© 2019 IJSRSET | Volume 6 | Issue 6 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : https://doi.org/10.32628/IJSRSET196625

Subject Review : Comparison Between 3DES, AES & HiSea Algorithms

Shaimaa Khudhair Salah *1, Waleed Rasheed Humood 2, Ahmed Othman Khalaf 2, Zainab Khyioon Abdalrdha 3
*1-3Department of Computer Science, Collage of Education, University of Mustansiriyah, Baghdad, Iraq

ABSTRACT

Security is one of the main sources of information protection, especially sensitive information that is transmitted over the Internet. Encryption is one of the most important elements used, which is an effective and necessary element to provide high-level security communication between different entities by transmitting unclear and encrypted information that does not allow unauthorized person to access, the method of choosing the appropriate and correct encryption algorithm is important to provide a secure connection that provides a more efficient and accurate encryption system. In this paper, we will review the algorithms (Triple DES, AES & HiSea) for secret key encryption that are most commonly used for this type of encryption.

Keywords : Symmetric Algorithms, Secret Key, Triple DES, AES, HiSea.

I. INTRODUCTION

Many algorithms are designed and developed in order to provide security for most of the information traveling around the world through the network. The main focus in algorithms is to rely on the key where in the algorithms we use one key to encrypt and retrieve text, While in asymmetric we use different keys, one of which is public and the other private for encryption and decryption [1].

Symmetric encryption has a number of advantages and disadvantages. One of the most important advantages is that encryption is fast and includes authentication because it is a secret key used between the two parties and uses one key for encryption and does not require additional operations because it is a fast technology. A disadvantage of this method of encryption is that if you know the key, it will reveal the encryption method, as in Figure 1 that show the keys[2].

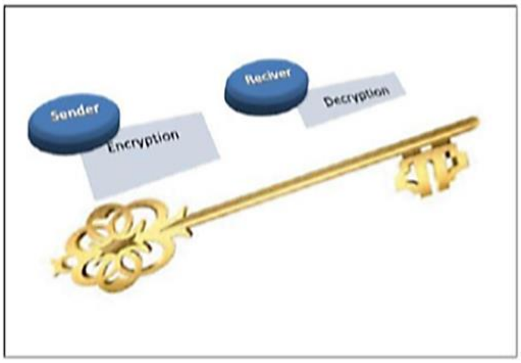

Figure 1 : Secret Key[2].

One of the most important features of this type of public key is the use of two keys represents the strength where it is not easy to break easily, but the disadvantages that it requires a very long time because of the length of the keys used as in Figure 2 that show the keys [2].

Figure 2 : Public Key[2].

In this paper, the focus is on symmetric encryption algorithms where the selected encryption algorithms were compared (3DES,AES & HiSea) in order to review the importance of algorithms and know the strengths and weaknesses of each algorithm in terms of comparing the performance of algorithms, the review paper is arranged as follows: Section II illustrates the selected algorithms; Section 3 provides a comparison of the performance of the algorithms; The conclusion from the audit work is illustrated in Section 4.

II. METHODS AND MATERIAL

Secret Key (Symmetric Algorithms)

In this section, encryption relies on using the same key for encrypting and retrieving text[3]. In this section we will focus on each of the algorithms (3DES,AES & HiSea) in order to compare them and extract the most important differences and advantages that among them in terms of quality, strength and effectiveness of the algorithm from all aspects of its application.

A. Triple Data Encryption Standard (3DES):

TDES is an algorithm that uses three keys where three times the DES keys to increase security where the number of keys increases the attacker's complexity to break the algorithm and the size of each key is 56 bits in order to encrypt each block of data [4]. Figure 3 illustrates the TDES process.

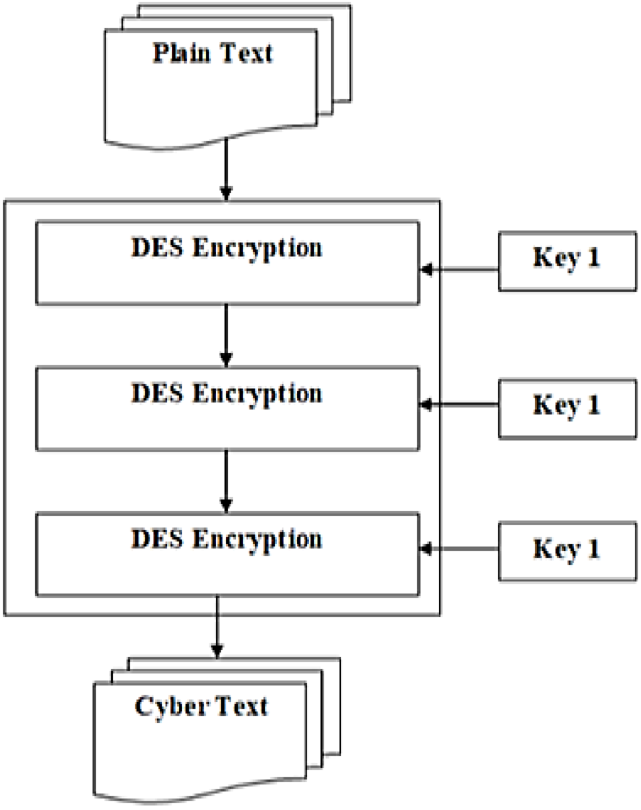

Figure 3 : TDES process [4]

The algorithm has three keys as mentioned for encryption and can be a key of either 56, 112 or 168 bits. As a result of the increase in the number of keys, this results in a process that is slow and much slower than the traditional design. In order to retrieve the original text in the decryption process, which is the reverse process where it uses a 56-bit key length and keeps 8 bits of the least important bits of each byte as parity. So the total number of keys for a Triple DES key strength is only 168 bits. When performing encryption [4].

Finally, the Triple DES algorithm is stronger than DES because Triple DES depends on three keys but DES is based on one key, but Triple DES is slower than DES because it uses three keys in the data encryption process [5].

B. Advanced Encryption Standard (AES):

AES was proposed by NIST in 2001. It can use a set of databases provided by the AES algorithm [6]. In the encryption process, the AES algorithm, (10, 12, and 14) uses rounds of keys for each of (128,192, and 256) sequentially to eventually produce an encrypted message [7]. The 128-bit AES algorithm divides information into 4 basic active blocks that are treated as a line of bytes that are collected into a 4 * 4 array called "state". In the encryption and decryption phase, we add a stage that is considered a round head and before the final round produces 9 rounds that are considered essential through the process of every 4 conversions occurring which are represented by four basic ones ; 1) Sub-bytes, 2) Shift-rows, 3) Mix-columns and 4) Add round Key.

The whole process is illustrated in Figure 4: The encoding and decoding process of the advanced standard encryption algorithm and the previous steps are used in reverse [8]:

a- Substitute Byte transformation:

In this type of byte conversion law substitution of 8-bit is known as (Rijndael s-box) and the AES algorithm in this type takes a 128-bit data block, ie it contains 16 bytes for each database element.

b- Shift Rows transformation

In this type of transfer, it is easy to change the data in the rest of the case periodically based on the remaining three lines. Shift 1 circular to the left of the second line. And two bytes in the third row and run on everyone in succession.

c- Mix columns transformation

In this conversion the multiplication of each column is performed and bytes in this type are treated as multiple names.

d- Add round key transformation

This type of operation uses a similar bit to the 128-bit XOR of the circular key and 128-bit of the current state.

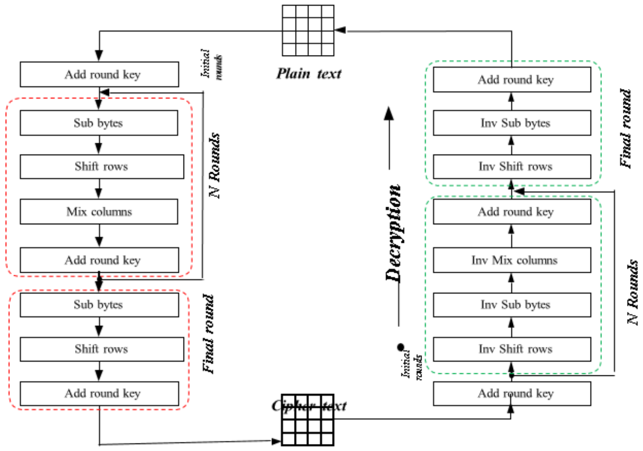

Figure 4 : The Encryption and Decryption Process for the Advanced Standard Encryption Algorithm [9].

C. Hybrid Cube Algorithm (HiSea)

HiSea is an asymmetric block encoding that uses an integer in the process of encrypting plain text and decrypting encrypted text and keys. The HiSea coding algorithm was developed and updated by Sapiee Jamel in 2011. Plain text is a 64-byte ASCII decimal type for the encryption process, where Hybrid Cube (HC) relies on multiplying the inner matrix of layers between magic cubes (MC) [10] . The HC matrix of the 4x4 command is defined as $H_{i,\ j}$, i {1, 2, 879} and j {1, 2, 3, 4} as follows:

$$H_{i,\ j} = MC_{i,\ j}\ MC_{i\ 1,\ j} \qquad (1)$$

where the $MC_{i,\ j}$ is a j^{th} layer of i^{th} magic cubes. Assume we have coordinates {x = 1, 2, 3, 4} where we multiply with the matrix of the MC 1 layer to produce HC 1 and then we generate HC 2 by multiplying the coordinates of the MC 2 layer with{X = 1, 2, 3, 4} Similarly we complete the rest of the layers Until a new HC cube is constructed based on MC layers, the complexity can be increased using a combination of several HC layers input for the design of complex algorithms in coding and decoding[11], [12].

Figure 5. illustrates the overall design of HiSea where plain text, keys, and encrypted text in the encryption process are formatted in matrix 4 order. 8. The following steps are used for the encryption algorithm:

1) Plain text is formatted with ASCII symbols as 64 characters and four arrays of plain text are created as P1-P4. The output (P1) is used as the intermediary for the P2 encryption process and the P2 result as the intermediary for the P3 encryption process. Until we get to P4. This is done to increase the complexity of encryption.

2) The encrypted text named P1´ is created by mixing P1 with the primary matrix (IM) and so on until we reach P4. Then P1´ is added with Session Key 1 (K1). Use the Mix Row and Mix Col function to create a post in Cipher text 1 (C1).

3) C2 is created which is Cipher text 2 (C2) where it consists of adding plain text which is P2 where it is mixed with P1´ to produce P2´ and then mixed with K2 which is session key 2 and produced by Mix Row and Mix Col

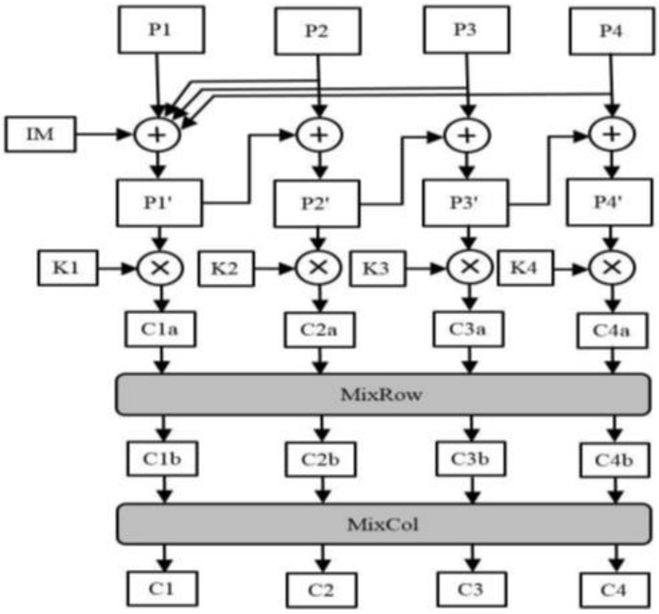

Figure 5. The Overall Design of (HiSea)[13].

4) Previous operations are repeated depending on P3 and P4 to create 3 (C3) and 4 (C4) HiSea encryption text, which is characterized by security and large space and has difficult keys for the attacker to guess or calculate or time-consuming [14], [15].

Performance comparison between 3DES, AES & HiSea Algorithms

In this part we will describe performance analysis based on research studies and how to address the security aspects of how to develop algorithms based on criteria for assessing the quality of the algorithm. In addition, it has shown a number of studies that combine development and security in this area. Some researchers have focused on cryptographic algorithms, evaluating their performance and generally relying on block coding performance on the size for block, length for key used and the number of rounds, as shown in Table 1, as shown in Table1. Structure of 3DES, AES & HiSea Algorithms which shows a comparison between the structure of algorithms used in this research to compare the performance of algorithms for symmetric encryption (3DES, AES & HiSea). On the other hand, evaluate the work performance of (3DES, AES & HiSea) algorithms in terms of throughput, Level of Security, Encryption Speed Effectiveness, etc. is also shown in Table 2. Comparison of productivity power for (3DES, AES & HiSea) algorithms, the selected algorithms were compared in terms of Published, developed by, Algorithm Structure, Block cipher, and the attack type of the algorithm as shown in Table 3. General description of (3DES, AES & HiSea) algorithms. This research has noticed that the HiSea algorithm is better than the rest. During the evaluation, the efficiency of the algorithm was determined and its strength determined the strong encryption and considered a solution to several problems for any system being designed or developed.

TABLE 1. THE STUCTURE OF THE (3DES, AES & HiSea) ALGORTHIMS

3DES type	Structure of 3DES		
	Cipher Key Length	**Data Block Size**	**Number of rounds (N)**
2DES	112 bits for key length	64 bits for block size	48 for number of rounds
3DES	168 bits for key length	64 bits for block size	48 for number of rounds
AES type	**Structure of AES**		
AES 128	128 bits for key length	128 bits for block size	10 for number of rounds
AES 192	192 bits for key length	128 bits for block size	12 for number of rounds
AES 256	256 bits for key length	128 bits for block size	14 for number of rounds
HiSea type	**Structure of HiSea**		
HiSea	1 – 4096 set of integers	64 characters	4 for Number of rounds

TABLE 2. COMPARISON OF PRODUCTIVITY POWER FOR (3DES,AES & HiSea) ALGORITHMS

3DES type	Throughput	Level of Security	Encryption Speed	Effectiveness	Flexibility or Modification
3DES	Lower than DES	Adequate security	Very slow	Slow in software	YES, Extended from 56 to 168 bits
AES type					
AES	Lower than 3DES	Excellent security	Fast	High efficiency in (software and hardware)	Yes, the key size is 256 multiplier 64.
HiSea type					
HiSea	Lower than AES	Highly secure	Moderate	Efficient in software	No

TABLE 3. GENERAL DESCIPTION OF (3DES, AES & HiSea) ALGORITHMS.

3DES type	Published	Developed by	Algorithm Structure	Block cipher	Attacks
3DES	1998	IBM	Feistel	Binary	The type of attack is brute force, explicit unknown text, and, Chosen plaintext
AES type					
AES	2001	Joan Daeman, Vincent Rijmen	Permutation - Substitution	Binary	Side channel attack
HiSea type					
	2011	Sapiee Jamel	Substitution-Permutation	Non-Binary	Not yet

III. CONCLUSION

In this paper, a comprehensive review of the symmetric encryption algorithms was conducted and three algorithms (3DES, AES & HiSea) were selected for the importance of these algorithms in the encryption aspect and high security in this area. We have provided a detailed summary of the 3DES, AES and HiSea algorithms. The discussion on these algorithms was particularly focused and we showed the most important comparison according to the performance evaluation that is mentioned in Table (1,2,3). Based on the availability of resources, HiSea can be used in systems where data reliability and confidentiality are top priorities. By comparison, we observed that this review solved the need to develop hybrid cryptographic algorithms. This combines the features of various algorithms to enhance safety and its desire for most encryption techniques.

IV. ACKNOWLEDGEMENT

The authors would like to thank AL_Mustansiriyah University (www.uomusiriyah.edu.iq), Baghdad-Iraq for its support in the present work.

V. REFERENCES

[1]. D Paul Joseph , M Krishna& K Arun ,(2015). “Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms”, International Journal of Advanced Research in Computer Science, Volume 6, No. 3, (Special Issue).

[2]. Ali M Alshahrani1 and Prof. Stuart Walker ,(2014). “IMPLEMENT A NOVEL SYMMETRIC BLOCK CIPHER ALGORITHM”, International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 4.

[3]. E. Kalai Kavitha, (2012). “Performance Evaluation of Cryptographic Algorithms: AES and DES for Implementation of Secured Customer Relationship Management (CRM) System”, IOSR Journal of Computer Engineering (IOSRJCE) ,ISSN: 2278-0661, Volume 7, Issue 4, PP 01-07 www.iosrjournals.org

[4]. M. S. Premalatha, B. Ramakrishnan,(2019). “TDWOA: Effective Triple DES with Whale Optimization Algorithm for Trust Based Offloading System”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-4.

[5]. Mohit Marwaha, Rajeev Bedi, *Amritpal Singh, and Tejinder Singh , (2013). “COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS”, Singh et al., International Journal of Advanced Engineering Technology, July-Sept,pp.16-18.

[6]. Singh, G, (2013).“A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, International Journal of Computer Applications, Vol. 67, No. 19.

[7]. Singh, M. G., Singla, M. A., & Sandha, M. K, (2011).”Cryptography Algorithm Comparison for Security Enhancement in Wireless Intrusion Detection System”, International Journal of Multidisciplinary Research, Vol. 1, No. 4, pp.143-151.

[8]. Mandal, A. K., Parakash, C., & Tiwari, A. (2012). “Performance evaluation of cryptographic algorithms: DES and AES”, 2012 IEEE Students’ Conference on Electrical, Electronics and Computer Science. doi:10.1109/sceecs.2012.6184991.

[9]. Omar G. Abood, Shawkat K. Guirguis ,(2018). “A Survey on Cryptography Algorithms”, International Journal of Scientific and Research Publications, Volume 8, Issue 7. DOI: 10.29322/IJSRP.8.7.2018.p7978.

[10]. S. Jamel, T. Herawan, and M. M. Deris,(2010). “A cryptographic algorithm based on hybrid cubes,” Computational Science and Its Applications ICCSA, vol. 6019, pp. 175–187.

[11]. S. Jamel, M. M. Deris, I. Tri, R. Yanto, and T. Herawan,(2011). "HiSea: A non binary toy cipher," Journal of Computing, vol. 3, no. 6, pp. 20–27.

[12]. M. F. Mushtaq, S. Jamel, and M. M. Deris,(2017). "Triangular Coordinate Extraction (TCE) for hybrid cubes," Journal of Engineering and Applied Sciences, vol. 12, no. 8, pp. 2164–2169.

[13]. Muhammad Faheem Mushtaq, Sapiee Jamel, Abdulkadir Hassan Disina, Zahraddeen A. Pindar, Nur Shafinaz Ahmad Shakir, and Mustafa Mat Deris, (2017). " A Survey on the Cryptographic Encryption Algorithms", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 8, No. 11.

[14]. S. Jamel, M. M. Deris, I. T. R. Yanto, and T. Herawan,(2011)."The hybrid cubes encryption algorithm (HiSea)," Communications in Computer and Information Science, Springer-Verlag Berlin Heidelberg, vol. 154, pp. 191–200.

[15]. M. F. Mushtaq, S. Jamel, K. M. Mohamad, S. A. A. Khalid, and M. M. Deris,(2017)."Key generation technique based on triangular coordinate extraction for hybrid cubes,"Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 9, no. 3-4, pp. 195-200.

Cite this article as :

Shaimaa Khudhair Salah, Waleed Rasheed Humood, Ahmed Othman Khalaf, Zainab Khyioon Abdalrdha, "Subject Review: Comparison Between 3DES, AES and HiSea Algorithms ", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 6, pp. 97-103, November-December 2019. Available at doi : https://doi.org/10.32628/IJSRSET196625

Journal URL : http://ijsrset.com/IJSRSET196625