https://dx.doi.org/10.4314/dujopas.v10i4b.16
ISSN (Print): 2476-8316
ISSN (Online): 2635-3490
Dutse Journal of Pure and Applied Sciences (DUJOPAS), *Vol. 10 No. 4b December 2024*

Indepth Analysis of Various Cryptography Techniques

Auyo SG[1], Yushau A[2], Yabo AS[3], Faskari MH[4], Babandi U[5], Ibrahim AA[6], Abdullahi MI[7], Marafa AI[8]

[1, 2, 5, and 7] Department of Computer Science
Jigawa State Polytechnic

[3] Department of Computer Science
Umaru Ali Polytechnic
Sokoto.

[4] Department of Computer Science
Federal University of Agriculture, Zuru

[6] Department of Information Technology
Federal University Dutse

[8] Department of Business Administration and Management
Kebbi State Polytechnic Dakin Gari

Email: Salihuauyo@gmail.com

Abstract
In an increasingly digital world, cryptography is essential to guaranteeing the security, privacy, and integrity of data. Even if cryptographic techniques have advanced significantly, the increasing complexity of cyber threats calls for a deeper comprehension of these approaches in order to improve data protection. This study conducts a thorough analysis of a number of cryptographic methods, including symmetric algorithms like AES, DES, Blowfish, and 3DES as well as asymmetric strategies like RSA, RC6, ECC and Diffie-Hellman. Critical characteristics like encryption and decryption time, throughput, power consumption, memory utilisation, and security resilience are all evaluated in this study. Through simulation-based experiments and a thorough analysis of the body of current literature, the study determines the strength and weakness of each method in various contexts, such as cloud computing systems, multimedia, and text files. This study discovered a striking pattern in the areas of previous research. For the most part, researchers have focused on analysing the encryption and decryption times of popular algorithms like DES, 3DES, Blowfish, and AES. Because of their historical significance, broad use, and vital function in protecting data in a variety of applications, these algorithms have drawn a lot of attention. They are now among the most studied cryptographic algorithms to date because of the abundance of information gathered on their performance measures as a result of this intense focus.
The RC6, RC4, RC2, ECC, and D-H algorithms, on the other hand, have received relatively little attention.

Keywords: Cryptography, Data Security, Public key, Resource Usage, Secret Key

INTRODUCTION
In order to keep data safe from hackers, security is crucial. Cryptography is one of the most crucial techniques for guaranteeing data confidentiality (Vegesna, 2019). Secret writing for

Author for Correspondence

data security protection is known as cryptography. Data that is well-hidden is difficult to read, alter, or falsify. Important information is protected by cryptography, which transforms it into ambiguous information that only authorised recipients may access. The authorised receivers then transform the ambiguous information back into the original text. Encryption is the process of converting original text into cryptic text (ciphertext) using a specific key; decryption is the process of doing the opposite (Salem, 2023).

The control of privacy and security poses difficulties for e-examination. Reliability and security are essential for an e-exam database (Fluck, 2019). Therefore, it is necessary to verify the identity of an e-exam user. Significant issues like hacking and leakage are common with computerized tests. Encrypting the database's internal questions is one way to solve the problem. The process of transforming plaintext into unintelligible text is called encryption (Sunday and Olufunminiyi, 2023).

Asymmetric cryptography, which uses both public and private keys to encrypt and decrypt data, and symmetric cryptography, which uses the same key to encode and decode data, are the two basic methods for data encryption (Al-shabi, 2019).

Blowfish, Triple-DES (3DES), Advanced Encryption Standard (AES), and Data Encryption Standard (DES) are a few examples of symmetric algorithms. Both RSA and ELGAMAL Schema are the most well-known asymmetric algorithms.

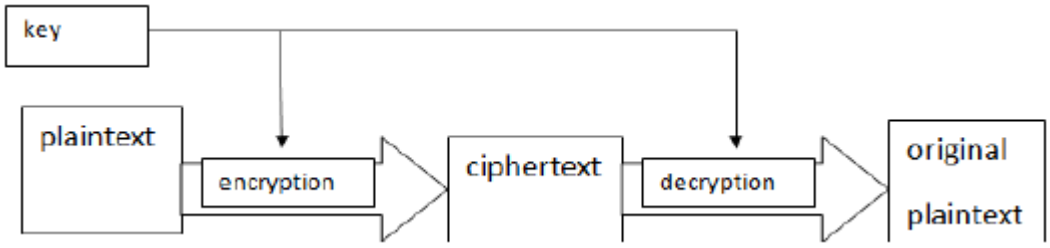


Figure 1: Symmetric Cryptosystem
Source: Alemami *et al.*, (2019)

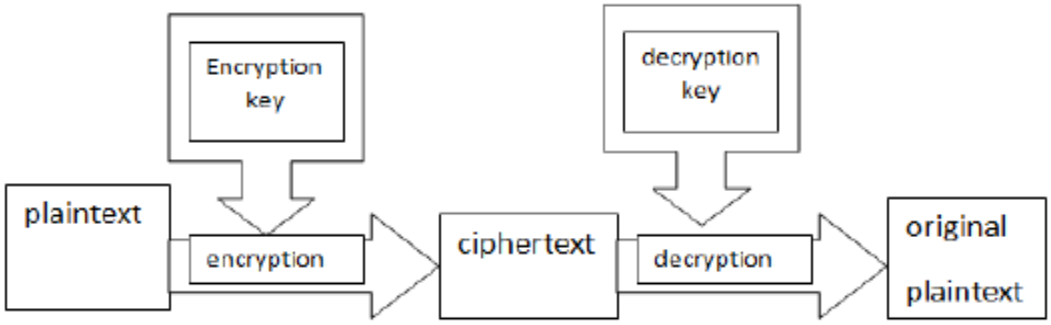


Figure 2: Asymmetric Cryptosystem
Source: Al-shabi, (2019)

This study fills in the gaps in the literature, which mostly concentrates on well-known algorithms like AES and DES while under-examining methods like RC4, RC6, Diffie Hellman and ECC. Additionally, it looks at the limited assessment of hybrid models, the effect of key size, and algorithm performance in environment such as .NET and cloud computing. This study fills a knowledge gap by offering a thorough examination of the effectiveness, security,

and practicality of a variety of cryptographic techniques in many different kinds of environments.

Why Cryptography is used

Authentication: A system's ability to verify the sender's identity.
Maintaining confidentiality means that only authorized parties should be able to access information that has been transmitted (Nandy *et al.,* 2019).
Integrity: Transmitted information can only be changed by authorized persons.
The assurance that something cannot be denied is known as non-repudiation.
Access control ensures that only those who are authorized can access the information provided (Mohammed *et al.,* 2024).

Assessment Criteria

Research by Panahi *et al.,* (2021) argued that, the following are the description of some of the parameters that affect encryption performance.

i. Time of encryption: Depending on the length of the key and data block, it is measured in milliseconds. It has a direct impact on how well the encryption technique performs. When an algorithm's encryption time is quick, it is considered to have advanced performance.
ii. Decryption time: Also expressed in milliseconds, this is the amount of time needed to recover the original text from the ciphertext. When an algorithm's decryption time is quick, it is considered to be performing better.
iii. Memory utilization: Because it impacts system cost, low memory usage is preferred.

Cryptography Algorithms

To determine the optimal encryption schemes based on several characteristics, this section explains a variety of encryption algorithms.

S-DES, or the Simplified Data Encryption Standard

The following are the steps that make up the S-DES algorithm:
Generation of S-DES keys: S-DES depends on the use of a 10-bit shared key that is shared between the sender and the recipient. As shown in Fig. 3, this key is used to generate a pair of 8-bit subkeys (K1, K2) for use in particular phases of the encipherment and decipherment procedures (Alemami *et al.*, 2019).

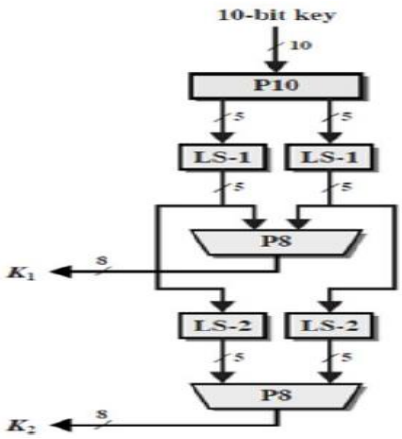


Figure 3: SDES Key Generation
Source: Alemami *et al.,* (2019)

DES Data Encryption Standard

The first symmetric encryption algorithm, DES, was first presented by International Business Machines Corporation in 1972. The National Bureau of Standards agreed to adopt it as a Federal Information Processing Standard in 1977. It uses a preliminary permutation to process a 64-bit input and follows the same procedures as S-DES. S-DES has two rounds and uses eight bits for input, whereas DES has sixteen rounds (Wu and Dai 2020).

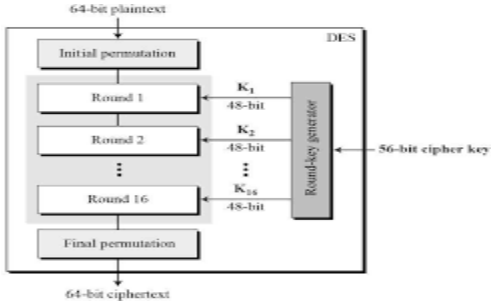


Figure 4: DES Round of Cryptosystem
Source: Wu and Dai (2020)

Triple DES (3DES)

International Business Machines Corporation, or IBM, proposed 3DES in 1998. DES can be replaced with 3DES, which uses the DES algorithm three times for every data block and has a larger key size. For the 3DES, the block length is 64 bits, the number of rounds is 48, and the key length is 112 and 168 bits. This algorithm's greater key size than DES is intended to improve security and protection. When used for the encryption process, it takes longer than DES, though (Alabdulrazzaq and Alenezi 2020)

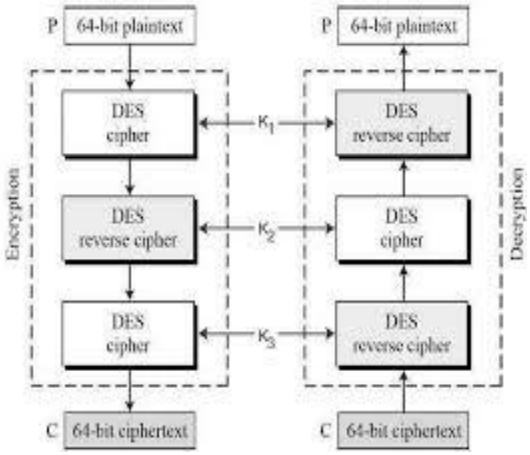


Figure 5: 3DES Cryptosystem
Source: Alabdulrazzaq and Alenezi (2020)

The Blowfish

Schneier B created the symmetric block cipher known as Blowfish in 1993. Blowfish is an unpatented, license-free, and quick algorithm. It employs a 64-bit block and a key length between 32 and 448. For the encipherment process, the Blowfish algorithm uses 16 rounds (Fig. 6). Typically, Blowfish uses four S-boxes instead of just one. Because it depends on key length, it takes longer to process, but it offers good security (Singhal *et al.,* 2022).

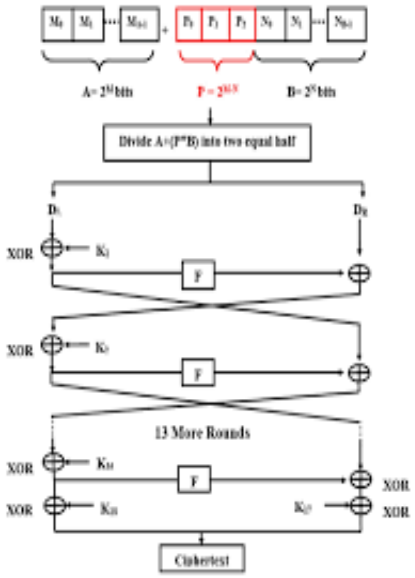
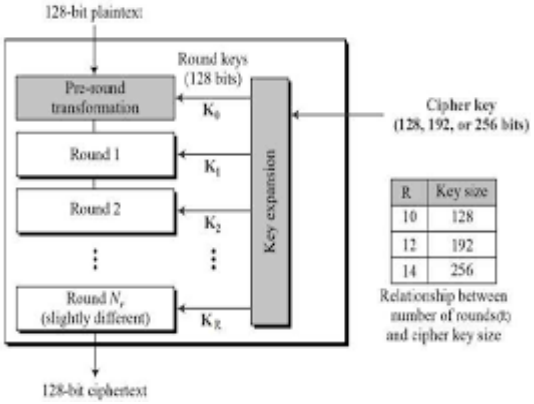


Figure 6: Blowfish Round of Cryptosystem
Source: Singhal *et al.*, (2022)

Advanced Encryption Standard (AES)

Advanced Encryption Standard (AES) AES, also known as "Rijandael," is a block cipher with a block size of 128 bits. The algorithm is called AES-128, AES-192, or AES-256 depending on the key size. Each round consists of four layers, specifically replacement byte, shift rows, blend column, and add round key, as shown in Fig. 7. For 128-bit keys, the encipherment consists of ten rounds of processing, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys (Rao *et al.*, 2021).



R	Key size
10	128
12	192
14	256

Figure 7: AES Algorithm
Source: Rao *et al.*, (2021)

Cryptographic Algorithms in Comparison for Data Security and Effectiveness in Modern Applications

The integrity and confidentiality of all data transmitted between the web server and the browser are ensured by a secure socket layer (SSL) channel. Authentication, privacy, encryption, and confidentiality are all necessary for the systems used in e-learning, which includes e-exams (Alemami 2019).

RSA techniques are used for both encrypting and decrypting data using the Diffie-Hellman key. Furthermore, Diffie-Hellman and RSA are said to be strong enough for business use.

RSA, DES, AES, and elliptical curve cryptography can all be used with the Diffie-Hellman key to encrypt and decrypt messages (Schwenk 2022). In this paper, the most widely used encryption and decryption algorithms AES, DES, 3DES, and Blowfish are compared side by side.

According to the simulation results, out of all the encryption algorithms utilized, 3DES performs the best when combined with Electronic Codebook (ECB) and Cypher Blocker Chaining (CBC). Additionally, a performance evaluation of a few chosen symmetric encipherment algorithms AES, DES, 3DES, Blowfish, RC2, and RC4 is carried out. Battery and time consumption increase with key size length (Pramanik *et al.,* 2019). The areas of encryption and decryption utilizing the DES, AES, and RSA algorithms have been examined and studied in several research. These algorithms are expected to be used for improved and safe communication in the future (Kudair *et al.* 2023). It is suggested to use ASCII algorithms for encryption and decryption. This new approach is dependable, secure, quick, and efficient.

The following is how this algorithm is used: A subset of starting and ending integers is produced using any random number; a modulus is then chosen, and the subset is then divided by mode; the remainder is the substitution array (Sanders *et al.* 2019).

Before transmitting data to the cloud, a basic data protection model based on the AES algorithm and Diffie-Hellman is suggested. The analysis's findings indicate that the proposed method outperforms the Diffie-Hellman and AES algorithms in terms of speed. Due to its combination of both algorithms' properties, the suggested approach is extremely safe for cloud computing (Ametepe *et al.,* 2022). However, research by Alabdulrazzaq and Alenezi (2022) different data sets are used to test the current encryption and decryption techniques (AES, Blowfish, DES, and 3DES). The results of the simulation show that the Blowfish method performs the best out of all the algorithms that were compared and that the best encryption solutions may be obtained by combining the public and secret keys. The goal of this strategy is to benefit from both the speed aspects of private key systems and the safety advantages of public key systems (Karanam et al. 2023).

Kudair *et al.* (2023) DES, 3DES, and RSA algorithms, in particular, are evaluated based on criteria such as memory utilization and encryption time. The entire encrypted plaintext is divided by the total encipherment time for each algorithm to get the throughput. For simulation, ASP.NET and Java are utilized. The findings of Schwenk (2022) demonstrate that DES encryption is twice as fast as RSA encryption and uses less power. Despite this, 3DES takes longer than DES, uses more power, and has lower throughputs. In terms of throughput and power consumption, the DES algorithm outperforms the other methods. To solve the security issues with cloud storage, a method that combines AES and Blowfish is suggested. The login page uses the Blowfish technique to protect user names and passwords. The Blowfish algorithm is used at the first level when a file is uploaded and stored on the cloud, and the AES method is used at the second level to encrypt data. The AES method is used at the first level of the file download, and the Blowfish algorithm is used at the second level to decrypt the data. A great level of security is provided by multilevel encryption (Sinha *et al.* 2020). Table 1 below, depict summary of reviewed literature in terms performance and security in various applications

Table 1: Assessment of Cryptographic Algorithms Performance and Security in Various Applications and Environments

Reference	Evaluation Parameter	Compared Algorithm	Findings	Domain
Schwenk (2022).	1. Security	1. RSA 2. Diffie-Hellman 3. Both RSA and Diffie-Hellman	Elliptical Curve Cryptography, RSA, DES, and AES can all be used with the Diffie Hellman Key. When RSA and Diffie-Hellman are combined, the results can be more robust than when they are used alone.	Text file
Alabdulrazzaq and Alenezi (2022).	1. Security 2. Encryption Time	1. DES 2. 3DES 3. AES 4. Blowfish	Better performance is achieved when 3DES is used with ECB and CBC.	Simulation in .Net Classes
Ametepe *et al.,* (2022)	1. Encryption Time 2. Security	1. AES 2. Diffie-Hellman	The suggested technique, which combines Diffie Hellman and AES, performs better in terms of security and encryption time.	Cloud Computing
Rameel and Asif (2024).	1- Throughput 2- Encryption time 3- Decryption time 4- Power consumption 1.	DES 2- 3DES 3- AES 4- BLOWFISH 5- RC6 6- RC2	Compared to its rivals, Blowfish performs better.	Audio files Video files Text files
Chen *et al.,* (2020)	1. Encryption Time	1- DES 2- BLOWFISH	Increasing the key size will lengthen the encryption time, whereas, in DES, the key size has no bearing on the encryption time.	XML Files Video Files
Karanam *et al.,* (2023)	1- Throughput 2- Memory utilization 3- Encryption time 4- Decryption time	1- AES 2- RC4	RC4 outperforms AES across all assessed metrics.	Text File

Kudair *et al.,* (2023)	1. Computation Time 2. Memory Utilization	1- DES 2- AES 3- RSA	While AES uses more memory, DES offers a faster encryption time. However, the RSA technique generates output files that are modest in size.	Text File
Patel (2019)	Processing Time 2- CPU Usage 3- Throughput	DES AES	Higher throughput and lower CPU utilization are provided by AES, whereas DES is quicker and easier to use.	Text File
Alabdulrazzaq and Alenezi (2022)	1- Encryption time 2- Decryption time 3- Security 4- Power consumption	1- DES 2- 3DES 3- AES 4- BLOWFISH 5- RSA 6- ECC	While RSA uses more power overall, AES, Blowfish, and ECC have faster encryption and decryption times, while 3DES and AES are safer.	Text File
Amorado *et al.,* (2019)	1. Security	1- S-DES 2- Enhanced S-DES	Although enhanced S-DES requires more time to encrypt, it is more secure than S-DES.	Text File
Sinha *et al.,* (2020)	Throughput 2- Encryption ratio	1- DES 2- 3DES 3- AES 4- BLOWFISH 5- Diffie Hellman	In a cloud setting, RSA is more secure.	Cloud Environment

As shown in Figure 8 below, the majority of researchers concentrated on the encryption and decryption time of the DES, 3DES, Blowfish, and AES algorithms, while the least amount of attention was paid to RC6, RC4, RC2 ECC, and D-H algorithms.

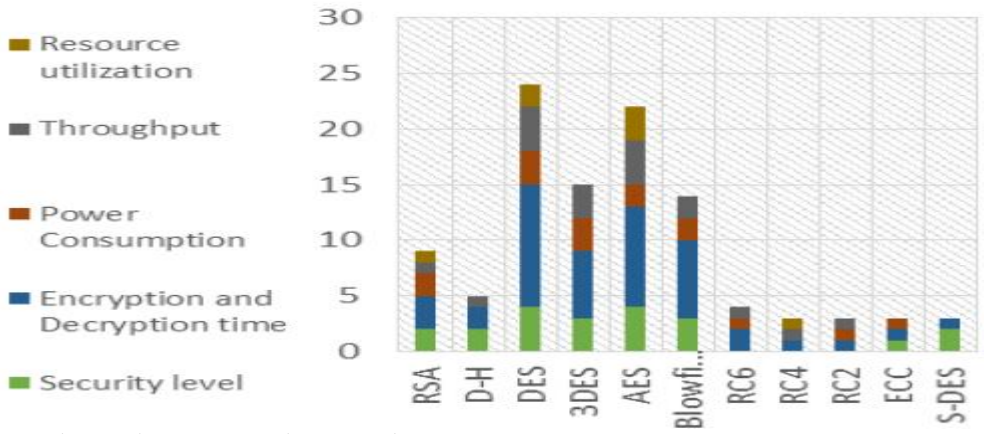


Figure 8: Research Number Compared to Tested Parameters

CONCLUSION

The parameters of the cryptographic methods, such as CPU utilization, memory, throughput, and encoding and decryption times, vary.

To improve the overall safety and security of encipherment methods, this study examines the desire to develop a combined encipherment algorithm that combines several encipherment algorithms based on all relevant parameters.

Based on these crucial parameters, this study shows the possibility of creating a hybrid encryption algorithm that combines the advantages of several different algorithms. In order to handle new cybersecurity risks and the expanding needs of contemporary applications, this research also highlights the necessity of continuously assessing and modifying cryptographic algorithms, guaranteeing reliable and scalable data protection solutions.

REFERENCES

Alabdulrazzaq, H. and Alenezi, M.N., 2022. Performance evaluation of cryptographic algorithms: DES, 3DES, blowfish, twofish, and threefish. *International Journal of Communication Networks and Information Security*, *14*(1), pp.51-61.

Alabdulrazzaq, H. and Alenezi, M.N., Performance Analysis and Evaluation of Cryptographic Algorithms: DES, 3DES, Blowfish, Twofish, and Threefish.

Alemami, Y., Mohamed, M.A. and Atiewi, S., 2019. Research on various cryptography techniques. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(2S3), pp.395-405.

Al-Shabi, M.A., 2019. A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), pp.576-589.

Ametepe, A.F.X., Ahouandjinou, A.S. and Ezin, E.C., 2022. Robust encryption method based on AES-CBC using elliptic curves Diffie–Hellman to secure data in wireless sensor networks. *Wireless Networks*, *28*(3), pp.991-1001.

Amorado, R.V., Sison, A.M. and Medina, R.P., 2019, March. Enhanced data encryption standard (DES) algorithm based on filtering and striding techniques. In *Proceedings of the 2nd International Conference on Information Science and Systems* (pp. 252-256).

Chen, L., Li, J. and Zhang, Y., 2020. Adaptively secure efficient broadcast encryption with constant-size secret key and ciphertext. *Soft Computing*, *24*, pp.4589-4606.

Fluck, A.E., 2019. An international review of eExam technologies and impact. *Computers & Education*, *132*, pp.1-15

Khudair, J., Abd Ghan, K. and Baharon, M.R.B., 2023. Comparative Study in Enhancing AES Algorithm: Data Encryption. *Wasit Journal for Pure sciences*, *2*(2), pp.316-339.

Mohammed, N.S., Dawood, O.A., Sagheer, A.M. and Nafea, A.A., 2024. Secure Smart Contract Based on Blockchain to Prevent the Non-Repudiation Phenomenon. *Baghdad Science Journal*, *21*(1), pp.0234-0234.

Nandy, T., Idris, M.Y.I.B., Noor, R.M., Kiah, L.M., Lun, L.S., Juma'at, N.B.A., Ahmedy, I., Ghani, N.A. and Bhattacharyya, S., 2019. Review on security of internet of things authentication mechanism. *IEEE Access*, *7*, pp.151054-151089.

Panahi, P., Bayılmış, C., Çavuşoğlu, U. and Kaçar, S., 2021. Performance evaluation of lightweight encryption algorithms for IoT-based applications. *Arabian Journal for Science and Engineering*, *46*(4), pp.4015-4037.

Patel, K., 2019. Performance analysis of AES, DES and Blowfish cryptographic algorithms on small and large data files. *International Journal of Information Technology*, *11*(4), pp.813-819.

Pramanik, P.K.D., Sinhababu, N., Mukherjee, B., Padmanaban, S., Maity, A., Upadhyaya, B.K., Holm-Nielsen, J.B. and Choudhury, P., 2019. Power consumption analysis, measurement, management, and issues: A state-of-the-art review of smartphone battery and energy usage. *ieee Access*, *7*, pp.182113-182172.

Rameel, M. and Asif, Z., 2024. Fortifying Information Security: A Comparative Analysis of AES, DES, 3DES, RSA, and Blowfish Algorithm. *communications*, *2*, p.5.

Rao, A. V. K., Chivukula, V. A. D., Adupala, S. K. R., & Cholleti, A. R. (2021, December). Multi-Layer Encryption Algorithm. In *CS & IT Conference Proceedings* (Vol. 11, No. 21). CS & IT Conference Proceedings.

Salem, H. (2023). *Towards trustworthy computing on untrustworthy hardware* (Doctoral dissertation, University of Edinburgh).

Sanders, P., Mehlhorn, K., Dietzfelbinger, M. and Dementiev, R., 2019. *Sequential and Parallel Algorithms and Data Structures* (pp. 403-404). Springer.

Schwenk, J. (2022). Cryptography: Confidentiality. In *Guide to Internet Cryptography: Security Protocols and Real-World Attack Implications*. Cham: Springer International Publishing. (pp. 13-41)

Singhal, V., Singh, D. and Gupta, S.K., 2022. Crypto STEGO Techniques to Secure Data Storage Using DES, DCT, Blowfish and LSB Encryption Algorithms. *Journal of Algebraic Statistics*, *13*(3), pp.1162-1171.

Sinha, K., Priya, A. and Paul, P., 2020. K-RSA: Secure data storage technique for multimedia in cloud data server. *Journal of Intelligent & Fuzzy Systems*, *39*(3), pp.3297-3314.

Sunday, A.E. and Olufunminiyi, O.E., 2023. An efficient data protection for cloud storage through encryption. *International Journal of Advanced Networking and Applications*, *14*(5), pp.5609-5618.

Vegesna, V.V., 2019. Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes. *Indo-Iranian Journal of Scientific Research (IIJSR) Volume*, *3*, pp.69-84.

Wu, Y. and Dai, X., 2020. Encryption of accounting data using DES algorithm in computing environment. *Journal of Intelligent & Fuzzy Systems*, *39*(4), pp.5085-5095.