Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: January, 2023 **2023, 20(4): 1414-1424** **E-ISSN: 2411-7986**

DOI: https://dx.doi.org/10.21123/bsj.2023.7315

Digital Data Encryption Using a Proposed W-Method Based on AES and DES Algorithms

Wisam Abed Shukur ***Luheb Kareem Qurban*** ***Ahmed Aljuboori*** *

Computer Science Department, College of Education for Pure Science/Ibn Al-Haitham, University of Baghdad, Baghdad, Iraq.
*Corresponding author: a.s.aljuboori@ihcoedu.uobaghdad.edu.iq
E-mail addresses: wisam.a.s@ihcoedu.uobaghdad.edu.iq, laheeb.k.k@ihcoedu.uobaghdad.edu.iq,

Received 10/4/2022, Revised 9/9/2022, Accepted 11/9/2022, Published Online First 20/1/2023, Published 1/8/2023

Abstract:

This paper proposes a new encryption method. It combines two cipher algorithms, i.e., DES and AES, to generate hybrid keys. This combination strengthens the proposed W-method by generating high randomized keys. Two points can represent the reliability of any encryption technique. Firstly, is the key generation; therefore, our approach merges 64 bits of DES with 64 bits of AES to produce 128 bits as a root key for all remaining keys that are 15. This complexity increases the level of the ciphering process. Moreover, it shifts the operation one bit only to the right. Secondly is the nature of the encryption process. It includes two keys and mixes one round of DES with one round of AES to reduce the performance time. The W-method deals with Arabic and English texts with the same efficiency. The result showed that the proposed method performs faster and more securely when compared to standard DES and AES algorithms.

Keywords: Advanced Encryption Standard AES, Data Encryption Standard DES, Decryption, Encryption, Keys Encryption.

Introduction:

One of the biggest issues with the expanding usage of computers and the necessity for inter-location communication is the security of digital data [1]. Digital data must be secured to maintain its secrecy, integrity, validity, and availability to just the intended recipient. Data security before it is transferred over a network can be ensured via encryption, which encrypts data in a form that is unreadable to unauthorized parties and can only be decoded by the authorized party [2].

The wide use of the internet leads millions of users to exchange data electronically. Therefore, the need for security and information protection becomes a paramount goal [3]. To fulfill this goal, encryption methods must be used to secure messages between sender and receiver. The advancement of technology affects day-to-day life where information exchange is vital to complete one's essential needs, most of which are carried out using the internet, such as managing finances, communication, and education. Failure to protect this information greatly harms both the client and the beneficiary; therefore, hybrid techniques are proposed to benefit from the advantages of hybridizing the suggested algorithms.

Several encryption algorithms have been used recently [4,5]. They can be divided into asymmetric uses a public key, and symmetric uses a private key. The asymmetric algorithms include two keys one for the encryption and the second for the decryption which can be divided into asymmetric uses a public key, and symmetric uses a private key. The asymmetric algorithms include two keys, one for encryption and the second for decryption [6]. However, the symmetric algorithm involves one key for both encryption-decryption processes. Some algorithms use public-key encryption, such as digital signature and digest message algorithms[7, 8]. The plaintext (original message before encryption) is subjected to different replacements and transformations by the encryption method to produce encrypted text (scrambled message after encryption). Numerous encryption methods are commonly utilized in information security [9].

Nonetheless, (AES) Advanced Encryption Standard and (DES) Data Encryption Standard use

secret key encryption. DES and AES have been found as vulnerable to strong attacks, though the need to find a new method to overcome this problem becomes a necessary target.

Because it combines security, hardware, and software performance, efficiency, and flexibility, the (AES) is one of the most widely used symmetric algorithms [10]. The National Institute of Standards and Technology (NIST) developed AES, which has key lengths of 128, 192, and 256 bits, to replace DES [11] and 3DES. It accepts data with a length of 128 bits and treats it as an array of bytes, treating the data as a 4 by 4 matrix referred to as states. The number of AES rounds depends on the key length [12] and how many different transformations are applied to the states to encrypt the plaintext into ciphertext. Because of its ease of use and excellent efficiency, the AES encryption algorithm is one of the most widely used.

In contrast to other algorithms, it consumes greater computing power [13]. AES uses AddRoundKey, SubBytes, ShiftRows, and MixColumns as its four transformations, with MixColumns having the highest computational cost of the four. Multiplication and addition are the two arithmetic operations that makeup MixColumns. It is an expensive transition because using software to perform AES necessitates computer resources and slows down the encryption process [14].

This paper uses a combination of DES and AES to obtain a high-security algorithm. W-method proposes a new hybrid key based on AES and DES to prevent attackers from getting original data.

The remaining sections of this paper are organized as follows: Section 2 discusses a brief of the related work, while Section 3 describes the materials and methods of this work, specifically the AES and DES algorithms. Section 4 explains the proposed method W-Method; Section 4 discusses experimental results while comparing the performance of (AES and DES)' with the proposed method to show better results. Section 5 contains the conclusion.

Brief of Related Work:

To demonstrate the effectiveness of each technique on the same text files based on three factors: computation size, memory use, and outputs byte. The research [15] conducted a comparative analysis of encryption algorithms for data transfer on AES, DES, and RSA. The research proved that AES and DES require medium memory for implementation, but the RSA needs a large one. Both AES and DES are the best if time and memory are major factors. According to the author, future work will concentrate on the combination of those algorithms as well as ways to speed up encryption and utilize less memory.

Research on the performance assessment of cryptographic algorithms was presented by [16]. Based on time as a parameter, the author compared different cryptographic algorithms including AES and DES. On various multimedia such as video files, and texts, these various cryptography techniques are assessed. Depending on the size of the file, different files are processed at varying speeds. The authors noticed that the AES algorithm executes with a faster throughput level and less processing time than the other algorithms. The study, therefore, suggested that in the future, the effectiveness of such a combination should be evaluated for additional factors including time utilization and bit shifting.

Several studies proved that integrating algorithms can increase performance compared to original algorithms [17–19] and [20]. This paper is an attempt to combine two cryptography algorithms. This combination has shown better performance and improved the level of security. This section discusses some of these studies. The research [21] proposed a hybrid algorithm that depends on combining PRESENT and SPECK. It creates a random key space with minimum 22560 potentially unique combinations of the secret keys in order to defeat brute force attacks and improve the performance. While [22] merged Rivest, Shamira, and Adleman (RSA), AES, and MD5 hashing to generate the essential points of authentication and integrity of the ciphered data. The paper [23] combined AES and Blowfish algorithms using symmetric and asymmetric techniques. This hybrid method has increased the level of security. In addition, the only recipient can decrypt the ciphered text. Whereas [24]integrated biometrics into a cryptographic algorithm. It generates a key from a binary string that overcame the twenty percent error in identifying the iris code. This integration made identifying individuals easier a need for a central database. The research [25] stated a CARCA algorithm that combines asymmetric RSA with symmetric AES algorithms. It protects the holy Quran from the attacker by encrypting the hash digest of the gear function. The authors in [26] argue that DEA (International Data Encryption Algorithm) and International Data Encryption Algorithm (IDEA) perform faster when compared to the original DEA and IDEA. It takes a very long time for the cryptologist to decrypt the information without knowing the key, which provides a high level of security.

Some surveys, such as [27] conducted a comparison between cryptography algorithms. They

proved that the combined techniques perform better with increasing the level of security. The above-mentioned studies would have been more interesting if they had included the rounds of generating keys. Therefore, our paper has considered the rounds to reduce the time. In addition to adding complexity to generating keys, it strengthens the proposed algorithm against attackers.

Materials and Methods:

DES and AES Algorithms

DES is considered a block cipher algorithm [28]. It is widely used and popular because using a key-symmetry encryption algorithm that is considered a standard. Because the DES is classified as unsafe, the request for a new algorithm appears, as stated in[29]. Another name for DES is the symmetry encryption standard that some researchers called; in 1972, the DES algorithm was developed at IBM[15]. This algorithm is based on the Feistel technique entirely. It was approved by the National Bureau of Standard (NBS) when the United States National Security Agency evaluated the strength of DES [9]. Using symmetric keys in both processes ciphering / deciphering is illustrated in Fig. 1[6].

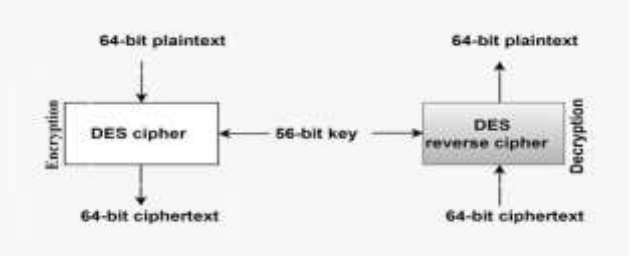

Figure 1. Used keys in ciphering / deciphering DES.

DES takes a fixed-length string of plaintext bits; the plaintext will convert to cipher text with the same length by many complicated operations. In the case of DES, the block size is 64 bits. The used key by the DES consists of 64 bits, but just 56 bits are used [30], and 8 bits are used to check parity. The effective length of the key is 56 bits, and the 8th bit of the selected key is discarded [31]. This process is shown in Fig.2, while the entire cycle for ciphering / deciphering procedures by DES is shown in Fig. 3[15].

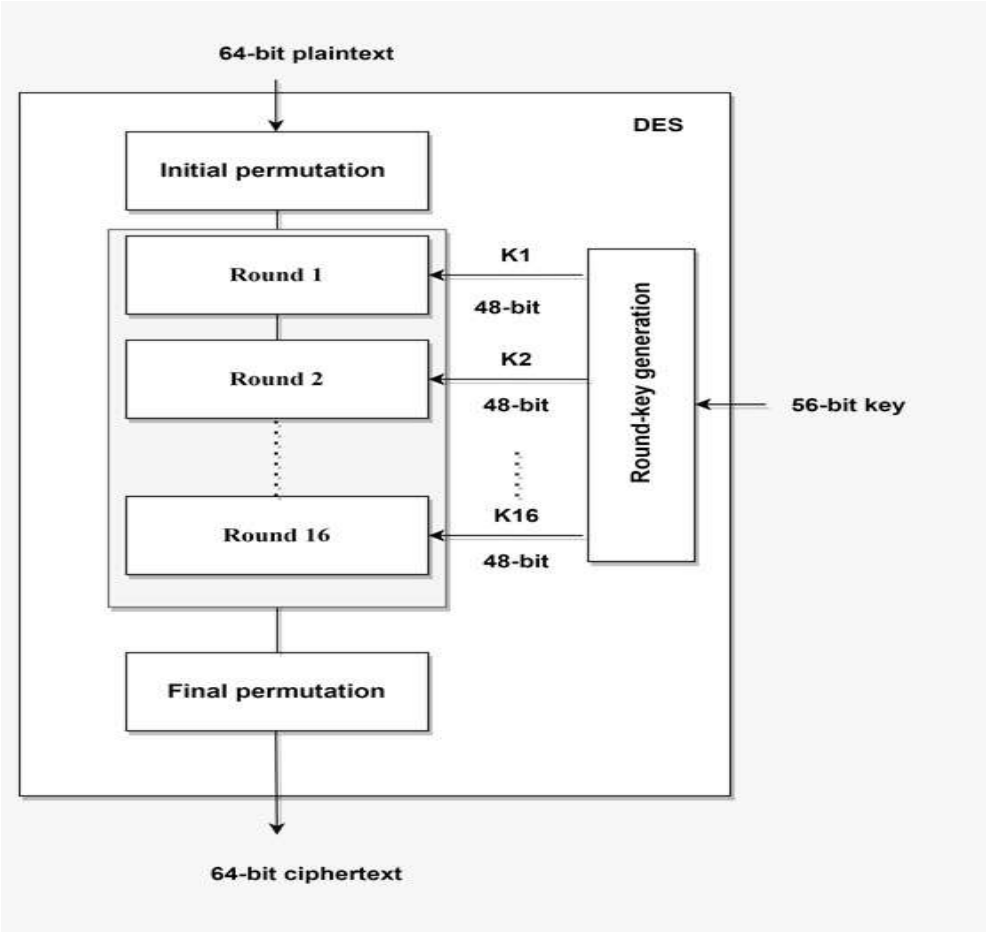

Figure 2. Encryption process with used keys by DES algorithm.

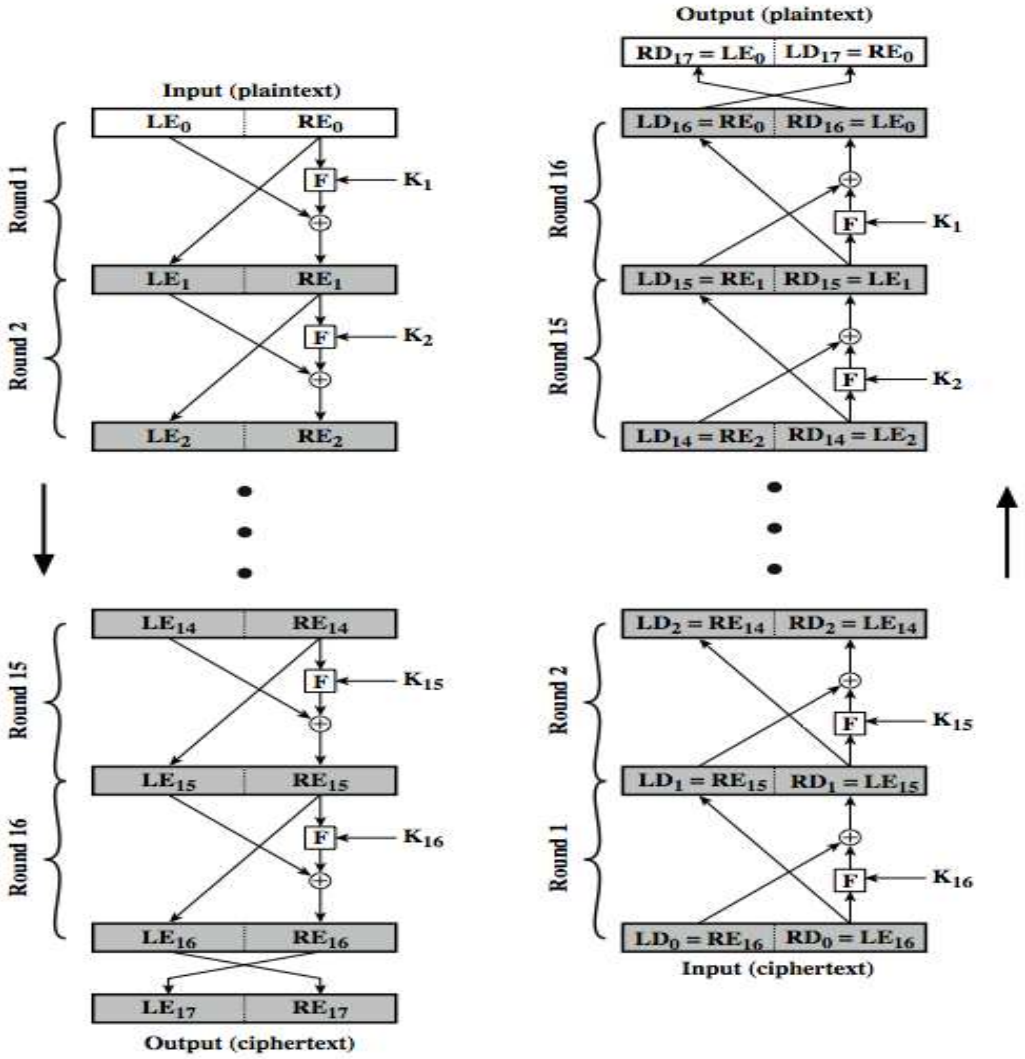

Figure 3. Full cycle for ciphering / deciphering procedures by DES.

AES is considered a symmetric block cipher. For both encryption and decryption procedures, using the duplicate keys generated, the AES is like DES [32]. The main difference between AES and DES is using different sizes of keys and blocks. This means not just the 56 bits of key size and 64 and DES' block [33]. In AES, 128, 160, 192, 224, and 256 bits are chosen as the block and key size independently [34]. The AES is not dependent on Feistel structure; the input data block is initialized and processed in a similar style for each round [35]. A key length is a specified number of AES factors. The number of actual rounds is 10 when the size of the key is 128 bit, the number of actual rounds is 12 when the size of the key is 192 bit, and the number of actual rounds is 14 when the size of the key is 256 bit [36]. The actual or most common number of critical sizes is 128 bit. There are many characteristics of AES that robustness against most known attacks, compactness for a wide range of platforms such as fast coding, and simplicity of design [37]. The general structure of AES is shown in Fig. 4. the plaintext and key are 128 bits depicted as a square matrix of bytes. The used key is expanded into an array of the key that schedules words. The ordering of bytes is noted within the matrix by column[38]. The algorithm starts with a different round key stage, followed by 9 rounds of four and the tenth round of three stages. This approach is applied for both encryption and decryption procedures. The four stages are as follows[39]: 1. Substitute bytes 2. Shift rows 3. Mix Columns 4. Add Round Key. The last round leaves out the stage of Mix Columns. The first nine rounds of the decryption algorithm consist of the following: 1. Inverse Shift rows 2. Inverse Substitute bytes 3. Inverse Add Round Key 4. Inverse Mix Columns Again [40]. The tenth round leaves out the stage of an Inverse Mix Columns. The general structure of the AES algorithm is shown in Fig. 4

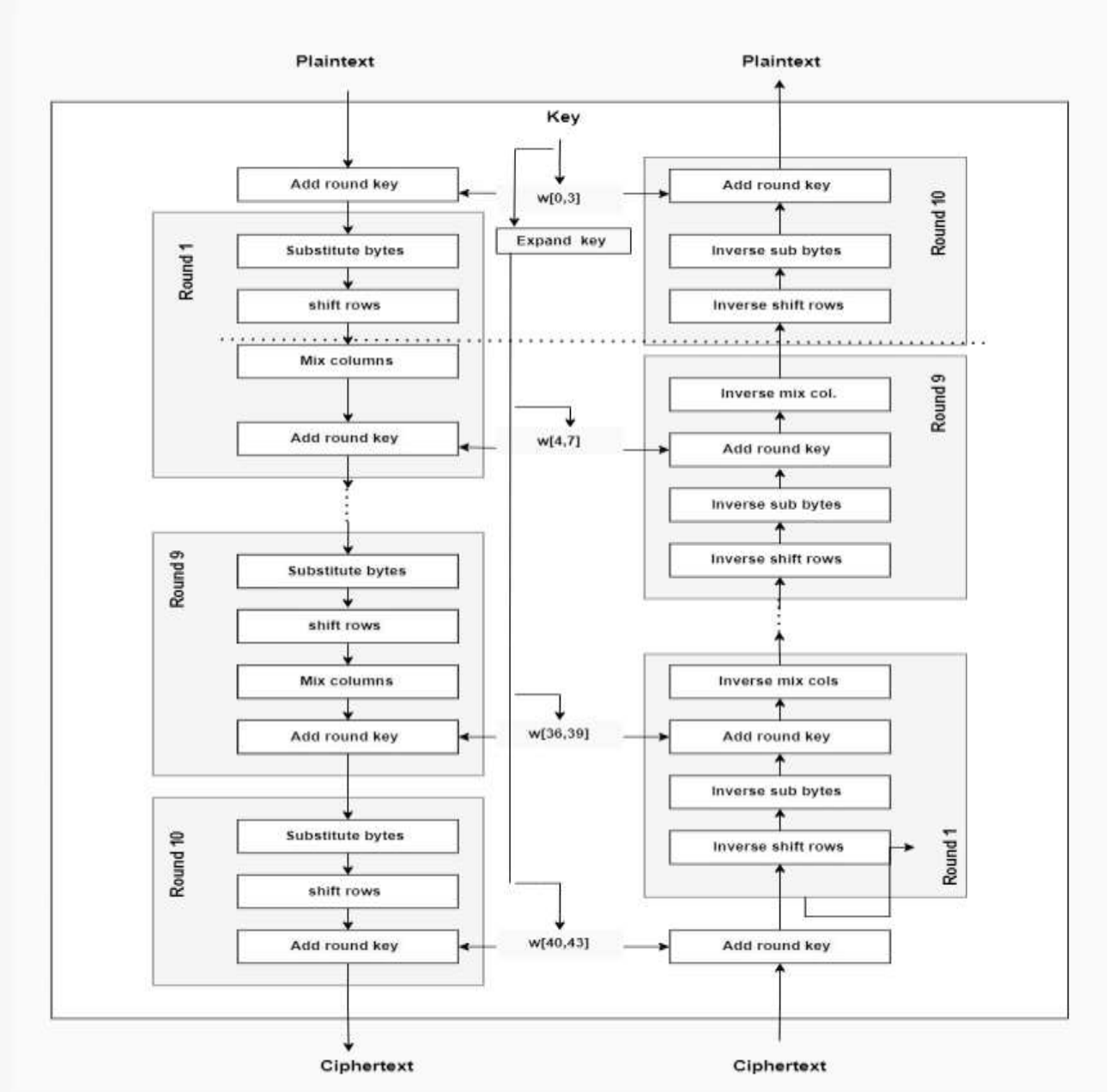

Figure 4. The general structure of the AES algorithm.

The Proposed W- Method

The proposed W-method has two parts, key generation, and ciphering process. Each part has a new style in the operational procedures. The basic idea of the proposed W-method is to merge the process in both parts based on DES and AES entirely. The combining process for key generation and encryption processes is the backbone of this research. W-method takes all the benefits of both DES and AES to suggest a new key generation approach. The strength of the W-method lies in combining both DES and AES algorithms to avoid defects. When complexity is added to the keys generation procedure, the strength of the cipher is increased. The complexity of the W-method is represented by using 16 keys and 8 rounds generated and applied via the mixing procedure of DES and AES.

Baghdad Science Journal
2023, 20(4): 1414-1424
P-ISSN: 2078-8665
E-ISSN: 2411-7986

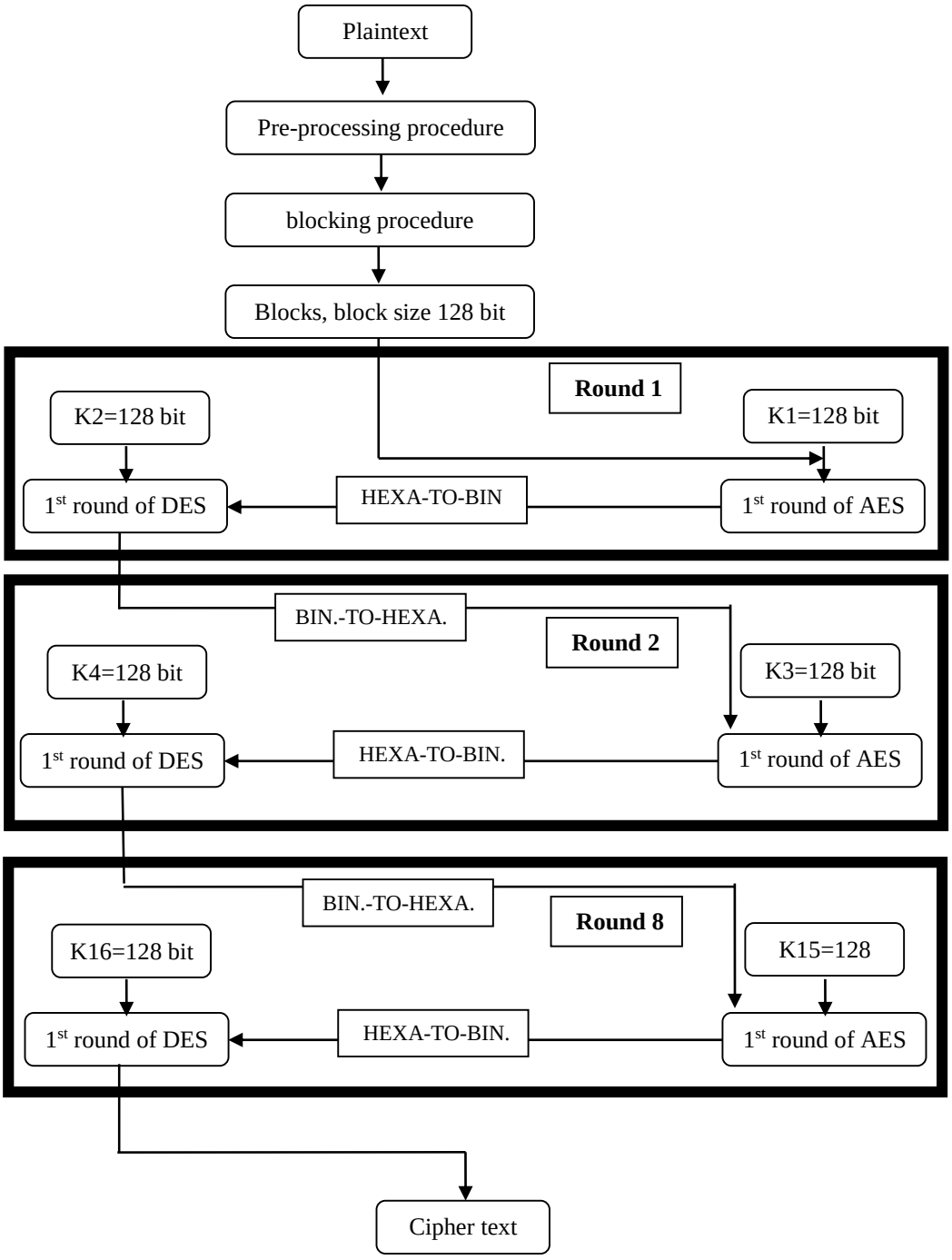

Figure 5. The general architecture of the proposed W- method.

The first key is generated by merging 64 bits of DES with 64 bits of AES to produce 128 bits as a root key for all remaining keys that are 15. All 15 keys will be generated from the mother key that is K1 by applying the shifting procedure to the right one bit only; the shifting procedure is accumulated. Each round uses two keys and applies just one round of DES and AES; therefore, 16 keys must be available at this stage. The plaintext is divided into blocks, and each block has a size of 128 bits. The input to the key generation part is 128 bit, and the output of the key generation part is 128-bit, considering many pre and post-processing steps. The general architecture of the proposed W-method is shown in Fig. 5.

Keys Generation Procedure

In this procedure, there are three stages. The first stage is converting, the second stage is blocking, and the third stage is key generation. The first stage deals with an input that is text either in Arabic or English language. This stage is found in each round because DES deals with binary form while AES deals with the Hexa form. Therefore,

this stage will convert each one to another. The second stage is blocking, dividing processed input text, either binary or Hexa, into blocks; each block contains the same number of bits. All blocks are equal in size. The size of each block is 128 bits. Just one block will entire to proposed W-method at a time. The third stage is a key generation used in the encryption procedure. The principle of operation in this stage uses DES and AES to generate the mother key from merging outputs of them. The text file used as the key is uploaded and read for both DES and AES. The DES accepts 64 bit as binary input while AES accepts 128 bit as input but in Hexa form.

The generating steps in DES functions by the exception of adding 8 bit (zeros) on the left side to obtain the final output that 64 bit. In AES, the key that has a size 128 bit will be divided into left and right, and each one of them has the same size that is 64 bit. To compromise between DES and AES, the right side will be deleted and utilize the left side that has a size 64 bit. The final step in AES is applying converting procedure to convert Hexa to binary. The important notice in DES is that not to perform PC-2. The final step in this stage is to perform merging between outputs of both to produce a mother key that has a size 128 bit with binary form. The key generation is shown in Fig. 6.

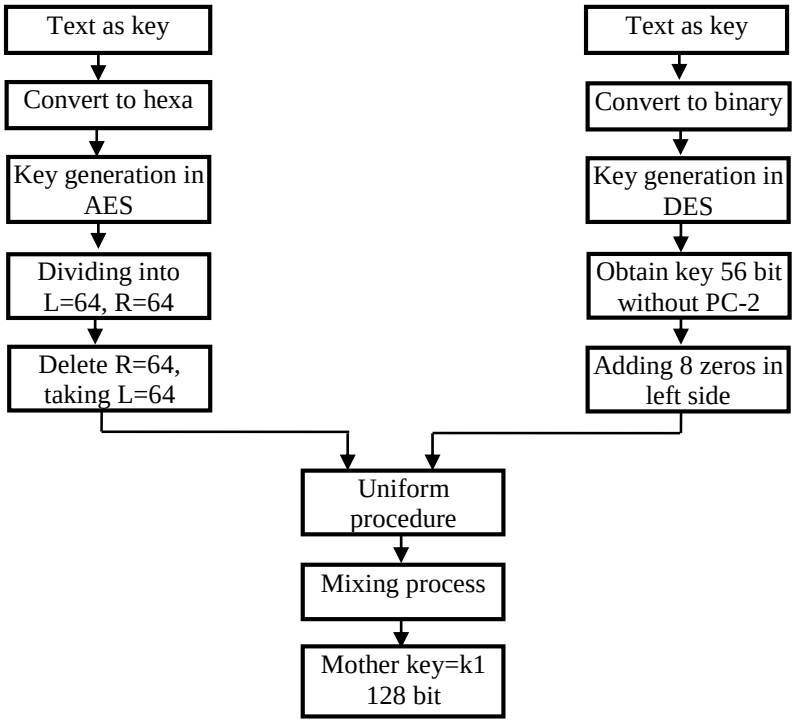

Figure 6. The key generation stage.

All 15 keys will generate from the mother key generated previously as the following operations: K2= shift one bit to the right direction of k1, K3= shift one bit to the right direction of k2, K4= shift one bit to the right direction of k3. K5= shift one bit to the right direction of k4, K6= shift one bit to the right direction of k5, K7= shift one bit to the right direction of k6. K8= shift one bit to the right direction of k7, K9= shift one bit to the right direction of k8, K10= shift one bit to the right direction of k9. K11= shift one bit to the right direction of k10, K12= shift one bit to the right direction of k11, K13= shift one bit to the right direction of k12. K14= shift one bit to the right direction of k13, K15= shift one bit to the right direction of k14, K16= shift one bit to the right direction of k15. K1 and k2 are used in round 1, K3 and k4 are used in round 2, K5 and k6 are used in round 3, K7 and k8 are used in round 4, K9 and k10 are used in round 5, K11 and k12 are used in round 6, K13 and k14 are used in round 7 and K15, and k16 are used in round 8 of proposed W- method. Pairs of keys will use in each round. It is evident that 8 rounds are needed, so 16 keys becomes essential.

Encryption Procedure

After key generation, the encryption procedure is started. To encrypt sensitive data, one must perform eight rounds. Each round uses two generated keys from the previous stage and two operations of ciphering, the first operation is applying the first round of AES, and the result will be considered plaintext to the first round of DES.

This means the plaintext will encrypt double times in each round, representing the strength of the proposed method. At the same time, the complexity is presented by ciphering a plaintext sixteen times with different keys each time. In each round the processed string should be converted from Hexa to binary and binary to Hexa. Using different keys in each round increases the complexity of the cipher algorithm. DES encryption is done by using 128 bit instead 64 bit for each round. However, the PC-2 in DES is not performed to obtain 64 bit instead 56 bit. The pseudo-code of the W-method is shown in Algorithm 1:

Algorithm 1: encryption procedure of TheW-method:

```
Input: pi where p is plaintext
    Ki where k is generated key
Output: ci where c is ciphertext
   Begin
       Load plaintext from file f
       Apply converting procedure
       Apply blocking procedure pi
       R=1, i=1.
While (r< =8)
       Load pi
       Read pi
       Load keys from file k
       Read ki=ki+1
       Apply 1st round of AES
       Apply 1st round of DES
     End;
  R=R+1.
  i=i+1.
 End.
```

Decryption Procedure

On the receiver side, the destination party must decrypt the received encrypted message using the same keys used in the encryption procedure since the type of encryption is a symmetric key. The decryption procedure is done by performing eight rounds on decrypted messages. To obtain an original text according to an algorithm is shown in Algorithm 2:

Algorithm 2: decryption procedure of the W-method:

```
Input: ci where c is ciphertext
Output: pi where p is plaintext
     ki where k is generated key
  Begin
       Load ciphertext from file c
       Apply converting procedure
       Apply blocking procedure pi
       Key generation procedure
       R=8, i=16.
    While (r > =1)
       Load ci
Read ci
       Load keys from file k
       Read ki=ki-1
 Apply 1st round of AES
       Apply 1st round of DES
    End;    R=R-1.    i=i-1.
 End.
```

Results

Our method experiments show the possibility of encrypting Arabic and English texts; all special characters and spaces are encrypted. The practical application of the W-method shows the performance and implementation of DES and AES separate from the W-method, as illustrated in Fig.7:

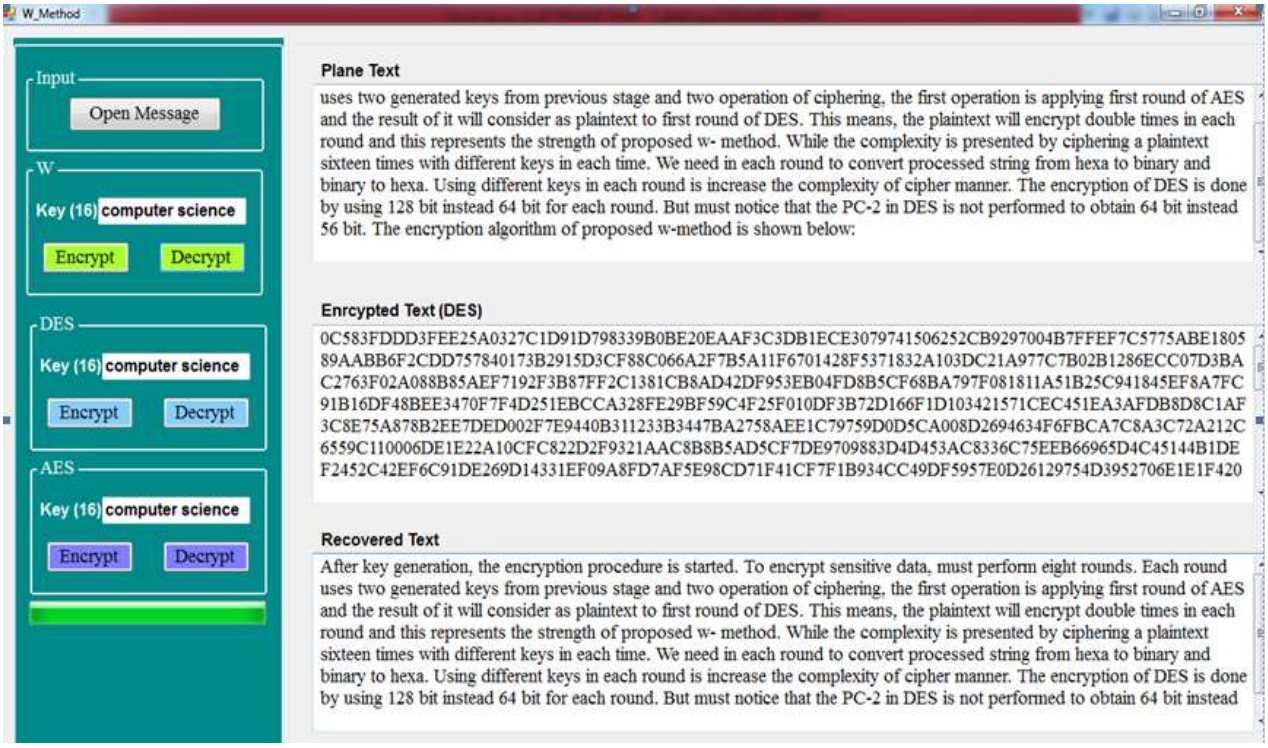

Figure 7. main menu and encryption procedure of the W-method.

There are many evaluation factors used to measure the performance of DES and AES compared to the W- method. Ten evaluation factors were considered. The obtained results are shown in Table 1 below, the factors are the time of ciphering, deciphering, usage of memory, effects of avalanche, security, robustness, entropy, complexity, required coding bits, and efficiency. What can be seen is that W-method shows improvement in speed, security, memory, robustness, and keys type while the inefficiency, size of keys, and coding bits W-method is similar to AES. Moreover, complexity is high both in the W-method and DES.

Table 1. Comparison between DES, AES and W-method

Evaluation metric	DES	AES	W-method
Speed	slow	fast	faster
Security	low	high	Very high
Memory	High (16)	Low (10)	Lower (8)
Coding Bits	more	less	less
Complexity	high	Medium	high
Efficiency	low	high	high
Robustness	bad	good	Very good
Keys Type	Symmetric	Symmetric	Symmetric
Size Of Key	64 bit	128 bit	128 bit

The encryption time depends on three elements; the first is the size of the key, the second is the size of the plaintext block, and the third is a method of ciphering mode. In the practical experiment, the encryption time is measured in a millisecond. In general, the performance is affected by the time of encryption. The required time to recover plaintext from encrypted text is called the time of decryption. The time of encryption and decryption is shown in Table. 2.

Table 2. The time of encryption and decryption.

Cipher method	Encryption Time in a millisecond	Decryption Time in a millisecond
DES	3.71	3.21
AES	3.68	3.04
W-method	2.97	2.16

Conclusion:

This study proposes an integration of AES-DES algorithms as means of strengthening the current ciphering process. The hybrid algorithm gives a better performance than the standard algorithms. AES and as it is merged with DES scored better on the analysis of average time because it may vary depending upon the algorithm speed. One cannot get the different times for the same input for encryption as well as decryption because of the similarity. The proposed algorithm, which is a combination of two strong encryption standards, will function as an effective and trustworthy encryption method for data. This can also employ a double-key strategy to fend off linear attacks.

In this case, the encryption algorithm's security can be enhanced further. Improving DES security by
shifting the operation one bit only to the right and including two keys of mixing one round of DES with one round of AES to reduce the performance time. Finally, the implementation of the W-method provides the list below:

1. The W-method can encrypt spaces, all special characters, and English and Arabic texts.
2. The strength of the W-method is higher than DES and AES.
3. The W-method is faster than DES and AES.
4. The increasing number of keys in each round is possible and easy.
5. In future work, encrypting multimedia will be considered not only plain texts.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Baghdad.

Authors' contributions statement:

W.A.S and A.A. conceived of the presented idea. W.A.S. developed the theory and performed the computations.

A.A. and W.A.S verified the analytical methods. W.A.S encouraged A.A. to investigate [a specific aspect] and supervised the findings of this work. L.K. implemented the practical side. All authors discussed the results and contributed to the final manuscript.

References:

1. Tang Y, Elhoseny M. Computer network security evaluation simulation model based on neural network. J Intell Fuzzy Syst 2019; 37(3): 3197–3204.
2. Zaman S, Alhazmi K, Aseeri MA, Ahmed Muhammad R, Khan R T, Kaiser M, et al. Security threats and artificial intelligence based countermeasures for internet of things networks: a comprehensive survey. Ieee Access 2021; 9: 94668–94690.
3. Al-Hassani MD. A Novel Technique for Secure Data Cryptosystem Based on Chaotic Key Image Generation. Baghdad Sci J. 2022: (19)4: 905-913.
4. Shukur WA, Badrulddin A, Nsaif MK. A proposed encryption technique of different texts using circular link lists. Period Eng Nat Sci 2021; 9(2): 1115–1123.
5. Wisam AS, Khalid KJ, Luheb KQ. A Proposed Hybrid Text Cryptographic Method Using Circular Queue. Int J Civ Eng Technol. 2018; 9(7): 1123-32 .
6. Hossen MS, Tabassum T, Islam MA, Karim R, Kobita AA, Rumi LS. Digital signature authentication using asymmetric key cryptography with different byte number. Evol Comput Mob Sustain Networks Lect Notes Data Eng Commun Technol 2021; 53.
7. Saepulrohman A, Ismangil A. Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA). Int J Electron Commun Syst 2021; 1(1): 11–15.
8. Kavin BP, Ganapathy S. A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves. Int Arab J Inf Technol 2021; 18(2): 180–190.
9. Kumar Y, Munjal R, Sharma H. Comparison of symmetric and asymmetric cryptography with existing vulnerabilities and countermeasures. Int J Comput Sci Manag Stud 2011; 11(03): 60–63.
10. Hidayat T, Mahardiko R. A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing. Int J Artif Intell Res 2020; 4(1): 49–57.
11. Basu K, Soni D, Nabeel M, Karri R. Nist post-quantum cryptography-a hardware evaluation study. Cryptol ePrint Arch 2019; https://ia.cr/2019/047
12. Abdul Hussien FT, Rahma AMS, Abdul Wahab HB. A secure environment using a new lightweight AES encryption algorithm for e-commerce websites. Secur Commun Networks 2021; 2021.
13. Kareem SM, Rahma AMS. New method for improving add round key in the advanced encryption standard algorithm. Inf Secur J A Glob Perspect 2021; 30(6): 371–383.
14. Palit T, Moon JF, Monrose F, Polychronakis M. Dynpta: Combining static and dynamic analysis for practical selective data protection. IEEE Symp Secur Priv. 2021; p. 1919–1937.
15. Patil P, Narayankar P, Narayan DG, Meena SM. A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. Procedia Comput Sci 2016; 78: 617–624.
16. Bhat B, Ali AW, Gupta A. DES and AES performance evaluation. In: IEEE Int. Conf. Comput.Comm Aut, 2015; p. 887–890.
17. Aljuboori AS, Coenen F, Nsaif M, Parsons DJ. Performance of case-based reasoning retrieval using classification based on associations versus Jcolibri and FreeCBR: a further validation study. J Phys Conf Ser. 2018; : 12130.
18. Aljuboori AS, Abdullatif FA, Mahmmed DY. The Classification of Fetus Gender Based on Fuzzy C-Mean Using a Hybrid Filter. In: Journal of Physics: Conference Series. IOP Publishing, 2021; p. 22084.
19. Mohammed DY, Al-Karawi K, Aljuboori A. Robust speaker verification by combining MFCC and entrocy in noisy conditions. Bull Electr Eng Inform 2021; 10(4): 2310–2319.
20. Aljuboori A. Enhancing case-based reasoning retrieval using classification based on associations.

2016 6th Int Conf Inf Commun Manag 2016; 52–56.
21. Hoomod HK, Naif JR, Ahmed IS. A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system. Period Eng Nat Sci 2020; 8(4): 2333–2345.
22. Mahdi Ebadati OE, Eshghi F, Zamani A. A Hybrid Encryption Algorithm for Security Enhancement of Wireless Sensor Networks: A Supervisory Approach to Pipelines. Comput Model Eng Sci 2020; 122(1): 323–349.
23. AbdElminaam DS. Improving the security of cloud computing by building new hybrid cryptography algorithms. Int J Electron Inf Eng 2018; 8(1): 40–48.
24. Hao F, Anderson R, Daugman J. Combining cryptography with biometrics effectively. IEEE Trans Comput, 2006; 55(9): 1081-1088.
25. Ahmad MA. Protection Of The Digital Holy Quran Using IT Techniques. PhD [dissertation].Sydney: University of Malaysia; 2014. https://studentrepo.iium.edu.my/bitstream/123456789/5515/2/t00011304352AbdulateffAhmad_SEC_24.pdf
26. Kumar P, Parihar SS. Working Analysis of Multistage Cloud Security Algorithms. Int J Res Appl Sci Eng Technol. 2022; 10 (Issue I Jan): 1327-1338
27. Almuhammadi S, Al-Shaaby A. A survey on recent approaches combining cryptography and steganography. Comput Sci Inf Technol (CS IT) 2017; 7(2): 63-74.
28. Beenu VP. Mathematical formulation of des algorithm [J]. Int J Pure Appl Math 2018; 118(10): 363–376.
29. Curzon P, McOwan PW. Computational Thinking: Die Welt des algorithmischen Denkens–in Spielen, Zaubertricks und Rätseln 2018; 2th ed. St. Springer: Verlag; 229 p. https://www.amazon.com/Computational-Thinking-algorithmischen-Denkens-Zaubertricks/dp/3662567733
30. Khlif N, Ghorbel A, Aydi W, Masmoudi N. Generation of Chaotic Signal for Scrambling Matrix Content [J]. Int Arab J Inf Technol 2020; 17(4): 548–553.
31. Yang L, Yang B, Xiang C. Quantum public-key encryption schemes based on conjugate coding. arXiv Prepr arXiv11120421. 2011;
32. Albahar MA, Olawumi O, Haataja K, Toivanen P. Novel hybrid encryption algorithm based on AES, RSA, and TwoFish for bluetooth encryption. J inf secur 2018; 9 (2): 168-176.
33. Abhilasha CP, Nataraj KR. Software Implementation of AES Encryption Algorithm. Int J 2016; 6(5): 159-171.
34. Priya S, Karthigaikumar P, Teja NR. FPGA implementation of AES algorithm for high speed applications. Analog Integr Circuits Signal Process 2021;1–11.
35. Nabil M, Khalaf AA, Hassan SM. Design and implementation of pipelined and parallel AES encryption systems using FPGA. Indones J Electr Eng Comput Sci 2020; 20: 287–299.
36. Rajashree S, Sukumar R. CBC (Cipher Block Chaining)-Based Authenticated Encryption for Securing Sensor Data in Smart Home. In: Smart IoT for Research and Industry. Springer, 2022; p. 189–204. https://link.springer.com/chapter/10.1007/978-3-030-71485-7_12
37. Lu Z, Mohamed H. A Complex Encryption System Design Implemented by AES. J Inf Secur 2021; 12(2): 177–187.
38. Shaji N, Bonifus PL. Design of AES architecture with area and speed tradeoff. Procedia Technol 2016; 24: 1135–1140.
39. Kumar P, Rana SB. Development of modified AES algorithm for data security. Optik (Stuttg) 2016; 127(4): 2341–2345.
40. Forhad MSA, Riaz S, Hossain MS, Das M. An improvement of advanced encryption standard. Int J Comput Sci Netw Secur 2018; 18(11): 159–166.

تشفير البيانات الرقمية باستخدام طريقة W المقترحة بناءً على خوارزميات AES و DES

وسام عبد شكر **لهيب كريم قربان** **احمد صبيح توفيق**

قسم علوم الحاسبات، كلية التربية للعلوم الصرفة/ ابن الهيثم، جامعة بغداد، بغداد، العراق.

الخلاصة:

يقترح هذا البحث طريقة تشفير جديدة. فهو يجمع بين خوارزميتين للتشفير ، وهي DESوAES لإنشاء مفاتيح هجينة . يقوي هذا المزيج طريقة W المقترحة عن طريق توليد مفاتيح بطريقة عشوائية ذات امان عالي. في الأساس ، يمكن تمثيل موثوقية أي تقنية تشفير بنقطتين. أولاً ، هو توليد المفتاح ، وبالتالي ، فإن نهجنا يدمج 64 بت من DES مع 64 بت من AES لإنتاج 128 بت كمفتاح جذر لجميع المفاتيح المتبقية التي تبلغ 15. هذا التعقيد يزيد من مستوى عملية التشفير. بالنهاية ، ينقل العملية قليلاً إلى اليمين فقط. ثانيًا بمقدار بت واحد مما يغير طبيعة عملية التشفير. يشتمل الطريقة المقترحة على مفتاحين ويمزج جولة واحدة من DES مع جولة واحدة من AES لتقليل وقت الأداء. تتعامل طريقة W مع النصوص العربية والإنجليزية بنفس الكفاءة. تظهر النتيجة أن الطريقة المقترحة تعمل بشكل أسرع وأكثر أمانًا عند مقارنتها بخوارزميات DES و AES القياسية.

الكلمات المفتاحية: معيار التشفير المتقدم AES، معيار تشفير البيانات DES ، فك التشفير، تشفير المفاتيح، التشفير.