also showed that BLOWFISH has the highest entropy i.e. Blowfish has strong resistance against brute force attacks and AES requires the highest number of bits to be encoded optimally an encrypted data and DES demands less number of bits be encoded optimally.

ISBN :978-81-945631-7-4

2 Algorithms in Consideration

2.1 AES

Advanced encryption standard (AES) is a block cipher encryption algorithm, it uses a symmetric key of variable length 128 bit,192 bit and 256-bit keys, it allows a data block of 128 bits at a time for encryption process and number of rounds depends on the key size selected i.e. 10 rounds for 128 bit, 12 rounds for 192 bit and 14 rounds for 256-bit keys, AES Is the most used widely accepted encryption algorithm for data encryption

2.2 3DES

Triple data encryption standard (3DES) is an improvised version of the DES algorithm it uses the sequential implementation of DES algorithm on the plain text three times with three types of keys. Due to improvements in modern computers and high computational powers, the old DES algorithm became prone to brute force attacks so adding two more layers over the same algorithm made it enough complex. It uses a key of 168 and 112 bits and 64-bit block size and 48 rounds.

2.3 BLOWFISH

BLOWFISH is a block cipher encryption algorithm, this algorithm is open source with no patent and has a huge application base, this algorithm has a block size of 64 bits and has a variable-length key which varies from 32 bits to 448 bits, this algorithm works on fiestal network. This algorithm was designed as a suitable replacement for existing algorithms as a fast and secure algorithm.

2.4 TWOFISH

TWOFISH is a symmetric block cipher with 128-bit block size and key size up to 256 bits it was one of the top five finalists of the advanced encryption standard contest. It is the next generation of blowfish algorithm; this algorithm also works on Feistel structure like the blowfish algorithm.

ISBN :978-81-945631-7-4

2.5 IDEA

IDEA is a symmetric block cipher algorithm which operates on a 64-bit block with a 128-bit key, this algorithm was used as a replacement for DES algorithm, it consists of 8 identical rounds and provides decent security to the data.

3 Proposed Methodology for Comparison

This paper takes five main types of encryption algorithms into account for analysis, these algorithms are thoroughly analyzed based on raw data and data collected from previous researches. The algorithms are analyzed both qualitatively and quantitatively over certain parameters which play a crucial role in defining the quality and nature of an encryption algorithm. Furthermore, the comparative analysis of the undertaken algorithms is quantified by a fitness function which represents all the crucial technical parameters under consideration to give out a fixed value for each algorithm.

3.1 Various Characteristic Parameters

Block size. Block size is the number of bits or bytes processed by a block cipher; each encryption algorithm has a specific block size i.e. that algorithm can process the number of bits equal to the block size in each step. The more the number of blocks the more secure the ciphertext will be.

key size. is the amount of bits or bytes used to make a key for the algorithm to encrypt the data, key can be called an alphanumerical sequence which helps the algorithm to frame the cipher from the plain text and the same key is further required to descramble the ciphered data, key is nothing but a lock, different encryption algorithms use different sized keys, some algorithms are flexible regarding size of keys and have multiple options for size of keys, the size of key plays a very important role in deciding the strength of an encryption algorithm we can say that the encryption strength is directly proportional to the size of the key because as the length of the key will be increased the chances of cracking the key by any means will be decreased.

Rounds. Rounds in encryption algorithms are defined as the iteration of a set of operations on the given data multiple times, a single round consists of the set of operations and which are specifically defined for each encryption algorithm explicitly. Also, each of the discussed algorithms has a definite round sequence as per the definition of that specific algorithm. Number of rounds of a particular encryption algorithm directly reflects the complexity of the output cipher data from that algorithm, in other words, we can say that the provided normal input sequentially passes through the rounds adds more and more complexity to the cipher and will make it

ISBN :978-81-945631-7-4

quite difficult to decrypt, although having more number of rounds can increase time overhead for the algorithm and it may be possible that for larger chunk of data the algorithm may take a tremendous time to encrypt.

Avalanche effect. Avalanche effect is a desirable property of a cryptographic algorithm typically for block-cipher based algorithms. It says that if a single bit or byte in the input plain text is changed then there should be a considerable change in the output cipher. This parameter is so far the most crucial parameter which defines the quality of an encryption algorithm. In the case of the quality of block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. A good cipher must satisfy avalanche> 50% moreover, it is suggested to use more than one test case and take the average value of the avalanche effect.

Encryption Time. Encryption time is the time required by the encryption algorithm to encrypt the plain text to ciphertext, encryption time should be less as it reflects the performance of the algorithm.

Decryption Time. Decryption time is the time required by the algorithm do decrypt the cipher using the same key, this time must be less than encryption time, it also depends upon the key size and the ciphertext size.

3.2 Fitness Function

The fitness function is introduced to quantize the overall characteristic parameters taken into consideration above, into a value to arrive on a single point of conclusion for the result. The fitness function is the implementation of the weighted sum model of multiple criteria decision analysis methods. Due to the non-monotonicity of the characteristic parameters of encryption algorithms concerning the size of the input plain text, we analyzed the fitness function of the algorithms for different input sizes and calculated individual fitness values.

F = fitness value
B = block size
K = key size
R = rounds
E = encryption time
D = decryption time
A = avalanche effect

$$F = [\ 0.4K + 0.5A + 0.3(B+R) + \{(E+D)/E*D\} *1000]$$

All the weights associated with the parameters are decided based on the priority of that particular factor in the analysis of the algorithm.

ISBN :978-81-945631-7-4

We have given the most priority to the avalanche effect because the avalanche effect defines the randomness of the ciphertext concerning the change in plain text.

Key is the second most prior thing in deciding the quality of the encryption algorithm, the larger the size of the key the lesser it will be prone to brute force or other attacks. Apart from key size and avalanche effect the block size and rounds of the iteration are the aspects that describe the performance of the algorithm during the runtime of encryption and decryption.

Encryption time and decryption time are system dependent and may vary with the system configuration but relative values remain almost constant and encryption, decryption time shows the significance of the performance of the algorithm, encryption and decryption time are inversely proportional to the performance of the algorithm/

Data Interpretation. The data of encryption time, decryption time and avalanche effect shown below in table 1, had been obtained by running tests for different file sizes and data strings respectively on an intel i5 9th generation processor clocked at 2.40ghz. we used NetBeans IDE for algorithm implementation using java cryptography extension and bouncy castle API.

Table 1. Encryption and Decryption time of algorithms for different file sizes

ALGORITHM	10 KB		100 KB		1 MB		10 MB	
	E (Ms)	D (Ms)	E (Ms)	D (Ms)	E (Ms)	D (Ms)	E (Ms)	D (Ms)
AES	667	0202	0663	0220	0695	0291	0746	0500
3DES	990	0263	1020	0291	1206	0531	1650	1082
BLOWFISH	1086	0276	1198	0324	1032	0450	1340	0719
TWOFISH	1152	0281	1050	0308	1099	0473	1292	0802
IDEA	1234	0301	1032	0308	1054	0401	1207	0914

All the characteristic parameters are shown in table (2) depend upon the design of algorithm some of the parameters have the flexibility to attain more than one value, we have taken a single value of each parameter for more accurate and precise analysis and the same values have been used for obtaining the dependent data.

Table 2. Value of various parameters of each algorithm used for testing and data generation purposes.

Algorithm	Key size	Avalanche effect (%)	Block size	Rounds
AES	256	72.34	128	14
3DES	168	55.50	64	48
BLOWFISH	256	56.57	64	16
TWOFISH	256	70.33	128	16
IDEA	128	56.13	64	8

ISBN :978-81-945631-7-4

The data tabulated in the above tables are further used for the calculation of the fitness function. The values of the function are tabulated below (the values are rounded up to their nearest integer values for convenience).

Table 3. values of the fitness function for different file sizes

Algorithms	Fitness function (F)			
	10kb	100kb	1mb	10mb
AES	188	187	186	184
3DES	133	133	131	130
BLOWFISH	159	157	158	156
TWOFISH	185	184	183	182
IDEA	104	105	104	102

4 Result and Analysis

In this section, we will discuss the result obtained by the analysis of the undertaken factors.

4.1 Fitness Trends

Fig. 1. fitness function vs file size for different algorithms

Figure 1 shows what the fitness function concluded: The best algorithm for encryption is AES for all the four ranges of data size the second one is TWOFISH algorithm,

ISBN :978-81-945631-7-4

as the fitness function is attaining the second-highest value for TWOFISH for all four file sizes, the two fish algorithm was the finalist in advanced encryption standard contest the winner was AES algorithm after TWOFISH comes to BLOWFISH then 3DES and then IDEA

4.2 Encryption and Decryption Time

As per the needs of the end-user of the algorithm, one must need to know the requirements and available trade-offs' which most commonly in the field of cryptography is of encryption and decryption time. Below we discuss the performance of the algorithms concerning their encryption and decryption time.

Encryption time.

Fig. 2. Encryption time vs File size

As far as encryption time is concerned AES algorithm proves to be the least encryption time taking algorithm for all file sizes with the maximum value of 746ms for 10mb file and 667ms for a 10 kb file. After AES, 3DES is the second least time taking encryption algorithm with 990ms for a 10kb file and 1020ms for a 100kb file. In 1mb and 10mb file size blowfish is proved to be more efficient than 3DES.

ISBN :978-81-945631-7-4

Decryption time.

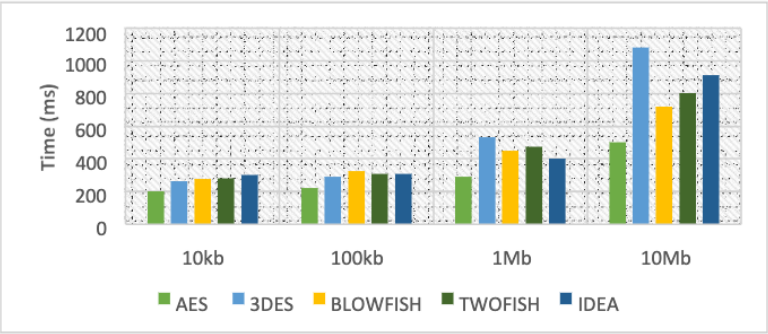

Fig. 3. Decryption time vs File size

For decryption time AES tops the rest as it takes a minimum time 0f 202ms for a 10kb file to decrypt and a maximum of 500ms for a 10mb file to decrypt. After AES there is a 3DES algorithm that has the second least decryption time for 10kb and 100 kb file range and then blowfish for 1mb and 10 Mb file range. 3DES takes the highest value among all others in the 10 Mb file range.

4.3 Avalanche Effect

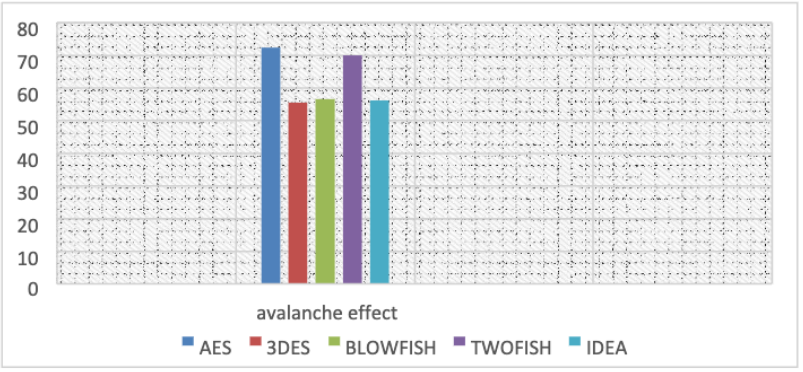

Fig. 4. Avalanche effect of given algorithms

ISBN :978-81-945631-7-4

The highest avalanche effect is shown by the AES algorithm with 73% and then the second-highest avalanche effect is shown by the TWOFISH algorithm with 70% after TWOFISH there are BLOWFISH, IDEA and then 3DES, the least avalanche effect is shown by 3DES of 55%.

Table 4. Average scaling of algorithms

Algorithm	Average value of fitness function F
AES	186.25
3DES	131.75
BLOWFISH	157.5
TWOFISH	183.5
IDEA	103.75

AES > TOWFISH > BLOWFISH > 3DES > IDEA

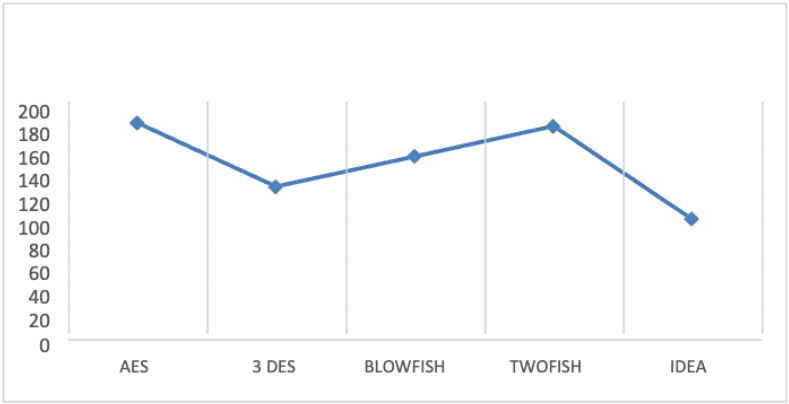

Fig. 5. Average values of the fitness function

As per the average values of the fitness function, we can say that the AES algorithm is the best encryption algorithm with the value 186.25, and the one with the least value i.e. IDEA is least preferable encryption algorithm.

ISBN :978-81-945631-7-4

5 Conclusion and Future Work

We conclude that we have proposed a noble approach for the comparison and analysis of the algorithm using Fitness function. Accordingly, AES has proved to be the best encryption algorithm when compared overall. The rating of each of the algorithms is done based on the average value of fitness function.

The work carried out on the various algorithms will help any technical or nontechnical personality to understand the significance of encryption algorithm in the field of data security, the analysis carried out here based on the quantization of characteristic parameters can be stretched to a new level of limits which can include space complexity, byte entropy and many other factors which can describe the algorithm more accurately and precisely. As mankind has now taken the computational power to a new level where there is a threat to the stored data, and thus there is a need to make it more secure and protected, encryption algorithms play a key role in the protection of the digital data. The algorithms are in a need of refurbishment and reanalysis, the work carried out here might be just a step, there are a lot more things to do.

References

1. Seth, S., Mishra, R.: Comparative Analysis Of Encryption Algorithms For Data Communication. International Journal of Computer Science and Technology. 2, 292-294 (2011).
2. Alanazi, H., Zahidan, A., Bahaa, B., shabbir, M., Al-Nabhani, Y.: New Comparative Study Between DES, 3DES, and AES within Nine Factors. Journal of Computing. 2, 152-157 (2010).
3. Chennam, K., Muddana, L., Aluvalu, R.: Performance analysis of various encryption algorithms for usage in multistage encryption for securing data in the cloud. 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). (2017).
4. Joseph, D., Krishna, M., Arun, K.: Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms. 4th National Conference on Recent Trends in Information. 6, (2015).
5. Patil, P., Narayankar, P., Narayan D.G., Meena S.M.: A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA, and Blowfish. Procedia Computer Science. 78, 617-624 (2016).

ISBN :978-81-945631-7-4