Advances in Dynamical Systems and Applications.
ISSN 0973-5321, Volume 16, Number 2, (2021) pp. 1557-1267

https://www.ripublication.com/adsa.htm

Encryption Algorithm for High-Speed Key Transmission Technique

A.B. Hajira Be[1], Dr. R. Balasubramanian[2]

[1] *Ph.D Research Scholar, Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India.*

[2] *Professor & Dean, Department of Computer Applications, Karpaga Vinayaga College of Engineering and Technology, Maduranthagam Taluk, Tamil Nadu, India.*

Abstract

Security plays a highly crucial role in business transaction. Nowadays, online transaction is used as the inevitable payment method in transferring funds or money. It is super easy for the transaction to be done online for which the whole process is much speedier than one can ever imagine. As the result, the data over the web is continuously exchanged by its users. Cryptography is the elementary category of computer security which changes data from its usual structure into a jumbled structure. This paper purports to present a distinct comparison among the three widely used methods namely data encryption standard, advanced encryption standard and blowfish algorithms symmetric, which are basically symmetric key methods for apply in online transaction process. As far as this study is concerned, the analogy is done using the parameters such as block size, key size, average delay, throughput, energy consumption, encryption time and decryption time. The internet facilitates communication among millions of people all through the world and in the same way, e-commerce is also utilized by huge masses all the time. For this reason, the security level has become the burning question and the issues concerned with online transaction also increase day by day. This paper tries to bring out a solution for which it has taken cryptography, the method of concealing information or data, as its principal task.

Keywords: e-commerce security methodology, cryptography, DES, AES, Blowfish, Encryption, Decryption

1. INTRODUCTION

Cryptography is a process that purports to transform the information so that it can be accessed to provide divergent security-associated ideas that include privacy, data

reliability, validation, endorsement and non-reputation. It is ascertained by two essential segments. The former is known as the algorithm and the latter is called a key. The entire process is a mathematics-oriented methodology in which the key is accessed for data transformation. This process affirms cryptographic security by making use of encryption and decryption. Cryptography is reasonably associated with encryption, for instance, the converting of data from the effortlessly comprehensible phase to the junk[1]. This helps to maintain a strategic distance from unnecessary users who are capable of understanding the data with ease and the senders who hold the capability to encode the data. Its fundamental and central objective is to keep the information secured protecting them from illegal hacking [2].

1.1. The Baseline Study

Algorithms for analogy:

Data Encryption Standard:

It was the principal encryption standard. It utilizes the key range of 56 bit with transferring 64 bit input block into a 64 bit output block. The key in fact resembles a 64-bit capacity; where, one bit in each 8 octets is utilized for uneven equality on every octet. Numerous assaults and techniques have been reported so far which are marked as the shortcomings of DES [3].

Advanced Encryption Standard:

This algorithm can be further named as Rijndael algorithm, which is basically a symmetric based block cipher which can move speedily among the information blocks of 128 bits and make use of symmetric keys such as 128, 192, or 256.This algorithm is recognized with the replacement of the Data Encryption Standard. By using this algorithm, the well-known brute force attack can be neglected [4].

Blowfish

The next one is Blowfish with the construction of block cipher by successfully accessed with a view to getting encryption and the security of data. It takes a uneven length key which is approximately computed between 32 bits and 448 bits, transforming it to be fit for authenticating the information's. This method was identified in 1993 by Bruce Schneier as a speedy, and best when compared to traditional algorithms. Afterwards, Blowfish is permitted and hence it can be utilized for everyone without costs. Although there is an issue that it experiences feeble keys, no attack is still proven n to be effectual against it (Bruce, 1996) (Nadeem, 2005)

1.2 Objectives

The objectives of this paper are cited below as it follows:

a). Upgrade a secure and effective payment transaction in order to avoid fraudulent activity.

b). Expand undefeated and successful information retrieval in e-commerce.

c). Reduce the time period of encryption and decryption, overall delay in average, energy consumption with a view to making transaction safer when compared with the present methodologies in online transaction.

1.2 Key Size and Encryption System

In terms of cryptography, a Key consists of both numeric and combination of alpha-numeric notions with the addition of character. The dimension of the key is the quantity of bits in a key utilized by a cryptographic method. Based on the upper bound calculation of each method in cryptography the key length can be defined. It stands the test of time and the intense scrutiny. This is mentioned because the safety of all algorithms may be mishandled by brutal force assaults. The key is utilized as the encryption which occurs on the simple text whereas the term of decoding works on the cipher text. It is really significant to find the appropriate key for each algorithm for better security. The distinguishing feature of the encryption algorithm is sustained by the secret concept, dimension key, initializing factor, and overall performance [4]. When the key size is enlarged it develops security which in turn makes comprehensive key searching harder.

2. DESCRIPTIONS

2.1. DES

Data security is one of the significant disadvantages of DES. Essentially DES utilizes one 64-bit key with 64-bits chunk, out of 64-bits key, 56-bits are accessed to choose the accurate cryptography modification, and the remaining 8 bits are used for problem detection. As far as DES is concerned, there are overall 16 rounds to carry out their activities; the primary assignment at every round is combination and substitution. The result of DES encryption is 64-bit cipher content. DES can simply be broken by brutal forces. In the beginning, DES was recognized as the standard algorithm with well-built security. Nevertheless, after some period of time, Brute power assault damaged DES. Subsequently, DES is reliably not a protected encryption algorithm [5].

2.2. AES

Advanced Encryption Standard is basically a block cipher based method with the availability of 128 bits block dimensional space with the permission of three various lengths such as 128,192 and 256.Each encryption process consists of several rounds which as explained here: 10 rounds of 128-bit key, 12 rounds of 192-bit keys , 12 rounds of 192-bit keys and 14 rounds of 256-bit keys which perform with the assistance of four steps such as substitution step, a row-wise permutation step, a column-wise mixing step and round key step[6]. While doing so, it is analysed that 128 bits-based AES block is very small. Moreover, Rijndael cipher is capable to compete with any block size. The condition for the dissimilar block sizes still have only four rows in the Rijndael cipher although the number of columns is sustained by the size of the block

2.3. BF (Blow Fish)

BF (Blow Fish) examined by Sahu et al. (2014) incorporates 64-bit chunk which is accessed as a conqueror of the Data Encryption Standard (DES) algorithm. It keeps the changeable key length range from 32-448 bits and most apparently 128-bits. Blowfish has variations of 14 rounds. Its mechanism is open source which is overtly accessible for internet utilities. Blowfish can by all means function up to 448-bits length which has in fact constrained the encryption time.

3. KEY LENGTH COMPARISON

3.1 DES:

Data protection is the most significant disadvantage of DES. The DES does not give strong protection due to its key length of 56 bits. DES might fully break by brute force assault. At first DES was acknowledged as the standard algorithm with strong protection however after some of the time Brute power assault cracked DES. Consequently, DES is certifiably not a secured encryptions algorithm. It can perform with 64 bits plain blocks with the dimension of key is 56 bits. This method used its 8 bits units for detecting the faults in the system. DES break ups the entire region into two sections, and hence it can be applied to 16 round of encryption handling process. Function f includes four phases as development, key blending, substitution and permutation. Protection in DES is the major issue due to 56 bit key length[7].

3.2 AES:

AES provides high security as a result of utilizing variable length key for example 128 bits. In addition to third, AES is a block cipher technique dependent on Feistel network, which uses 128 bits block size and unstable key length of 128, 192 and 256 bits. Based on the key length the number of rounds performed for cryptography varies between 10, 12, or 14 rounds. Every AES round executes key development, Substitute bytes, Shift rows, Mix columns and Add-round key. AES gives a high data protection. Different kinds of assault attempt to split AES like Square assault, key assault, differential assault and enhanced square assault. However, none of them is possible to break this technique. Thus, AES is an extremely protected encryption method. AES can also protect information against future assault.

3.3 Blowfish

Blowfish is a block encryption technique that consists of 64-bit block with the extension from 32-448 bits. It has an elevated protection point because of the adaptability of inconsistent key's length with 448 bits. Blowfish is a protected method against differential key assaults, since every bit of the master key includes various round key which is independent. It can process with 16 processing levels [8] , [9]. The two significant actions such as key development and Data Encryption can be utilized

along with the Substitution boxes in independent manner. This method is necessities with more time because of its extra dimension. The instance rate of uncontrollable speed for sub-key generation may results in brute-force attack. As a result, it can be fulfilled with better security. Dependability of this method is damage because of the utilization of expansive number of feeble keys. The initial four rounds are presented to second request of disparity assaults.

Analyse the block size, key size and round to the symmetric algorithms DES, AES, and Blowfish. The blowfish methodology is outstanding than the trade strategies. If it is analysed and compared with other strategies, the blowfish algorithm is safer and faster. It lessens the execution time, and it offers greater invulnerability. Above all, it ingests much less memory utilization when likened to some other methodologies [10-12].

Table 1: Key Length Comparison

Algorithm	**Key Size (in bits)**	**Block Size (in bits)**	**Round**	**Structure**	**Feature**
DES	64	64	16	Feistel	Not structure, enough
AES	128,192, 256	128	10,12,14	Substitution, Permutation	Replacement for DES, Excellent security
Blow Fish	32-448	64	16	Feistel	Excellent security

Table.1 interprets the blowfish technique that offers implausible insurance plans to examine symmetric algorithms, for instance, DES and AES. Figure 3.6 displays the analogy between key size and block size.

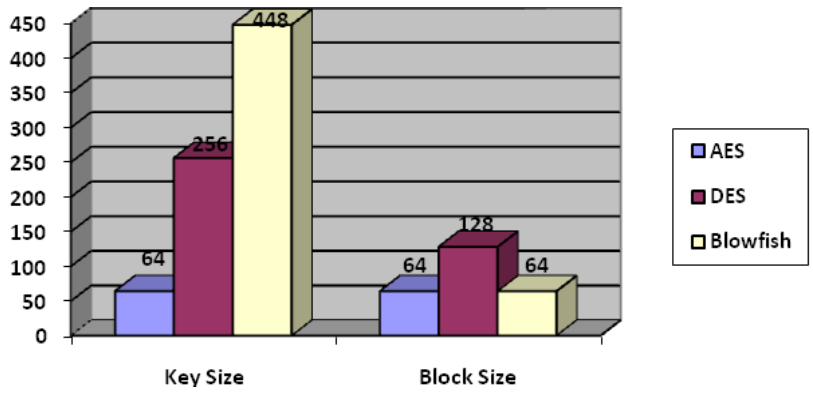

Figure: 1 Key size and block size comparison

DES:

It consists of key's size as 64 bits and block's size as 64 bits. In some specific cases, there are a very few assaults which are acknowledged to be the negative aspects of DES.

Algorithm:

Function DES_Encrypts (D, E) where M = (L, R)

D ←IP(D)

For round ←1 to 16 do

E_i ←SI (E, round)

L ←L xor F(R, Ei)

swap(L, R)

end

swap(L, R)←IP^{-1}(D)

return D End

AES:

In general, AES can be a modern type of encryption method which was previously suggested by NIST. The well-known brute force attack is a most prominent one, where the invader aims to check each and every characters and mixes to open the encryption process. Both advanced encryption standard and data encryption standard has the length of 128, 192, or 256 bits, by means of default 256. This encodes information block of 128 bits in 10, 12 and 14 round based completely on the key size. AES encryption is quick and elastic. It may especially fine be executed on exceptional structures mainly in tiny strategy. AES has been suspiciously observed for some protection purposes.

Algorithm

Ciphers(byte[] input, byte[] output)

{

byte[4,4] State;

copy inputs[] into states[]

AddRoundKeys for (rounds = 1; rounds < Nr-1; ++rounds)

{

SubBytesShiftRowsMixColumnsAddRoundKeys

}

SubBytesShiftRowsAddRoundKeys

Copy states[] to outputs[]

}

Blow Fish:

Divergent tests and research established their outcome that Blowfish algorithm is beneficial and it is also thoroughly worthy in terms of time consumption. Blowfish is, on the whole, a largely fulfilling and an exceptional algorithm in throughput and strength utilization. A variety of evaluations and search for an intense scrutiny demonstrated the occurrence of blowfish approach over a variety of techniques to the extent the managing time. Blowfish is larger than a number of strategies in throughput.

Algorithm:

Divide x1 into two 32-bit halve: x_{LL}, x_{RR} for j= 1 to 16:
$x_{LL}= x_{LL}$XOR $P1_j$
$x_{RR}= F1(x_{LL})$ XOR x_{RR}
swap x_{LL} and x_{RR}
next j
swap x_{LL} and x_{RR}(undo the last swap step)
$x_{RR}= x_{RR}$ XOR $P1_{17}$
$x_{LL}= x_{LL}$XOR $P1_{18}$
Recombine into $x_{LL}$and x_{RR}

From this table 1, it sums up that the blow fish technique is safer to analyse other symmetric key algorithms. It brings about valuable results within very less processing time and rounds. While boosting the key size of blowfish method 128 to 448, it becomes more protective to the messaging. It ensures high end information protection at the time of communications over some risky medium.

The DES, AES and Blowfish secure payment in economic and transactional process. It also incorporates proposed methodology for minimizing the average delay, encryption time, energy consumption, decryption time and getting better throughput as shown in Table 2.It is wholly understood that blowfish is doing its best on every specific restraint and functions veraciously within the parameters that are pertinent.

Table 2: Comparison of three traditional encryption methods

Algorithm	**Average Delay (s)**	**Throughput (Kbps)**	**Energy Consumption (Joules)**	**Encryption Time (s)**	**Decryption Time (s)**
DES	48.7766	28.13	83.087	0.434	0.451
AES	49.1367	5.27	72.087	0.314	0.321
BF	48.7349	35.2	85.544	0.262	0.253

Figure 2 represents the average hold-up in milliseconds and the future algorithm blowfish is likened to the extant algorithms -DES and AES.

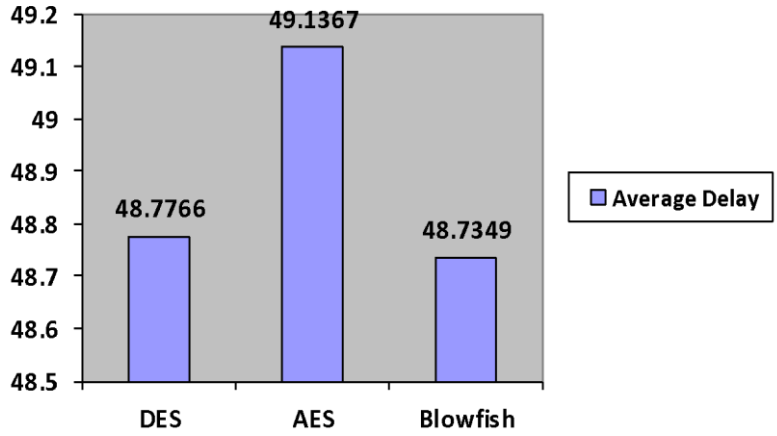

Figure 2: Analyses of average delay

Figure 3 pinpoints the throughput in kbps, and the BF algorithm is compared to subsisting algorithms such as DES and AES.

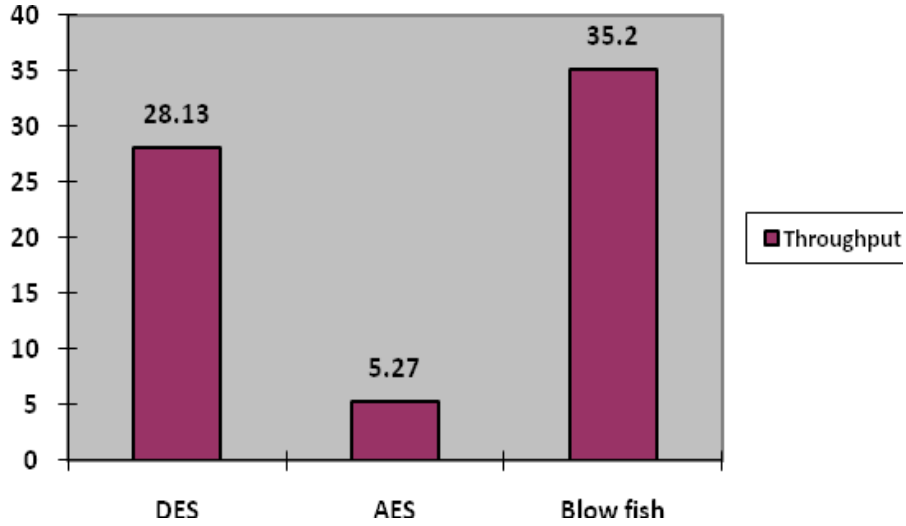

Figure 3: Throughput of E-Commerce

Figure 4 refers to the energy consumption in joules, and BF algorithm is computed to existing algorithms such as DES and AES.

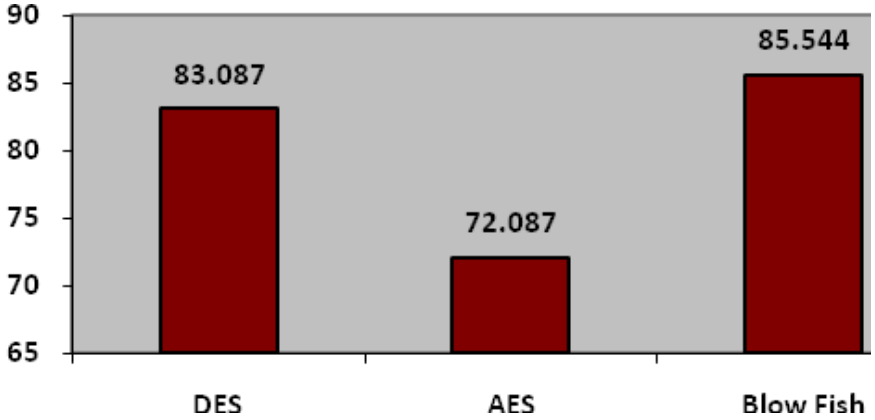

Figure 4: Energy Consumption of E-Commerce

Figure 5 illustrates the time period of both encryption and decryption in ms, and the BF algorithm is estimated. Figure 5 notes the dissimilarities between BF and the subsisting algorithms such as DES and AES.

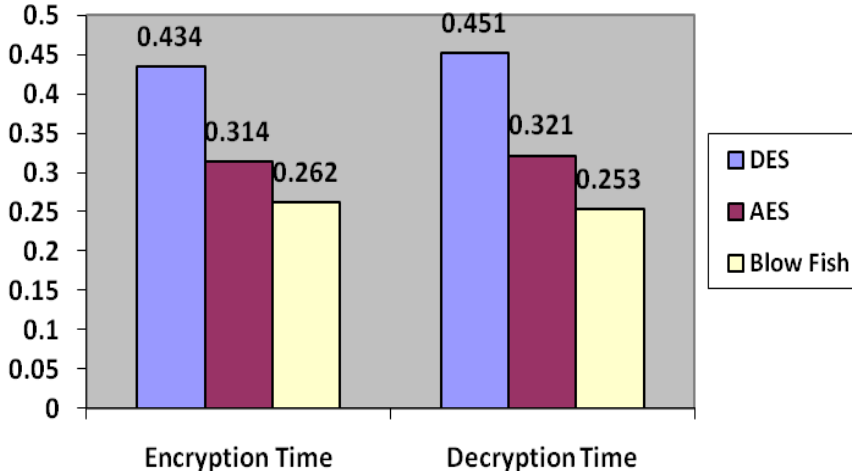

Figure 5: Encryption and Decryption time of E-Commerce

As experimented from Figure 1 to 5, the proposed method is evaluated based o the parameters such as average delay, throughput, encryption time, energy consumption and decryption time. Blow fish is computed with DES and AES methodologies valuing the factors like average delay, throughput, encryption time, energy consumption, and decryption time. AES is the challenger in close proximity which endows with the data privacy and integrity. It aims to lessen key complication, however it's security is not trustworthy many a time. BF augments the protection of the safe and successful payment transactions and by the way, it prevents fraudulent happenings. Blow BF 0.40 AD, 2.45 EC, 0.52 ET, and 0.68 DT qualify 7.02% throughput. To sum up, this paper standardizes the fact that the Blowfish methodology is the best algorithm.

4. CONCLUSION

This research paper has clearly dealt with the cryptography algorithms. The model is interpreted through the developer's compliance with standards and rules. It gives the detailed analogy of the key length and the analytical view of the cryptography methods in real-time applications. Blow fish algorithm is proven to be the well-built security because of its key size. Likewise, when it is compared with the other symmetric key algorithms, it consumes less processing time and rounds. To put it in a nutshell, Blow Fish can be called the numero uno method as it tremendously helps solve the increasing security-associated problems in online transaction.

REFERENCES

[1] Nath, S. Ghosh and M. A. Mallik, "Symmetric key Cryptography using Random Key Generator", Proceedings of International conference on Security and Management, , Las Vegas ,USA, Vol. 2, pp.239-244, 12-15 July, 2010.

[2] AL. Jeeva, V. Palanisamy and K. Kanagaram, "Comparative Analysis of Performance Efficiency and Security Measures of Some Encryption Algorithms", Proceedings of International Journal of Engineering Research and Applications, Vol. 2, pp.3033-3037, May-Jun 2012.

[3] Mr. Mukta Sharma and Mr. Moradabad R. B. "Comparative Analysis of Block Key Encryption Algorithms" International Journal of Computer Applications (0975 – 8887) Volume 145 – No.7, July 2016.

[4] Mr.MilindMathur and Mr. AyushKesarwani "Comparison between DES, 3DES, RC2, RC6, Blowfish and AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013

[5] AnnapoornaShetty , ShravyaShetty K , Krithika K "A Review on Asymmetric Cryptography – RSA and ElGamal Algorithm" International Journal of Innovative Research in Computer and Communication Engineering Vol.2, Special Issue 5, October 2014.

[6] Maryam Ahmed, BaharanSanjabi, DifoAldiaz, AmirhosseinRezaei,andHabeebOmotunde "Diffie-Hellman and Its Application in Security Protocols"International Journal of Engineering Science and Innovative Technology Volume 1, Issue 2,November 2012.

[7] Maryam Ahmed, BaharanSanjabi, DifoAldiaz, AmirhosseinRezaei,andHabeebOmotunde "Diffie-Hellman and Its Application in Security Protocols"International Journal of Engineering Science and Innovative Technology Volume 1, Issue 2, November 2012.

[8] Dr.Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May2013, pp. 571-575

[9] Method Applied to Cloud Computing" International Journal of Information &

Computation Technology. ISSN 0974-2239 Volume 4, Number 15 (2014), pp. 1519-1530.

[10] Sivakumar, N., Balasubramanian, D. R. "*Credit Card Fraud Detection: Incidents, Challenges And Solutions*." International Journal of Advanced Research in Computer Science and Applications, 2015.

[11] J. Sun *et al.*, "FraudVis: Understanding Unsupervised Fraud Detection Algorithms," *2018 IEEE Pacific Visualization Symposium (PacificVis)*, 2018, pp. 170-174, doi: 10.1109/PacificVis.2018.00029.

[12] Thakur, J. & Kumar, Nagesh. (2011). DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis. International Journal of Emerging Technology and Advanced Engineering. 1. 6-12.