DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

In-Depth Assessment of Cryptographic Algorithms Namely DES, 3DES, AES, RSA, and Blowfish

Samara Mohammed Radhi[1], Raheem Ogla[2]
[1,2]Computer Sciences Department, University of Technology, Baghdad, Iraq
[1]ce.19.45@grad.uotechnology.edu.iq, [2]raheem.a.ogla@uotechnology.edu.iq

Abstract— *Securing information is difficult in the modern internet era, as terabytes of data are generated daily online and online transactions occur virtually every second. The current world's information security relies heavily on cryptography, which makes the internet a safer environment. Making information incoherent to an unauthorized person is done through the use of cryptography. Providing legitimate users with confidentiality as a result. There are a wide variety of cryptographic algorithms suitable for this purpose. An ideal cryptography method would allow the user to do their job without breaking the bank. Unfortunately, there is no magic formula that can address every issue.Several algorithms balance cost and performance. A banking application needs robust security at a high cost, while a gaming software that sends user patterns for analytics cares more about speed and cost. Thus, choosing the appropriate encryption technique for the user. This study offers important insights in the process of selecting cryptographic algorithms in terms of each algorithm's strengths, weaknesses, cost, and performance . In order to demonstrate an entire performance analysis in this article, as opposed to just theoretical comparisons, this research developed and thoroughly examined the cost and performance of commonly used cryptographic algorithms, including DES, 3DES, AES, RSA, and blowfish. According to the findings, blowfish requires the smallest amount of time to decrypt files of various sizes (25K, 50K, 1M, 2M, 3M, and 4M), and it also consumes the smallest amount of memory. This makes it approximately three times faster than other cryptographic algorithms.*

Index Terms— *Cryptograph Algorithm, Security attacks , Key, Cipher*.

I. INTRODUCTION

Cryptography is used to protect data integrity when moving it between two parties in different places. The data is unintelligible until it is decrypted, which is the second part of the process that occurs after the recipient receives the encrypted message [1], [2]. The archiving, processing, and retrieval of data have all been greatly simplified by the advent of computing devices. Computers and services based on the internet are utilized by virtually all individuals, as well as all branches of the government, the judicial system, and businesses of varying sizes. The fact that cybercriminals are also rapidly adapting to new technologies places a heavy burden on information security professionals and computer scientists [3]. The technology that is relied on so heavily today is user-friendly and straightforward, but it does not come without inherent dangers. Everyone in this room is ecstatic about the effortless access to information and communication that is provided by their laptops and smartphones. Users have access to a wide variety of online programs around the clock, including social media platforms, retail and banking platforms, and more. On the other hand, if an attacker gets a hold of a banking password, the process of stealing

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

money can be carried out with the same ease. It is possible for someone else to access your social media accounts and use those credentials for malicious purposes. As a result, it is of the utmost importance to protect data while it is residing in applications, while it is moving through networks, and while it is being stored on computers [4], [5].

Encrypting data is a reliable method of keeping private data out of the wrong hands. The design of cyber defenses relies heavily on making it difficult for data to be intercepted. You can utilize this concept to protect all sorts of information, from government secrets to private data. There are two major categories of cryptography systems: asymmetric and symmetric. The difference between symmetric and asymmetric encryption methods is that the former requires the use of a single secret key for both transmission and reception, while the latter requires users to keep track of two separate keys [6], [7].

Several other cryptographic algorithms have been the subject of research. These algorithms include RSA, AES, DES, 3DES, and Blowfish. Efforts have been made to evaluate the algorithms' performances to determine their applicability to different information security requirements. Existing comparative studies have shown conflicting findings, and the selection of cryptographic algorithms used for comparison has been heavily weighted toward symmetric encryption techniques [8], [9]. Therefore, an attempt was made to strengthen some existing studies with the results obtained from the current study, and, in addition, both symmetric and asymmetric encryption/decryption algorithms were chosen for comparison in this study, as opposed to just symmetric algorithms in most previous studies.

The purpose of this article is to This research paper is broken up into five parts. The relevant research is discussed in the next section. The research materials and procedures are described in Section III. Algorithm implementation is shown in Section IV. The paper's evaluation criteria are presented in Section V. The study's findings are discussed in detail in Section VI, while its conclusion is presented in Section VII.

II. RELATED WORK

A comparison of symmetric and asymmetric cryptography with existing flaws and countermeasures, give a theoretical comparison of the algorithms for symmetric and asymmetric encryption is illustrated by Kumar et al. [4]. While Jeeva et al. [10] developed a comparison of symmetric and asymmetric cryptography algorithms, including such factors as key length, tunability, speed, encryption ratio, and security assaults, among others, to determine which is more effective for encrypting data and preventing unauthorized access. A new study conducted and released by Singh et al. [11]examines the similarities and differences between DES, 3DES, AES and RSA based on distinct criteria such as: key length, cipher type, block size, developed year, cryptanalytic resistance, possible keys, possible ascii keys, and time required to check all possible keys. A comparison of symmetric and asymmetric cryptography techniques was carried out by Tripathi and Agrawal [12] the factors that were taken into consideration were throughput, key length, tunability, speed, encryption ratio, and security attacks. Mahindrakar [13] evaluated the blowfish algorithm based on the avalanche effect provides a new performance measuring metric that is named the avalanche effect. David et al. [14] Compare popular algorithms like AES, DES, RSA, and the lightweight cryptographic algorithm Fernet to find the most efficient and secure cryptographic approach to minimize threats to data integrity and security in IoT applications.

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

Data security was improved by Dulla et al. [15] tweaks to the Blowfish algorithm and developed some sort of file-encrypting software. When a file is split into multiple parts according to the user's preferences, the encryption technique is put into action. To enhance the functionality of the program, they modified the Blowfish algorithm by modifying the F-function. Four S-boxes compose the F-function (S1, S2, S3, and S4). An experiment showed that the sped-up version of the Blowfish algorithm was 14% faster. A modified Blowfish method, suitable for 128-bit blocks, was proposed by Reyes et al. [16]. Although the Blowfish technique has been proven to be unbreakable, it has been incompatible with various implementations due to its short block length. By implementing a flexible choice encryption system and decreasing encrypted function operations via randomly selected rounds, this study develops a novel updated version of the Blowfish encryption system that can handle inputs of up to 128 bits in length. Using metrics including encryption quality, correlation coefficients, key sensitivity tests, and output file size, Shetty et al. [17] analyzed and contrasted various implementations of Blowfish. A new version of the 'f' function was developed by combining the XOR and addition of the old method. There were four distinct scenarios developed and evaluated. All the results from the tests performed on these use cases came to the same conclusion: the original Blowfish approach is smaller and more secure because of the improvements made to the algorithm.

III. CRYPTOGRAPHIC ALGORITHMS

This section makes a comparison. After implementing the methods, cryptography strength, complexity, and response time were tested. Encryption and decryption time measurements help gauge application responsiveness. Until now, neither the memory consumed nor the number of bits needed to optimally encode has been used to measure cost. Entropy and the avalanche effect, which measure cryptographic systems' robustness and attack resistance, have not been used in previous testing. To assess the efficacy of the algorithms in light of this, we have incorporated certain distinct metrics.

A. DES

The Data Encryption Standard (DES) is an example of a symmetric-key block cipher. This key is 56 bits long, and this block is 64 bits long. The usage of a vulnerable key allows for an attack to be carried out on the target. In 1972, IBM researchers were looking for an efficient way to encrypt data, and their efforts paid off when they found DES. The federal government of the United States adopted it as the default method of encryption [18]. DES originally used a 64-bit key, but the NSA only allowed its usage with a 56-bit key length, thus it discarded 8 bits of the original key and instead uses a 56-bit key compressed from the original 64-bit key to encrypt data in 64-bit blocks. DES is highly adaptable because it can operate in several modes, including CBC, ECB, CFB, and OFB. The usage of a vulnerable key allows for an attack to be carried out on the target. A supercomputer named DES cracker, along with the help of thousands of PCs over the Internet, cracked the DES encryption algorithm in 1998. This took only 22 hours [19], [20]. Data Encryption Standard Algorithm, is shown in *Fig. 1*.

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

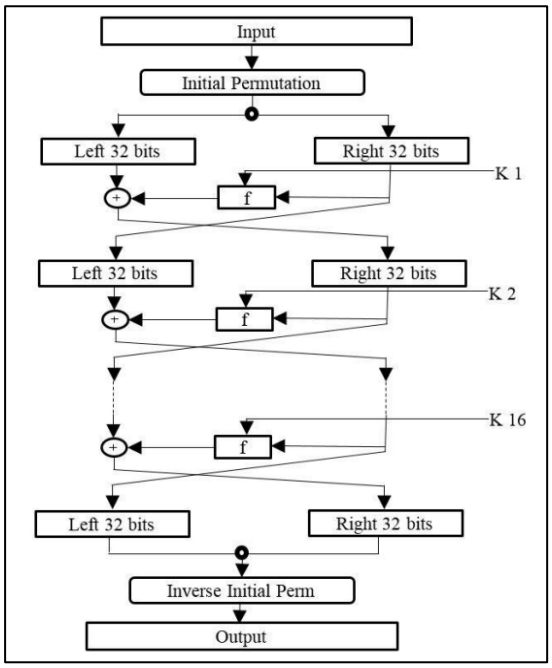

FIG. 1. THE DES ALGORITHM [21].

B. 3DES

In the discipline of cryptography, block ciphers are deployed, and one example of such an algorithm is Triple DES. Triple Data Encryption Algorithm (3DES) is another name for this technique. The Triple Data Encryption Standard, sometimes known as 3DES, was unveiled to the general public for the first time in 1998. Due to the fact that the DES cipher is used for encryption, this system is commonly referred to by its current signature. Each data set was encrypted using the Data Encryption Standard, decrypted, then encrypted again for maximum security. Keys can be 112 or 168 bits long, and blocks can be 64 bits long. It can make it either shorter or longer. The first version of DES was easily broken by brute force and other cryptanalytic methods since it was a weak cipher. Triple DES was created to offer a straightforward means of expanding DES's key size, making it more resistant to such assaults. The main goal in creating Triple DES was to avoid having to create a brand-new block cipher algorithm in order to achieve this [22], [23].The encryption and decryption diagram for 3DES is shown in *Fig. 2*.

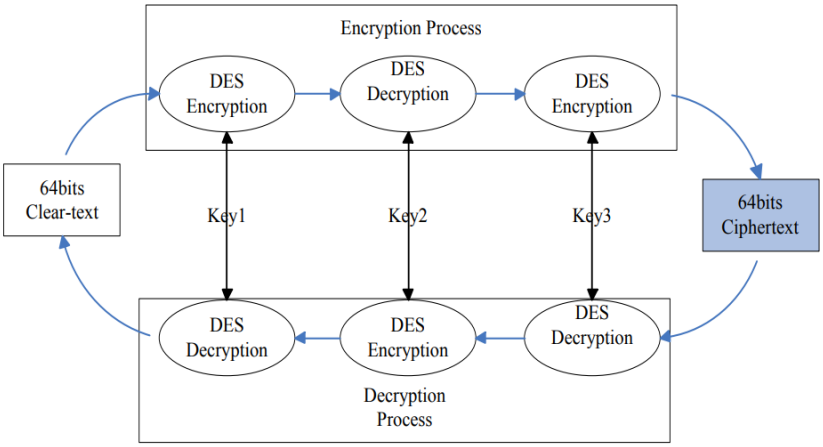

FIG. 2. A REPRESENTATION OF THE ENCRYPTION AND DECRYPTION PROCESSES USED BY 3DES [11].

Received 05/January/2023; Accepted 19/February /2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

C. AES

The Advance Encryption Standard (AES) is a cryptographic mechanism for safe data transfer over networks that was created in 1998 by Vincent Rijmen and Joan Daemen. This encoding uses a block structure with symmetric keys. Data and keys of 128, 192, or 256 bits in length can all be used effectively with the AES algorithm. AES supports data lengths up to 128 bits and may be deconstructed into its four component building blocks. The state, which consists of these squares, is represented as a 4-by-4 byte matrix. They go through rounds, during which time various changes are made to them [24], [25]. Depending on the key length (128, 192, or 256 bits), the number of rounds done during full encryption can be set to N = 10, 12, or 14. The AES algorithm, which is used in both hardware and software implementations, employs a permutation and substitution network during each iteration of the encryption process [26]. An illustration of the Advanced Encryption Standard Algorithm is shown in *Fig. 3*.

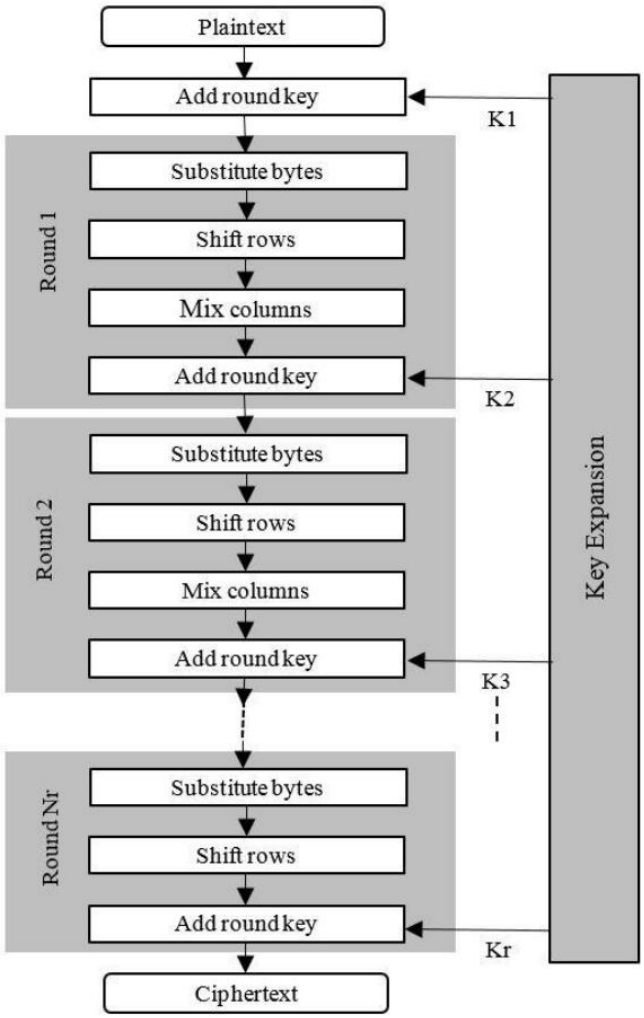

FIG. 3. AES ALGORITHM [21].

D. Blowfish

In 1993, the first copies of Blowfish were made accessible to the general audience. Block cipher with a symmetric key, 64-bit block size, key lengths from 32 bits to 448 bits. DES and 3DES are two of the most popular methods for encrypting data, but Blowfish, a symmetric block cipher, may soon replace them. It is suitable for both private and public

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

use in a business setting due to its ability to employ keys with lengths ranging from 32 bits to 448 bits [27], [28]. Bruce Schneier devised Blowfish as a quick and secure alternative to the standard encryption methods of the time. Since then, there has been a lot of research into it, and it's becoming increasingly popular as a safe method of encryption. Since Blowfish is not subject to any patents or licensing costs, it can be used in any setting without restriction [29], [30]. The Blowfish Encryption Algorithm is depicted in *Fig. 4*.

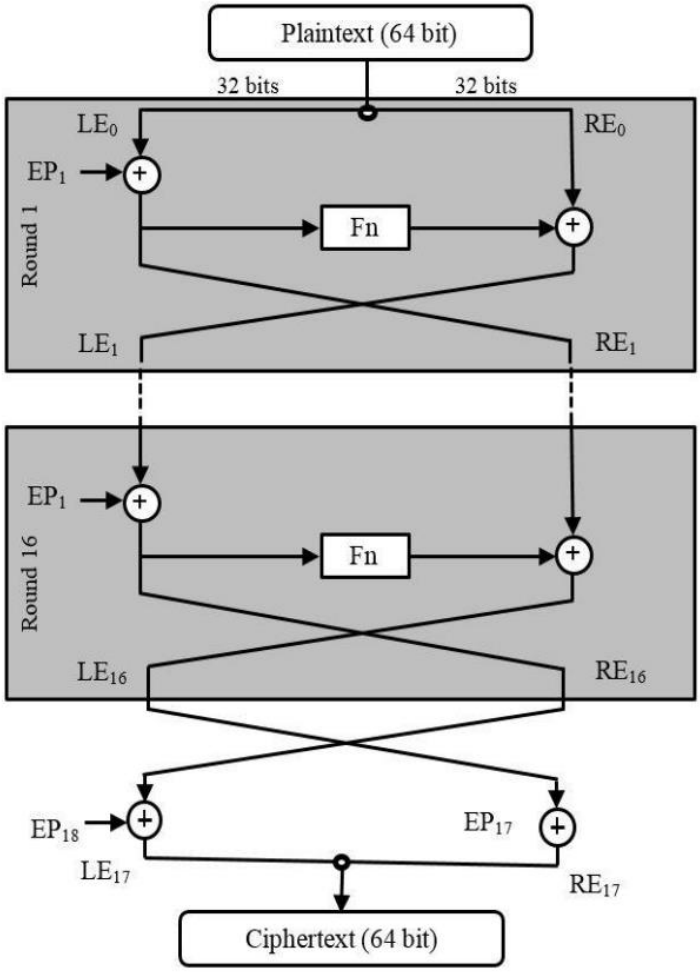

FIG. 4. RSA ALGORITHM A DIAGRAM OF THE BLOWFISH ENCRYPTION ALGORITHM [21].

E. RSA

Rivest, Shamir, and Adelman (RSA) created an asymmetric cryptographic algorithm. Since its debut in 1977, RSA a public key cryptosystem has seen extensive use. These three people are generally regarded as its progenitors. It produces two keys, one public for use in encrypting messages and another, private, for decrypting them at a later time. The public key is used for encrypting messages. The RSA algorithm has three distinct phases: the first is key generation, where a secret key is created and stored; the second is the actual encryption process, where plaintext is transformed into cipher text; and the third is decryption, where the reverse process, from encrypted text to plaintext, is performed. The initial process of the RSA algorithm is key generation. Finding the product of two large prime integers, often known as the factoring problem, is essential to the RSA method as shown in *Fig. 5*. There is some leeway in the key size, which can be between 1024 and 4096 bits [31].

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

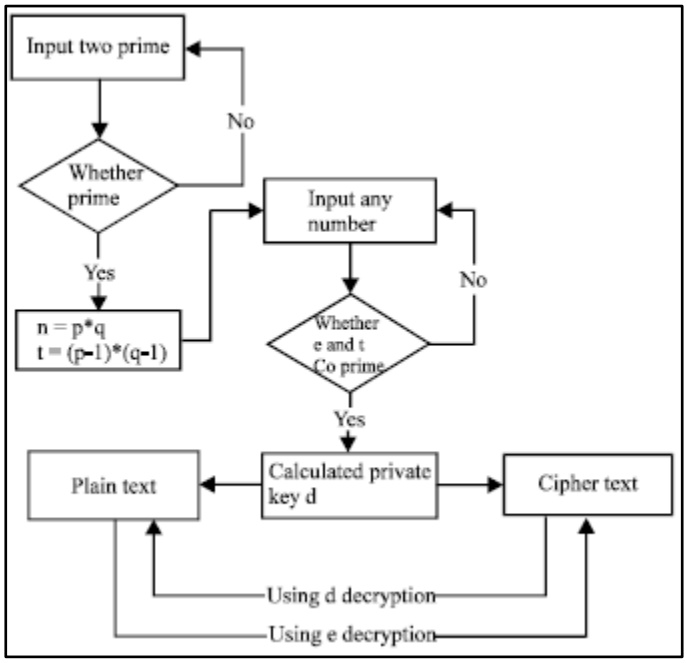

FIG. 5. RSA ALGORITHM [32].

IV. IMPLEMENTATION

The researchers have evaluated the level of protection offered by DES, 3DES, AES, blowfish, and RSA respectively. Python was utilized throughout the process of developing the algorithms. Capabilities such as encryption, decryption, key generation, infrastructure for key management, authentication, and authorization are all components of the whole picture. The encryption procedure used text files and image files of varied sizes as its input data (25 KB, 50 KB, 1 MB, 2 MB, 3 MB, and 4 MB). At the outset of decryption, the results of decrypting each encrypted file are written to individual files. This document serves as an input for the procedure. To facilitate a fair comparison of findings. The researchers have been utilizing the same setup for all of the implementation and analysis work to ensure that all of the algorithms being compared are being tested under identical memory and CPU conditions. All block cipher algorithms in built-in cryptography and security features are configured by default to use the same mode, dubbed ECB. When working with encrypted data, this mode is utilized both for encryption and decryption. To generalize, executing encryption and decryption requires creating a cipher object with the parameter's algorithm name and mode, initializing the cipher you created for encryption and decryption, and then calling the doFinal() function. To generate the key, use the class's built-in method.

V. EVALUATION PARAMETERS

There are many various techniques to encrypt data, each with its own set of advantages and disadvantages. Understanding the merits and limitations of different cryptographic algorithms is essential before applying any of them to a given application. This means these algorithms need to be evaluated again while considering a broader set of criteria. The

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

following measures are used in this work to compare different cryptosystems, and their respective explanations are provided below [10]:

A. Encryption Time

The time taken by an encryption algorithm to convert plaintext to ciphertext is known as the encryption time. How long it takes to encrypt a file depends on several factors, including the size of the key, the size of the plaintext block, and the mode. The research led to conclude that the amount of time needed for encryption can be expressed in milliseconds. How long it takes to encrypt data has an effect on how quickly the system responds. The time spent encrypting data must be reduced so that the system can process requests quickly.

B. Decryption Time

The time taken by a decryption algorithm to convert ciphertext to plaintext is known as the decryption time. How long it takes to encrypt a file depends on several factors, including the size of the key, the size of the ciphertext block, and the mode. Our research led us to conclude that the amount of time needed for decryption can be expressed in milliseconds. How long it takes to decrypt data has an effect on how quickly the system responds. The time spent decryption data must be reduced so that the system can process requests quickly.

C. Memory Used

The amount of RAM needed to implement various encryption methods varies. This memory need is conditional on the number of operations to be performed by the algorithm, the key size to be used, the initialization vectors to be used, and the types of operations to be performed. The overall price tag is affected by the available RAM. Minimizing the amount of RAM needed is a top priority.

D. Avalanche Effect

Diffusion is a property used in cryptography that provides insight into an algorithm's cryptographic strength. Small changes in the input can have a big effect on the output, thus keeping an eye on it is crucial. The researchers determined the avalanche effect by measuring the pounding distance. For purposes of information theory, a distance metric known as the Hamming distance is commonly employed. Easy software implementation leads us to utilize a method that calculates the hamming distance by adding bit-by-bit xors while accounting for the ASCII value. One benefits from having a large quantity of avalanche effect, which is the same as having a large amount of diffusion. The effectiveness of the encryption technique is mirrored in the avalanche effect [33].

Avalanche effect = (hamming distance ÷ file size) (1)

E. Entropy

Cryptographic techniques rely heavily on randomness, as this guarantees that information cannot be extracted by an opponent. For this reason, randomization is a mandatory attribute. One interpretation of entropy is that it is a means to put a numerical value on how random something is. It determines the extent to which one can trust the data presented. To ensure the safety of confidential data, we need security algorithms that can create a substantial quantity of randomness for use in encrypted messages. As a result, the interdependence between the key and the ciphertext is minimized or eliminated altogether. When there is a lot of noise in the system, the connection between the key and the

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

ciphertext gets complicated. This quality is sometimes referred to as confusion in some circles. It is desirable to have a high degree of confusion so that it is difficult for an attacker to make educated assumptions. This will make it more difficult for the attacker. Entropy is a measurement of how well a cryptographic technique works. Encryption algorithms are used to keep information secure [34], [35]. In order to calculate the entropy of a system, The researchers make use of Shannon's formula.

F. Number of Bits Required for Encoding Optimally

Decrease the number of bits needed to encode a character in a secret message. There is no getting around the fact that this needs to be completed. This metric provides us with a rough estimate of the necessary bandwidth for transmission by factoring in the fact that the encrypted bit will be delivered across a network after the encoding process has concluded. When encrypted data is encoded with fewer bits, its transmission and storage overheads are reduced. That's why it makes a difference to the final cost.

VI. RESULTS AND DISCUSSIONS

In this part of the article, we will talk about the findings that were acquired based on a total of six different evaluation criteria. Table I presents a comparison of symmetric and asymmetric algorithms based on a range of criteria, such as the length of the key, the size of the blocks, the number of rounds, the amount of power consumed, the avalanche effect, the amount of processing time, and the resources used.

TABLE I. PARAMETER-BASED EVALUATION OF SEVERAL ALGORITHMS

PARAMETERS	DES	3DES	AES	RSA	BLOWFISH
DEVELOPMENT	IBM in 1970.	IBM in 1978.	Vincent Rijmen, Joan Daeman in 2001	Ron Rivest, Shamir & Leonard Adleman in 1978	Bruce Schneier in 1993
KEY LENGTH	64 (56 usable)	168,112	128,192, 256	Key length depends on no. of bits in the module	Variable key length i.e. 32 – 448
ROUNDS	16	48	10,12,14	1	16
BLOCK SIZE	64	64	18	Variable block	64
ATTACKS FOUND	Exclusive Key search, Linear cryptanalysis, Differential analysis	Related Key attack	Key recovery attack, Side channel attack	Brute force attack, timing attack	No attack is found to be successful against blowfish.
LEVEL OF SECURITY	Adequate security	Adequate security	Excellent security	Good level of security	Highly secure
ENCRYPTION SPEED	Very slow	Very slow	Faster	Average	Very fast

A. Encryption Time

Fig. 6 indicates that encrypting data using the RSA method takes the most amount of time, whereas encrypting data with the blowfish algorithm takes the least amount of time and is the most effective. Both algorithms are shown to be used to encrypt data. The procedure that is commonly referred to as 3DES makes it possible to reuse DES implementations. This is performed by chaining together three separate instances of DES, each of which uses a different key. It is generally accepted that 3DES will

Received 05/January/2023; Accepted 19/February /2023
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

remain secure at least until the year "2112," although the performance of the security protocol diminishes when it is applied to software applications. This is due to the fact that the protocol was created for successful hardware implementation. In comparison to the other possibilities, the task can be completed by blowfish in the shortest amount of time. Blowfish is the name of an effective encryption technique for software that can be implemented on at least some different software platforms. Its performance is dependent on the capabilities of the platform with relation to memory management and cache storage because it uses key-dependent lookup tables.

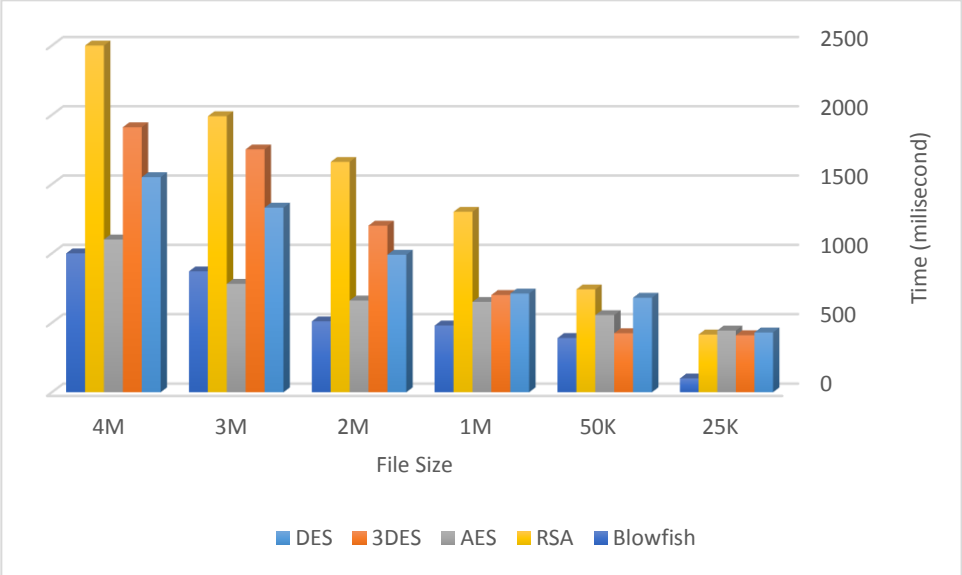

FIG. 6. COMPARISON OF DES, 3DES, AES, BLOWFISH, AND RSA ENCRYPTING TIMES AND FILE SIZES.

B. Entropy

As can be seen in Table II , the Blowfish algorithm yields the greatest average entropy score for each byte of encrypted data that it produces. Entropy can be thought of as a measurement of how random something is, which is one way to think about it. This is relevant with regard to the amount of entropy that information possesses. The capacity of cryptographic algorithms to produce random data is a characteristic that is not only required but also highly desirable. Blowfish makes use of the round function on both the s-array and the p-array, whereas AES places a significant emphasis on the utilization of both s boxes and p boxes. As a consequence of this, the information that is generated by AES and Blowfish contains a high degree of unpredictability. The purpose of encrypting information in the first place is to make it less susceptible to being attacked, and this accomplishes that aim in a way that was not possible before.

TABLE II. THE VALUES OF ENTROPY

	DES	3DES	AES	Blowfish	RSA
Mean Entropy of Encrypted Bytes	2.9477	2.9477	3.84024	3.93891	3.0958

C. Decryption Time

Fig. 7 demonstrates that the amount of time required to decrypt data is always going to be less than the amount of time required to encrypt the data. This is the case regardless of the complexity of the encryption algorithm. The decryption procedure that uses RSA requires the maximum amount of time, whereas the one that uses blowfish requires the least amount of time and is, as a result, the most

Received 05/January/2023; Accepted 19/February /2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

effective. Utilizing prime numbers, RSA, which is a public-key cryptosystem, uses a one-way function that is difficult to reverse. This is made possible by the usage of prime numbers. Because of this, it is incredibly secure. RSA is a fairly slow approach when compared to symmetric key algorithms because it involves modular exponentiation, multiplicative inverse, and both a public and a private key. In addition, it requires a public and a private key. This is due to the fact that it employs both a public key and a private key simultaneously.

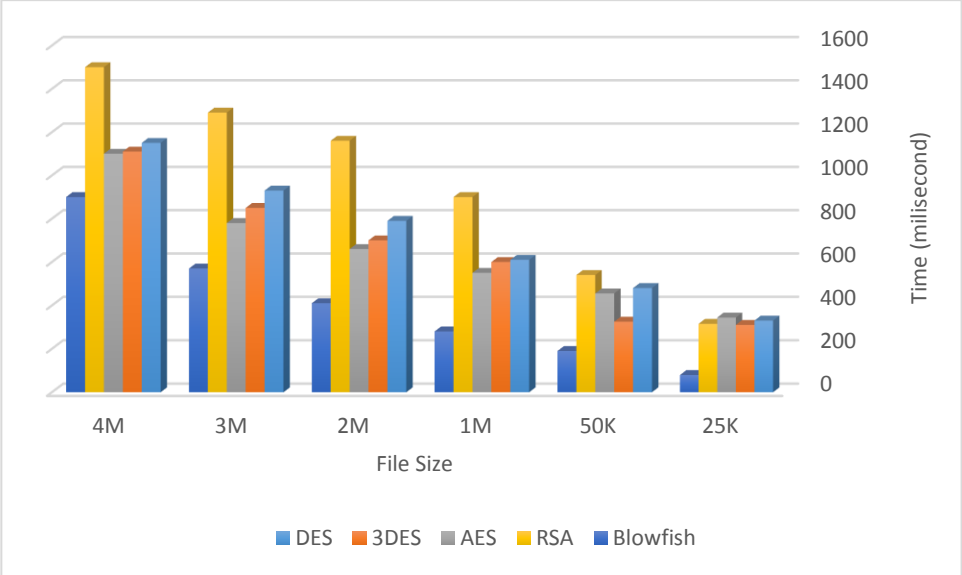

FIG. 7. COMPARISON OF DES, 3DES, AES, BLOWFISH, AND RSA DECRYPTION TIMES VERSUS FILE SIZES.

D. Memory Used

The information that was gathered regarding the amount of memory that was used by the unit operations of the outlined algorithms can be found shown in Table III. In contrast, the memory consumption rate for RSA is the highest, while the memory consumption rate for Blowfish is the lowest. RSA has the highest memory consumption rate per unit of operation. When working with either DES or AES, you'll need a memory size that falls somewhere in the middle. Therefore, the Blowfish algorithm is the best choice that can be made in this circumstance if the requirement of any application is for the smallest memory capacity that is still practicable.

TABLE III. MEMORY USAGE COMPARISON

Algorithm	Memory Used(KB)
DES	16.3
3DES	15.5
AES	14.7
Blowfish	13.6
RSA	19.58

E. Avalanche Effect

As can be observed in *Fig. 8*, the avalanche impact of the AES method is the most significant, whereas the avalanche impact of the RSA algorithm is the least significant. The avalanche effect can be used to gain some understanding of the extent to which information is propagated. A modification

Received 05/January/2023; Accepted 19/February /2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

to a single bit in the plaintext that results in a significant shift in the bits of the information that are produced as a direct consequence of the modification. The Advanced Encryption Standard, also known as AES, employs a multiplicative inverse network and an affine network to carry out transformations over a galois field in order to conduct affine and substitution permutation operations. The utilization of a substitution permutation network is what brings about this successful outcome. As a consequence of this, there is a significant amount of information mixing, which, in turn, results in a significant amount of output diffusion.

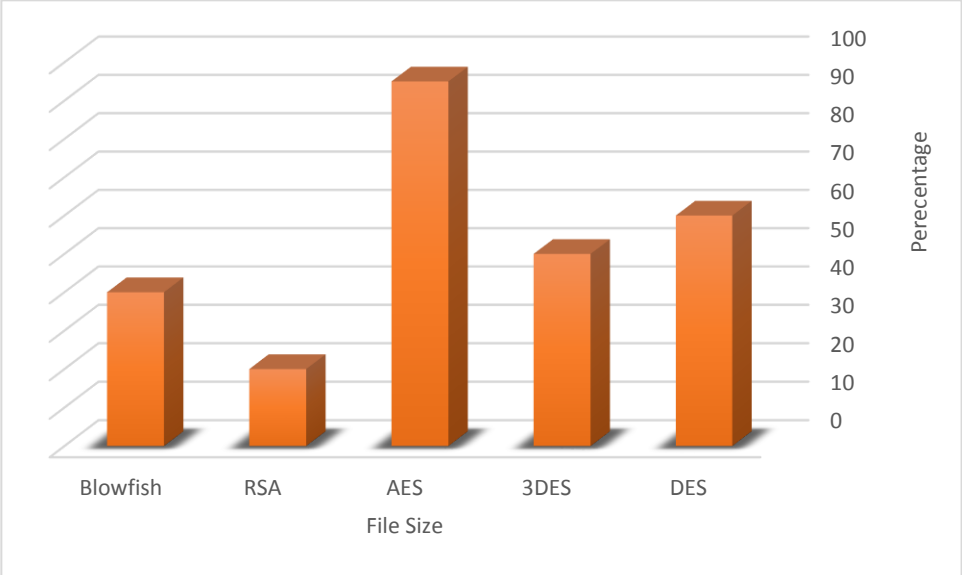

FIG. 8. AVALANCHE EFFECT FOR DES, 3DES, AES, BLOWFISH AND RSA.

F. Number of Bits Required to Encode Optimally

Table IV shows that for efficient encryption encoding, AES requires the most bits, whereas DES requires the fewest. Table IV suggests that the maximum possible bandwidth is required for transmission when using the Advanced Encryption Standard.

TABLE IV. OPTIMAL LENGTH FOR ENCODING

	DES	3DES	AES	Blowfish	RSA
Average amount of bits needed to encrypt a byte	25	38	256	128	42

VII. CONCLUSIONS

There are many various techniques to encrypt data, each with its own set of advantages and disadvantages. Understanding the merits and limitations of different cryptographic algorithms is essential before applying any of them to a given application. The experimental results show that compared to implementing AES, blowfish requires significantly less memory. Both DES and 3DES call for a medium amount of memory. Since the results show that RSA takes more time than other algorithms while encrypting and decrypting data, Blowfish is the best alternative for any application that needs the least amount of memory space. A blowfish can be caught in the shortest amount of time compared to other. Parameter avalanche effect evaluations showed that AES was the most secure method, leading us to conclude that it should be used anywhere strict confidentiality and integrity must be maintained. Exemplifying the Blowfish has the highest entropy score when compared to DES, 3DES, AES, and RSA; this suggests that it is also the most secure against attacks. The results indicate that

Received 05/January/2023; Accepted 19/February /2023

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

when it comes to encoding encrypted data, the Data Encryption Standard requires the fewest number of bits conceivable, whereas the Advanced Encryption Standard requires the greatest number of bits imaginable. This indicates that when transmitting data, AES requires the use of all available bandwidth. Blowfish is the perfect method to use when running time and memory are both significant considerations for a certain application, as it provides a higher level of security at a faster encryption speed than any other algorithms . Therefore, based on the research and evaluation conducted, the Blowfish encryption algorithm is the superior choice in terms of security and efficiency. However, when the available network bandwidth is the primary issue of the application, DES is the ideal approach to use.

REFERENCES

[1] A. M. R. Ibrahim ALattar, "A Comparative Study of Researches Based on Magic Square in Encryption with Proposing a New Technology," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 21, no. 2, pp. 102–114, 2021, [Online]. Available: https://ijccce.uotechnology.edu.iq/article_169704.html.

[2] T.W. Khairi, "Framework For Modeling and Simulation of Secure Cloud Services," Iraqi Journal of Computers, Communications, Control and Systems Engineering, vol. 22, no. 1, 2022.

[3] A. A. Zainab Muneef Hala bahjat, "Image Encryption Paillier Homomorphic Cryptosystem," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 21, no. 4, pp. 29–36, 2021, doi: https://doi.org/10.33103/uot.ijccce.21.4.3.

[4] Y. Kumar, R. Munjal, and H. Sharma, "Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures," IJCSMS International Journal of Computer Science and Management Studies, 2011.

[5] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A Comparative Analysis for Modern Techniques," International Journal of Advanced Computer Science and Applications, vol. 8, no. 6, 2017, doi: 10.14569/ijacsa.2017.080659.

[6] S. Gautam, S. Singh, and H. Singh, "A Comparative Study and Analysis of Cryptographic Algorithms: RSA, DES, AES, BLOWFISH, 3-DES, and TWOFISH," INTERNATIONAL JOURNAL OF RESEARCH IN ELECTRONICS AND COMPUTER ENGINEERING, vol. 7, no. 1, 2019.

[7] M. Harini, K. P. Gowri, C. Pavithra, and M. Pradhiba Selvarani, "COMPARATIVE STUDY AND ANALYSIS OF VARIOUS CRYPTOGRAPHIC ALGORITHMS," Int J Sci Eng Res, vol. 8, no. 5, 2017.

[8] S. B. Et. al., "A Comprehensive Survey on Cryptography Evaluation in Mobile (MANETs)," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 2, 2021, doi: 10.17762/turcomat.v12i2.2402.

[9] T. F. G. Quilala and R. L. Quilala, "Modified blowfish algorithm analysis using derivation cases," Bulletin of Electrical Engineering and Informatics, vol. 10, no. 4, 2021, doi: 10.11591/EEI.V10I4.2292.

[10] A. L. Jeeva, D. v Palanisamy, and K. Kanagaram, "Comparative analysis of performance efficiency and security measures of some encryption algorithms," International Journal of Engineering Research and Applications (IJERA) ISSN, vol. 2, no. 3, 2012.

[11] A. Singh, M. Marwaha, B. Singh, and S. Singh, "Comparative Study of DES, 3DES, AES and RSA," INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, vol. 9, no. 3, 2013, doi: 10.24297/ijct.v9i3.3342.

[12] R. Tripathi and S. Agrawal, "Comparative Study of Symmetric and Asymmetric Cryptography Techniques," International Journal of Advance Foundation and Research in Computer (IJAFRC), vol. 1, no. 6, 2014.

[13] M. S. Mahindrakar, "Evaluation of Blowfish Algorithm based on Avalanche Effect," International Journal of Innovations in Engineering and Technology, vol. 4, no. 1, 2014.

[14] V. David, H. Ragu, V. Nikhil, and P. Sasikumar, "Analysis of Algorithms for Effective Cryptography for Enhancement of IoT Security," in Lecture Notes in Networks and Systems, 2023, vol. 396, pp. 91–99. doi: 10.1007/978-981-16-9967-2_10.

[15] G. L. Dulla, B. D. Gerardo, and R. P. Medina, "An enhanced blowfish (eBf) algorithm for securing x64FileMessage content," in 2018 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment and Management, HNICEM 2018, 2019. doi: 10.1109/HNICEM.2018.8666434.

[16] A. R. L. Reyes, E. D. Festijo, and R. P. Medina, "Blowfish-128: A modified blowfish algorithm that supports 128-bit block size," in Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering, WCSE 2018, 2018. doi: 10.18178/wcse.2018.06.097.

Received 05/January/2023; Accepted 19/February /2023

 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.23.3.11

[17] V. S. Shetty, R. Anusha, K. Dileep, and P. Hegde, "A Survey on Performance Analysis of Block Cipher Algorithms," in Proceedings of the 5th International Conference on Inventive Computation Technologies, ICICT 2020, 2020. doi: 10.1109/ICICT48043.2020.9112491.

[18] J. B. Awotunde, A. O. Ameen, I. D. Oladipo, A. R. Tomori, and M. Abdulraheem, "Evaluation of four encryption algorithms for viability, reliability and performance estimation," Nigerian Journal of Technological Development, vol. 13, no. 2, 2017, doi: 10.4314/njtd.v13i2.5.

[19] S. D. Rihan, A. Khalid, and S. E. F. Osman, "A Performance Comparison of Encryption Algorithms AES and DES," International Journal of Engineering Research & Technology, vol. 4, no. 12, 2015.

[20] Ahmed Khalid and S. D. Rihan, "A Performance Comparison of Encryption A Performance Comparison of Encryption Algorithms AES and DES," International Journal of Engineering Research & Technology (IJERT), vol. 4, no. November, 2017.

[21] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, "A Survey on the Cryptographic Encryption Algorithms," International Journal of Advanced Computer Science and Applications, vol. 8, no. 11, 2017, doi: 10.14569/ijacsa.2017.081141.

[22] K. S and M. A, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System," International Journal of Scientific Engineering and Research (IJSER), vol. 2, no. 11, 2014.

[23] H. M. Fadhil, "Accelerating Concealed ISB Steganography and Triple-DES Encryption using Massive Parallel GPU," J Appl Sci Res, vol. 13, no. 3, pp. 17–26, Mar. 2017.

[24] Dr. S. Y. AMEEN, "SECURITY SERVICES PROVISION AND ENHANCEMENT IN CLIENT/SERVER NETWORKS USING AES," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 5, no. 1, pp. 42–57, 2005, [Online]. Available: https://ijccce.uotechnology.edu.iq/article_65592.html.

[25] A. F. Sameeh Jassim, "Designing a New Lightweight AES Algorithm to Improve the Security of the IoT Environment," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 22, no. 2, pp. 96–108, 2022, doi: https://doi.org/10.33103/uot.ijccce.22.2.9.

[26] S. M. Soliman, B. Magdy, and M. A. Abd El Ghany, "Efficient implementation of the AES algorithm for security applications," in International System on Chip Conference, Jul. 2016, vol. 0, pp. 206–210. doi: 10.1109/SOCC.2016.7905466.

[27] J. A. Mahdi, "Design and Implementation of Proposed B-R Encryption Algorithm," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 9, no. 1, pp. 34–50, 2009, [Online]. Available: https://ijccce.uotechnology.edu.iq/article_45841.html.

[28] A. T. H. Janan A. Mahdi Saleh M. Al-Qarrawy, "Design and Implementation of an Improvement Of Blowfish Encryption Algorithm," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 9, no. 1, pp. 95–109, 2009, [Online]. Available: https://ijccce.uotechnology.edu.iq/article_45854.html.

[29] P. Chnadra and M. A. Prof, "Superiority of Blowfish Algorithm," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 9, 2012.

[30] T. S. Algaradi and B. Rama, "A novel blowfish based-algorithm to improve encryption performance in hadoop using mapreduce," International Journal of Scientific and Technology Research, vol. 8, no. 11, 2019.

[31] M. Preetha and M. Nithya, "A Study and Performance Analysis of RSA Algorithm," International Journal of Computer Science and Mobile Computing, vol. 2, no. 6, 2013.

[32] N. Qi et al., "Analysis and research of the RSA algorithm," Information Technology Journal, vol. 12, no. 9, 2013, doi: 10.3923/itj.2013.1818.1824.

[33] A. T. H. Salma H. Abdullah Janan A. Mahdi, " A Proposed 512 bits RC6 Encryption Algorithm," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 10, no. 1, pp. 11–25, 2010, [Online]. Available: https://ijccce.uotechnology.edu.iq/article_45900.html.

[34] A. A.-S. Hiba Yaseen, "Load Balancing and Detection of Distributed Denial of Service Attacks Using Entropy Detection," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 21, no. 4, pp. 60–73, 2021, doi: https://doi.org/10.33103/uot.ijccce.21.4.6.

[35] M. K. Huda Abd UL Sahib, "Comparison of Three Proposal Methods in Steganography Encryption Secret Message using PVD and MapReduce," IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 21, no. 2, pp. 115–131, 2021, [Online]. Available: https://ijccce.uotechnology.edu.iq/article_169705.html.

Received 05/January/2023; Accepted 19/February /2023

 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*