Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 2, August 2021, pp. 1030~1038
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i2.pp1030-1038

Performance analysis of encryption and decryption algorithm

Pronika, S. S. Tyagi
Department of Computer Science & Engineering, Faculty of Engineering and Technology, Manav Rachna International Institute of Research & Studies, Haryana, India

Article Info

Article history:

Received Apr 5, 2021
Revised Jun 29, 2021
Accepted Jul 7, 2021

Keywords:

Cryptography
Data security
Decryption
Encryption
Network security
Performance comparison

ABSTRACT

In this tumultuous 21st century, we are surrounding by lots of applications such as social media websites all over the internet or this era can also define as digital era in which everything is accessible over the internet. There are billions of internet users all over the world and they share their information over the same and because of this lots of people intentionally trying to steal the confidential data of other people, so it is always advisable to share and store data in encrypted form. In this paper, we discuss different encryption and decryption algorithms and compare them with respect to time take by these algorithms for encrypting and decrypting different sizes of files.

Corresponding Author:

Pronika
Department of Computer Science & Engineering
Faculty of Engineering & Technology
Manav Rachna International Institute of Research & Studies, Faridabad, Haryana, India
Email: pronika.fet@mriu.edu.in

1. INTRODUCTION

Background: Crypto derived from a Greek word Krypto's, which means concealed. It is undauntedly related to encryption, which is the display of scrambling standard substance into what's known as cipher text and thusly back again upon appearance. Likewise, cryptography besides covers the absence of meaning of data in pictures utilizing methods, for example, microdots or joining together. In a larger picture cryptography can defined as the combination of encryption and decryption. Cryptography is defined as the process of converting plain text into cipher text and cipher text into plain text. Data security assumes a significant part during web correspondence in the present period of innovation [1], [2]. There are different cryptography techniques that give a way to make sure about trade and instalment to private interchanges and ensuring passwords [3]-[5]. Cryptography is vital for secure interchanges; it is not without help from anyone else adequate. The analysis of safe correspondences techniques that simply grant the sender and arranged recipient of a message to see its substance. When passing on electronic information, the most striking utilization of cryptography is to encode and unscramble email and other plain-messages. The most direct strategy uses the symmetric or "secret key" system. Here, data is mixed using a secret key, and subsequently both the encoded message and secret key are shipped off the recipient for deciphering. For the present circumstance, every customer has two keys: one open and one private. Senders request the open key of their proposed recipient, scramble the message, and send it along. Right when the message appears, only the recipient's private key will decipher it - which implies theft is of no use without the relating private key [6]-[8].

Problem Statement: Data is the new soil, and it is costlier than the oil in this era because most of us are using internet and out of which majority of people are not aware of theft associated with it. As in 2020

there are around 4.57 billion internet users in the world and out of these 4.57 billion internet users there are more than 4 billion people who are not aware of the risks associated with it and their mitigation strategy. Most of the internet users become the victim of intentional hackers because they are not well educated for this cybercrime. Digital eras bring lots of opportunity but with this data security risk also increase day by day because everyone's personal confidential information is over the internet because most of the applications ask for some details before allowing you to sign in. Therefore, if we are connected to internet then it's the responsibility of company's and end user both to protect their data and this can be done by using encryption and it help to achieve confidentiality, integrity, availability (CIA) triad.

Proposed: encryption is the fundamental structure square of data security and is the most un-troublesome and most critical way to deal with ensure a PC system's information can't be taken and scrutinized by someone who needs to use it for awful techniques. Used by both individual clients and enormous organizations, encryption is generally utilized on the web to guarantee the sacredness of client data that is sent between a program and a worker [9]-[11]. There are n number of encryption algorithm available to encrypt data but in this research paper we discussed only those algorithms which are very popular and widely used in the professional areas like Higher Education, IT Industry, Research and Military. Data encryption standard (DES), Data encryption standard version 3 (DES3), Blowfish, ARC4, MD5, AES [12]-[14] are some algorithms discussed in this paper. To find out the relation between the time taken by encryption algorithm to encrypt the data to the size of data. For this data files of different sizes have been selected. In this paper we discuss result of different encryption algorithms on files of size 1KB, 10KB, 100KB, 1MB and encryption time is measured in seconds.

Decoding is the way toward changing over scrambled or encoded information or text back to its unique plain organization that individual's PC applications can undoubtedly peruse and fathom [15]. This is something contrary to encryption which includes coding information to make it confused by everybody except just by those with coordinating decoding keys. What the decoding does is to decode the information and can manual, programmed utilizing suitable programming or by utilization of explicit keys, passwords or codes. This changes the indistinguishable or confused information to the first content documents, email messages, pictures, client information, and catalogues that clients and PC frameworks can peruse and decipher. Just the approved individuals can unscramble the information since the will require the keys. In the encryption-unscrambling measure, the individual who scrambles the information must give the beneficiaries the capacity to translate the information either by providing the manual or passwords or by the utilization of computerized decoding programming [16]-[18].

– DES
  Data encryption standard (DES) has been found vulnerable against particularly amazing assault and in this manner, the commonness of DES has been discovered fairly on not. DES is a square code and encodes data in squares of size of 64 piece each, in which plaintext of 64 bits goes as the commitment to DES, which produces 64 bits of cipher text.
- DES3
  Triple DES is an encryption method, which utilizes three occurrences of DES on same plain content. Triple DES is additionally helpless beside compromise assault due to which it gives absolute security level of 2^112 as opposed to utilizing 168 pieces of key. The square crash assault should likewise be possible considering short square size and utilizing same key to encode huge size of text. It is additionally defenceless against sweet32 assault.
- ARC4
  ARC4 (Alleged RC4) is the usage of RC4 (Rivest's cipher adaptation 4) an asymmetric stream figure planned by Ron Rivest in 1987. The organization that claims RC4 (RSA data inc.) never affirmed the accuracy of the spilled calculation. Dissimilar to RC2, the organization has never distributed the full detail of RC4, of whom it despite everything holds the brand name. ARC4 keys can fluctuate long from 40 to 2048 pieces.
- Blowfish
  Blowfish is one of the square code methods which splits a message into fixed length blocks during encryption and unscrambling. It is a 64-digit block code and it is quick calculation to scramble the information. It requires 32-digit chip at pace of one byte for each 26 clock cycles. It is variable length key square code up to 448 pieces [19].
- AES
  The advanced encryption standard (AES) is a symmetric square code picked by the U.S. government to secure grouped data. AES is executed in programming and equipment all through the world to scramble touchy information. It is fundamental for government PC security, cybersecurity, and electronic information insurance [20].

Different types of secure algorithms explained above, now we discussed the comparisons. Table 1 shows the comparisons between secured algorithms related to different factors.

Table 1. Comparison between secured algorithms

Factors	DES	AES	RSA	Blowfish
Invented by	IBM	Vincent Rijmen, Joan Daemen	Ron Rivest, Adi Shamir, and Leonard Adleman	Bruce Schneier
Year	1977	2001	1978	1993
Cipher	Symmetric Block Cipher	Symmetric Block Cipher	Asymmetric Block Cipher	Symmetric Block Cipher
Key Length	56	128-256	1024	32-448
Block Size	64	128	Not fixed	64
Security Level	Not adequate	Excellent	High	High
No. of Rounds	16	10-14	1	16
Speed of algorithm	Slow	Fast	Slow	Fast
Power Consumption	Low	Low	High	Low
Performance	DES considered insecure but it becomes secure when it comes in the form of Triple DES.	AES-CBC is what older clients commonly use. AES-CBC mode is susceptible to attacks such as Lucky13 and BEAST.	RSA performance degraded when we compare with DES.	Blowfish is informal replacement of DES and IDEA
Security Feature	DES taken as unsecured due to its small size.	Most CPUs now include hardware AES support making it very fast.	RSA used for digital signing but it is slower.	Blowfish gaining slowly popularity as a robust encryption algorithm.
Supported by SSH/ TrueCrypt	Triple DES supported by TrueCrypt.	Supported by TrueCrypt, SSH.	SSH v1 only uses RSA keys	Supported by SSH.

2. RELATED WORK

This section deals with the related work in the field of cryptography and its related algorithms. Tayal *et al.* [5] discussed the concept of cryptography; it is a process in which user secure his text and receiver can read that secured information. In cryptography, two types of keys used one is public key and other is private key. Dixit *et al.* [6] explained the concept of plaintext, ciphertext, and related terms of security of data like confidentiality, integrity and availability. In [7], [8] proposed the hybrid algorithm in the paper like ECC with Hill Cipher, ECC with AES. Hybrid algorithm means it is a combination of different types of algorithms. Abdullah [9] used AES algorithm in this paper and evaluation criteria of AES was cost and security. AES Encryption and decryption process explained in this paper. In [12]-[14] discussed different types of symmetric and asymmetric algorithms. Comparison between AES and DES using different parameters discussed in the form of table. Chinnasamy *et al.* [15] explained the weakness of traditional symmetric and asymmetric algorithm and proposed a new algorithm that is the combination of ECC and Blowfish, which provides the high security and confidentiality to the data. Tallapally and Manjula [16] proposed a multilevel security scheme that provide more security as compare to single level security in encryption. The proposed algorithm is faster and safe in multiple direction. In [17], [18] explained different types of cloud models, their advantages and disadvantages. Security issues related to data when user stored data on cloud also discussed with different parameters. Guo and Sun [19] proposed an order revealing encryption scheme in which cloud service provider cannot find or calculate the order of the plaintext until the comparison token not given to them. Chinnasamy and Deepalakshmi [21] discussed the hybrid method for secure storage of health care data in cloud. They explained operations of Blowfish, enhanced RSA algorithm, and compare the proposed scheme with time and it gives fast encryption time and efficient key management. Chinnasamy and Deepalakshmi [22] introduced improved key generation scheme for RSA algorithm and speed of proposed method is higher as compared to other RSA methods. In [23], [24] discussed hybrid algorithm for healthcare system and used One Time Pad with RSA algorithm in cryptography techniques. In [25]-[28] explained the data storage and data retrieval framework for cloud and discussed the searchable encryption process for data storage and decryption process for data retrieval. In [29], [30] authors discussed about the security using different cryptographic techniques. Comparisons of these techniques also described by authors and they give a method using elliptic curve cryptography to provide security using smaller key length.

3. RESEARCH METHOD

In this paper, comparing time taken by different algorithms for encryption and decryption of different size of file, we also find out there is a trade-off between security and time. Both factors security and time play a vital role for selecting an algorithm because if we compromise with any of these two then it may influence the performance of the system in terms of security and efficiency. Therefore, we are proposing that before selecting

an encryption or decryption algorithm we must check the size of a file we have to encrypt, or decrypt then based on that appropriate algorithm should be selected. There has consistently been a tradeoff between two things. If there should arise an occurrence of cryptographic calculations the tradeoff is between speed and security. On the off chance that we talk about speed and bargain on security, at that point in this situation Blowfish is more proficient than some other calculation including AES nevertheless, if security matters to us more than speed for this situation AES is generally productive. Here we are more worried about security that which calculation makes our information most secure with the goal that is the reason we will utilize AES. Each method has some powerless focuses. The week purpose of AES is speed because of its intricacy.

In this paper, we will discuss the performance of different cryptographic algorithm while encryption and decryption with different size of files like 1KB, 10KB, 100KB, and 1MB. First, one by one, algorithm applied on plain text to encrypt it in cipher text and then same algorithms used to decrypt the cipher text into plain text. The flowchart of proposed methodology is showing in Figure 1.

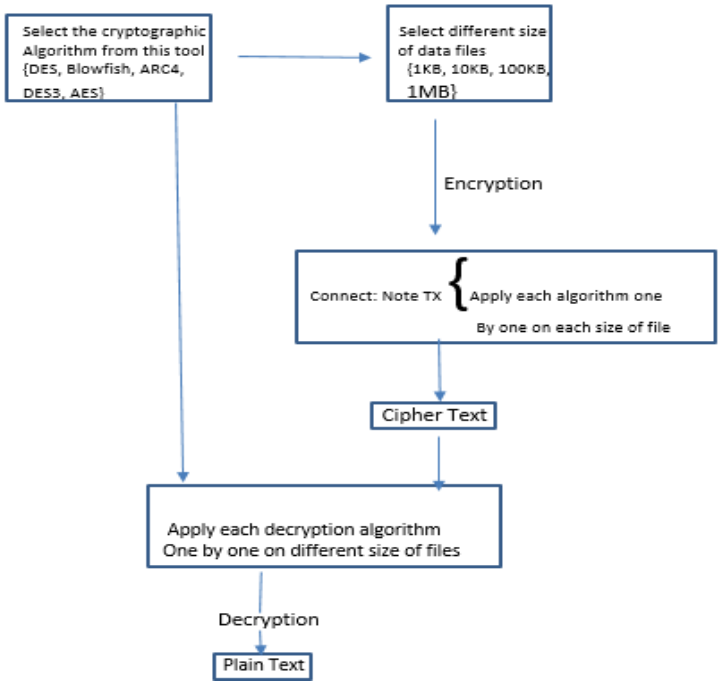

Figure 1. Flowchart of proposed methodology

4. RESULT AND DISCUSSIONS

4.1. Encryption

– DES

In this research work, we use the DES algorithm on different sizes of file and note down the time taken by these algorithms to encrypt the different file. Many times, it observed that many algorithms could encrypt small data files much faster than the large data files. DES is the first algorithm used in this research and it can encrypt 1KB of file in 0.000996828 seconds, 10KB of file in 0.001995087 seconds, 100KB of file in 0.009972572 seconds and 1MB of file in 0.040885448 seconds. These results of DES shown in Figure 2.

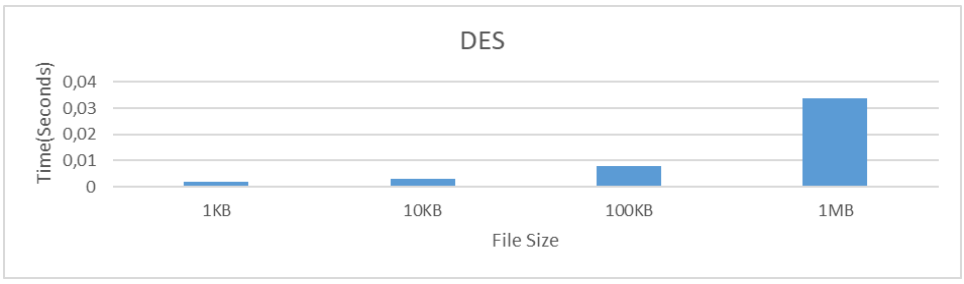

Figure 2. Comparison of time taken by DES algorithm to Encrypt files of different size

After DES, second algorithm discussed in this paper is modified version of DES popularly known Triple DES.

– DES3
DES3 is the other algorithm. It can encrypt 1KB of file in 0.001995087 seconds, 10KB of file in 0.001994133 seconds, 100KB of file in 0.01994729 seconds and 1MB of file in 0.095748663 seconds. These results of DES3 shown in Figure 3.

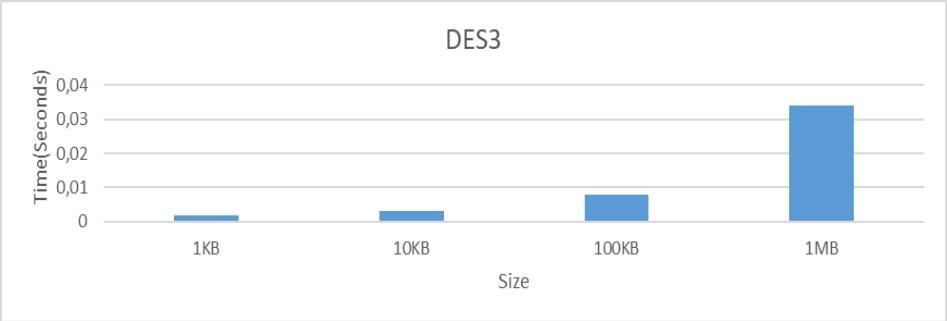

Figure 3. Comparison of time taken by DES3 algorithm to Encrypt files of different size

– ARC4
It can encrypt 1KB of file in 0.000989437 seconds, 10KB of file in 0.00199604 seconds, 100KB of file in 0.002984047 seconds and 1MB of file in 0.017950773 seconds. These results of ARC4 shown in Figure 4.

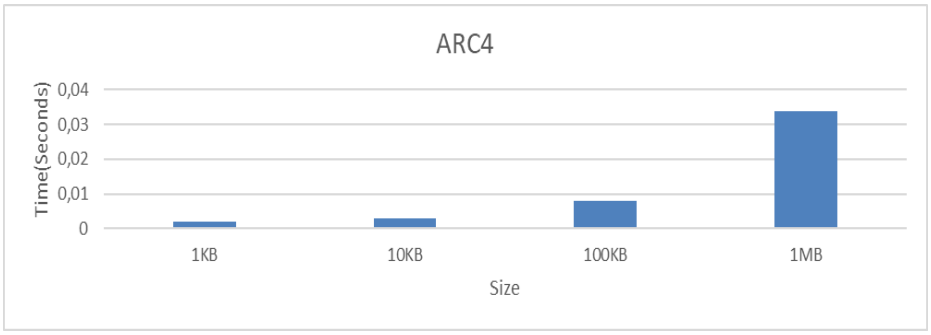

Figure 4. Comparison of time taken by ARC4 algorithm to Encrypt files of different size

– Blowfish
It can encrypt 1KB of file in 0.001996517 seconds, 10KB of file in 0.001995564 seconds, 100KB of file in 0.007981062 seconds and 1MB of file in 0.026927948 seconds. These results of Blowfish shown in Figure 5.

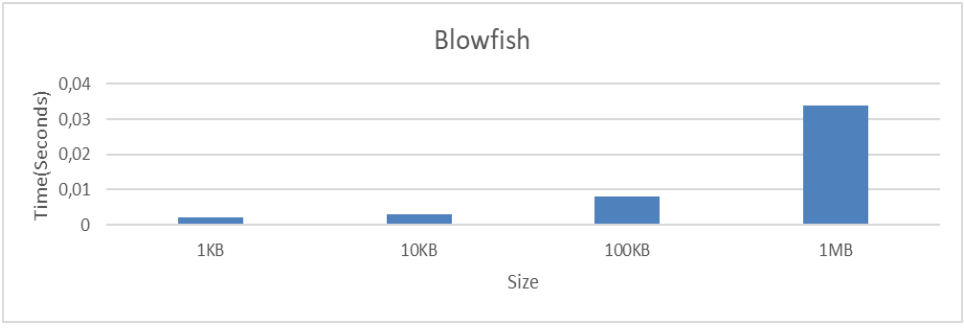

Figure 5. Comparison of time taken by Blowfish algorithm to Encrypt files of different size

– AES
The National Institute of Standards and Technology (NIST) began the advancement of AES in 1997 when it reported the requirement for an option in contrast to the data encryption standard (DES), which was beginning to get powerless against beast power assaults. It can encrypt 1KB of file in 0.00199604 seconds, 10KB of file in 0.002985477 seconds, 100KB of file in 0.007977724 seconds and 1MB of file in 0.033907175 seconds. These results of AES shown in Figure 6. Figures are best way to represent their results therefore these results of encryption shown in above graphs and their data shown in Table 2.

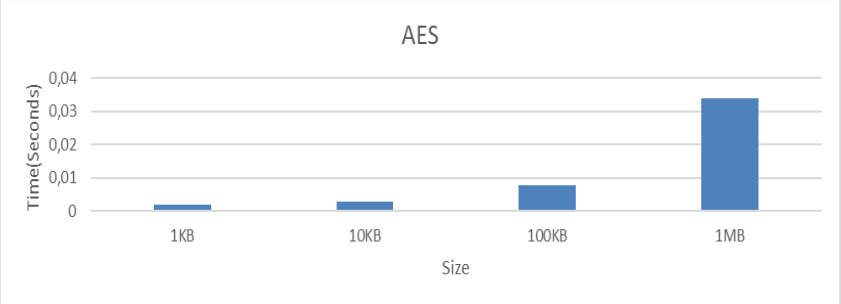

Figure 6. Comparison of time taken by AES algorithm to Encrypt files of different size

Table 2. Time take by cryptography algorithm for encryption

Size/Algorithm	DES	Blowfish	ARC4	DES3	AES
1KB	0.00099682	0.00199651	0.0009894	0.0019950	0.00199604
10KB	0.00199508	0.00199556	0.0019960	0.0019941	0.00298547
100KB	0.00997257	0.00798106	0.0029840	0.0199472	0.00797772
1 MB	0.04088544	0.02692794	0.0179507	0.0957486	0.03390717

4.2. Decryption

– DES
In this research work, we use the same algorithm on different sizes of file and note down the time taken by these algorithms to decrypt the different file. Many times, it observed that many algorithms could encrypt small data files much faster than the large data files. DES is the first algorithm used in this research and it can encrypt 1KB of file in 0.000996828 seconds, 10KB of file in 0.001995087 seconds, 100KB of file in 0.009972572 seconds and 1MB of file in 0.040885448 seconds. These results of DES shown in Figure 7.

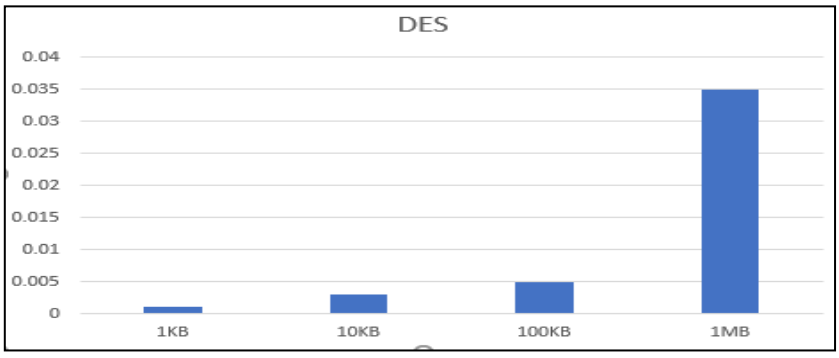

Figure 7. Comparison of time taken by DES algorithm to decrypt files of different size

– Blowfish
It can encrypt 1KB of file in 0.001996517 seconds, 10KB of file in 0.001995564 seconds, 100KB of file in 0.007981062 seconds and 1MB of file in 0.026927948 seconds. These results of Blowfish shown in Figure 8.

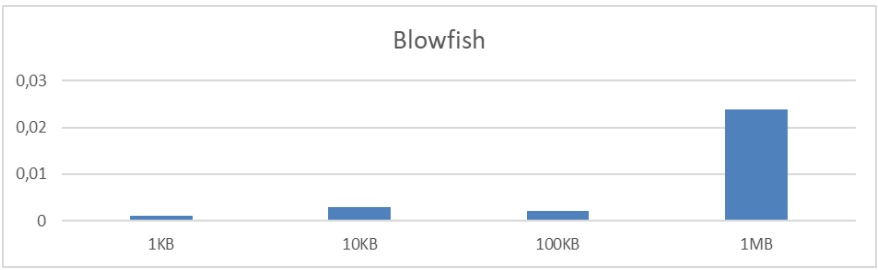

Figure 8. Comparison of time taken by Blowfish algorithm to decrypt files of different size

– ARC4
It can encrypt 1KB of file in 0.000989437 seconds, 10KB of file in 0.00199604 seconds, 100KB of file in 0.002984047 seconds and 1MB of file in 0.017950773 seconds. These results of ARC4 shown in Figure 9.

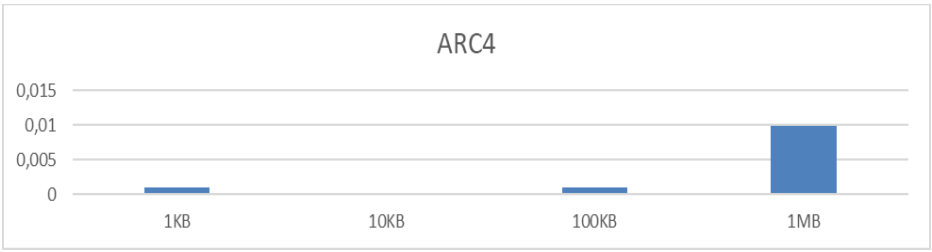

Figure 9. Comparison of time taken by ARC4 algorithm to decrypt files of different size

– DES3
It can encrypt 1KB of file in 0.001995087 seconds, 10KB of file in 0.001994133 seconds, 100KB of file in 0.01994729 seconds and 1MB of file in 0.095748663 seconds. These results of DES3 shown in Figure 10.

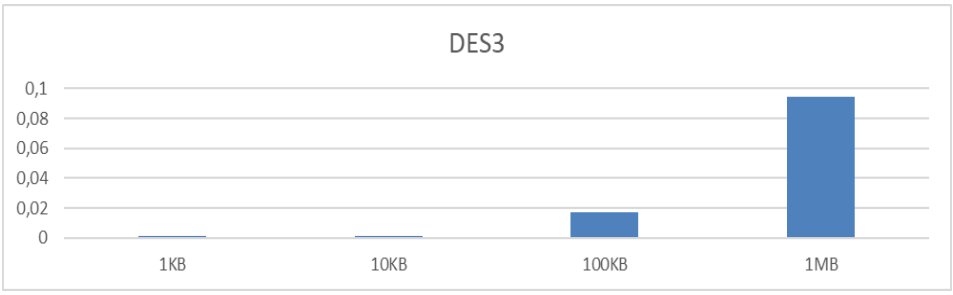

Figure 10. Comparison of time taken by DES3 algorithm to decrypt files of different size

Graphs are best way to represent their results therefore these results of decryption shown in above graphs and their data shown in Table 3.

Table 3. Time takes by cryptography algorithm for decryption

Algorithm/Size	1KB	10KB	100KB	1MB
DES	0.000994682	0.002992392	0.004985809	0.034943819
Blowfish	0.00099206	0.00299263	0.001995087	0.023936033
ARC4	0.000997305	0	0.000997543	0.009969234
DES3	0.00099659	0.00099802	0.016951561	0.094743252

5. CONCLUSION

The examination of various computations shows that the nature of model depends on the key organization, kind of cryptography, number of keys, number of pieces used in a key. All the keys rely upon the mathematical properties. The keys having a more prominent number of pieces requires more estimation time which fundamentally shows that the structure puts aside more exertion to scramble the data. AES data encryption is an even more mathematically powerful and rich cryptographic figuring, anyway its basic quality rests in the option for various key lengths. In this paper, we discussed different encryption and decryption algorithms and compared them with respect to time take by these algorithms for encrypting and decrypting different sizes of files. Different size of files is compared with respect to different encryption and decryption algorithm. To explain how size can affect the performance and time to encrypt and decrypt text, file size of 1 KB, 10 KB, 100 KB and I MB size of files are compared first for encryption with DES, Blowfish, ARC4, DES3 and AES. After encryption same size of files are decrypt using the DES, Blowfish, ARC4 and DES3 algorithm. From this comparison, it can conclude that DES algorithm is best suited to encrypt 1KB of file and ARC4 to encrypt 1MB of file whereas to decrypt 1MB of file ARC4 algorithm is best suited and DES3 is best suited to decrypt 1KB of file.

REFERENCES

[1] S. A. Hannan, and A. M. Asif, "Analysis of polyalphabetic transposition cipher techniques used for encryption and decryption," *International Journal of Computer Science and Software Engineering*, vol. 6, no. 2, pp. 41-46, Feb. 2017, doi: 10.1109/TBME.2011.2158315.

[2] J. Lai, R. H. Deng, C. Guan and J. Weng, "Attribute-Based Encryption with Verifiable Outsourced Decryption," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 8, pp. 1343-1354, Aug. 2013, doi: 10.1109/TIFS.2013.2271848.

[3] J. Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 10, pp. 2271-2282, Oct. 2013, doi: 10.1109/TKDE.2011.78.

[4] J. Li, X. Chen, M. Li, J. Li, P. P. C. Lee and W. Lou, "Secure Deduplication with Efficient and Reliable Convergent Key Management," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615-1625, June 2014, doi: 10.1109/TPDS.2013.284.

[5] S. Tayal, N. Gupta, P. Gupta, D. Goyal, M. Goyal, "A review paper on network security and cryptography," *Advances in Computational Sciences and Technology*, vol. 10, no. 5, pp. 763-770, 2017.

[6] P. Dixit, A. K. Gupta, M. C. Trivedi, V. K. Yadav, "Traditional and hybrid encryption techniques: a survey," in *Networking communication and data knowledge engineering*, Springer, pp. 239-248, 2018.

[7] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. Perumal, M. F. Ijaz, "Analytical Study of Hybrid Techniques for Image Encryption and Decryption," *Sensors*, vol. 20, no. 18, pp. 5162, 2020, doi: 10.3390/s20185162.

[8] S. Mishra and A. Dastidar, "Hybrid Image Encryption and Decryption using Cryptography and Watermarking Technique for High Security Applications," *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, 2018, pp. 1-5, doi: 10.1109/ICCTCT.2018.8551103.

[9] A. Abdullah, "Advanced encryption standard (aes) algorithm to encrypt and decrypt data," *Cryptography and Network Security*, vol. 16, pp. 1-11, 2017.

[10] S. R. Zeebaree, "DES encryption and decryption algorithm implementation based on FPGA," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp.774-781, 2020, doi: 10.11591/ijeecs.v18.i2.pp774-781.

[11] T. Hidayat and R. Mahardiko, "A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing," *International Journal of Artificial Intelligence Research*, vol. 4, no.1, pp. 49-57, 2020.

[12] P. Semwal and M. K. Sharma, "Comparative study of different cryptographic algorithms for data security in cloud computing," 2017 *3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall)*, 2017, pp. 1-7, doi: 10.1109/ICACCAF.2017.8344738.

[13] N. A. Al-gohany and S. Almotairi, "Comparative Study of Database Security in Cloud Computing Using AES and DES Encryption Algorithms," *Journal of Information Security and Cybercrimes Research*, vol. 2, no. 1, pp. 102-109, 2019.

[14] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," *2017 International Conference on Engineering and Technology (ICET)*, 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

[15] P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient Data Security Using Hybrid Cryptography on Cloud Computing," *InInventive Communication and Computational Technologies*, Springer, pp. 537-547, 2021.

[16] S. K. Tallapally and B. Manjula, "Competent multi-level encryption methods for implementing cloud security," *InIOP Conference Series: Materials Science and Engineering*, vol. 981, no. 2, p. 022039, 2020.

[17] E. M. Alsaadi, S. M. Fayadh, and A. Alabaichi, "A review on security challenges and approaches in the cloud computing," *InAIP Conference Proceedings*, vol. 2290, no. 1, p. 040022, 2020.

[18] N. Mohammed and N. Ibrahim, "Implementation of New Secure Encryption Technique for Cloud Computing," *2019 International Conference on Computing and Information Science and Technology and Their Applications (ICCISTA)*, 2019, pp. 1-5, doi: 10.1109/ICCISTA.2019.8830668.

[19] J. Guo and J. Sun, "Order-Revealing Encryption Scheme with Comparison Token for Cloud Computing." *Security and Communication Networks*, vol. 2020, 2020.
[20] Salma, R. F. Olanrewaju, K. Abdullah, Rusmala, and H. Darwis, "Enhancing Cloud Data Security Using Hybrid of Advanced Encryption Standard and Blowfish Encryption Algorithms," *2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT)*, 2018, pp. 18-23, doi: 10.1109/EIConCIT.2018.8878629.
[21] P. Chinnasamy and P. Deepalakshmi, "Design of Secure Storage for Health-care Cloud using Hybrid Cryptography," *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018, pp. 1717-1720, doi: 10.1109/ICICCT.2018.8473107.
[22] P. Chinnasamy and P. Deepalakshmi, "Improved key generation scheme of RSA (IKGSR) algorithm based on offline storage for cloud," *In Advances in Big Data and Cloud Computing*, Springer, pp. 341-350, 2018.
[23] P. Chinnasamy and P. Deepalakshmi, "HCAC-EHR: hybrid cryptographic access control for secure EHR retrieval in healthcare cloud," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-9, 2021.
[24] Karthik, Chinnasamy, and Deepalakshmi, "Hybrid cryptographic technique using OTP:RSA," *2017 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, 2017, pp. 1-4, doi: 10.1109/ITCOSP.2017.8303131.
[25] Pronika and S. S. Tyagi, "Secure Data Storage in Cloud using Encryption Algorithm," *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, 2021, pp. 136-141, doi: 10.1109/ICICV50876.2021.9388388.
[26] D. Taneja and S. S. Tyagi, "Information Security in cloud computing: A Systematic Literature Review and analysis," *International Journal of Scientific Engineering and Technology*, vol. 6, no. 1, pp. 50-55, 2017.
[27] V. Arora and S. Tyagi, "Analysis of Symmetric Searchable Encryption and Data Retrieval in Cloud Computing,". *International Journal of Computer Applications*, vol. 127, no. 12, pp. 46-51, 2015.
[28] V. Arora and S. S. Tyagi, "An efficient multi-keyword symmetric searchable encryption scheme for secure data outsourcing," *International Journal of Computer Network and Information Security*, vol. 8, no. 11, p. 65, 2016.
[29] D. Mahto and D. K. Yadav, "RSA and ECC: a comparative analysis," *International journal of applied engineering research*, vol. 12, no. 19, pp. 9053-9061, 2017.
[30] A. Tyagi, K. S. Pandian, and S. Khan, "Design and Implementation of Lightweight Dynamic Elliptic Curve Cryptography Using Schoof's Algorithm," *In International Conference on Computing Science, Communication and Security (COMS2)*, Springer, pp. 193-204, 2021.

BIOGRAPHIES OF AUTHORS

Ms. Pronika is presently working as an Assistant Professor in Department of computer Science & Engineering department in Manav Rachna International Institute of Research & Studies (MRIIRS), India from 2008. She completed her B.tech from KUK University, Kurukshetra in 2007 and M.Tech from Banasthali Vidyapith, Jaipur in 2009. Currently, she is pursuing Ph.D. from MRIIRS in computer science. Her area of interest is operating system, network security, database and cloud computing. She has more than 25 publications in reputed journals and conferences.

Dr. S.S. Tyagi is presently working as a Professor and Dean of Faculty of Compter Applications in Manav Rachna International Institute of Research & Studies, Faridabad, India. He completed his Phd. From Kurukshetra University, Kurukshetra and M.E. from BITS, Pilani and B. Tech from Nagpur University in computer science. He is having an experience of more than 27 years in academics/teaching and research. He is a senior member of various professional organizations like IEEE, ACM, CSI, QCI, and ASQ. He is past chair, IEEE Computer Society, Delhi Section. There are more than 70 publications to his credit in National and International Journals. He has guided 06 Ph.Ds and several M.Tech Thesis and guiding Ph.D scholars in the field of Cloud Computing, Adhoc Networks, and Wireless Security.