COMPUTATIONAL COMPLEXITY OF RSA AND ELGAMAL CRYPTOGRAPHIC ALGORITHMS ON VIDEO DATA

[1]ADENIYI ABIDEMI EMMANUEL, [2]ADEBIYI OLUBUNMI MARION, [3]OKEYINKA ADEREMI E., and [4]OLUDAYO O. OLUGBARA

[1-3]Department of Computer Science, College of Pure and Applied Sciences, Landmark University, Omu-Aran, Kwara State, Nigeria.

[2, 4]ICT and society Research Group, Luban Workshop, Durban University of Technology, P.O. Box 1334, Durban 4000, South Africa.

E-mail: [1]adeniyi.emmanuel@lmu.edu.ng

ABSTRACT

The study on the complexity of an algorithms have great impact on the whole fields of computer science, data security and data communication. The more efficient algorithms are the better the data security, communication and sharing of information on various platform. Data security is very important especially in an environment of unprotected data transmission network. There are various techniques of data transfer which leaves the users with the questions of how such data is being secure; cryptographic algorithms provides solution to the security of data transmission whereby ensuring integrity, confidentiality and authentication of any form of data. However, there are still challenges of which cryptographic algorithms is suitable in terms of computation speed and memory usage. Therefore, this study is concerned with the complexity of RSA and ElGamal cryptographic algorithms in terms of time and space usage while encrypting and decrypting video data in order to establish which of the algorithms is more efficient. C-sharp programming language was used to implement the RSA and ElGamal cryptographic algorithms and the experimental result showed that RSA cryptographic algorithm performed better in terms of time complexity while Elgamal cryptographic algorithm is memory efficient.

Keywords: *Cryptographic algorithm, Complexity, Video data, Data security, Data communication.*

1. INTRODUCTION

Comparative study provides a means of comparing two or more characteristics of different algorithms to a given problem to accomplish a level of efficiency. It is a quality and ability of performing tasks effectively without wasting resources such as time, memory and energy [1]. Thus, comparative study deals with the efficiency of algorithms that is identification of the better of two algorithms solving the same problem [2],[3]. An algorithm is simply a precise method usable by a computer for the solution of a problem [4]. An important property of an algorithm is its effectiveness. Ensuring algorithm effectiveness demands application of design techniques, which have been proven useful in devising good algorithms. Algorithms are usually written in order to fulfil the obligation of generality, which are then translated into executable programs in some chosen languages. Many of the algorithms studied by computer scientists that ensure data and information security are known as cryptographic algorithms [5]. There are many cryptographic algorithms and we must ensure that whichever algorithm has been chosen must be suitable and efficient for the given task. This study aim at comparing the RSA and ElGamal algorithms in terms of time and space complexity analysis for better resource allocation.

Data authenticity plays a big role in data processing, as it describes whether the data received at the collection point is original and was received exactly as it was sent by the sender [6]. Communication has always existed from the beginning of human existence, and it has been necessary for social development [7]. Humans communicate through several media including: verbal, non-verbal, written, oral, among others, and with these various methods of communication available, humans must then ensure a way to protect their communicated information so that someone who the information was not intended for should not have access to it, this method is known as cryptography. Cryptography is generally a method of converting plain data into an unintelligible form and vice-versa to prevent it from third parties known as adversaries [8].

In the earlier cryptography, the process was effectively based on encryption and decryption that are computed practically and solved by hands using paper and pen and this was known as classic cipher. Classic ciphers are classified into the conversion cipher and the replacement cipher [9],[10]. In the conversion cipher, the characters themselves appear unaffected, but are scrambled according to a well-defined basic encryption scheme in which each plain text is written backwards. In the substitution cipher, characters (or sets of words) are systematically substituted by other characters throughout the code (or group of letters). The Caesar cipher is a well-known illustration of the substitution cipher in which each letter in the message is replaced by the letter three positions forward in the alphabet. For example, a was replaced by d,b with e and so on while x,y, and z are replaced by a,b,c respectively.

Modern cryptography deal with the process of securing data based on mathematical techniques and use of computer. Modern cryptography is the foundation of the defense of computers and communication systems [1],[11]. Its foundation is based on various concepts of mathematics such as number theory, computational complexity theory, and probability theory. It is effectively a way of protecting information that is either stored or communicated over a network [12]. Modern Cryptography ensures confidentiality, integrity, non-repudiation and authentication of various forms of data especially the concerned video data.

There are 3 types of cryptosystems which are the private key (symmetric key) cryptosystem, public key (asymmetric key) cryptosystem and the hash functions. In private key cryptosystem, both the sender and the receiver share one single key [12],[13]. As shown in figure 1, the sender uses the key to encrypt the message and then sends the cipher file to the receiver who then applies the same key to decrypt the cipher file and get back the message. In public key cryptosystems, the encryption and decryption processes are based on two keys; public key that is known to everyone and private key which only the recipient knows [12],[14]. As shown in figure 2 the sender uses the receivers public key to compose the cipher file and then sends it over to the receiver, who then uses his/her private key to decrypt the cipher file and get the message. In hash functions, no key is used. A fixed-length hash text is computed as per plain text.

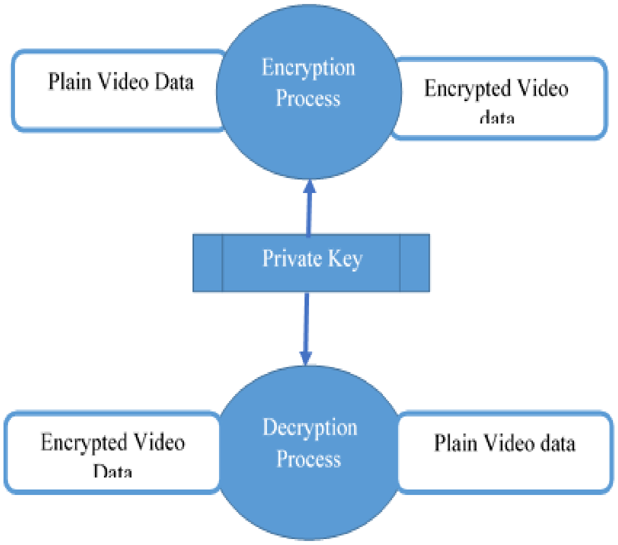

Figure 1: Symmetric Algorithms

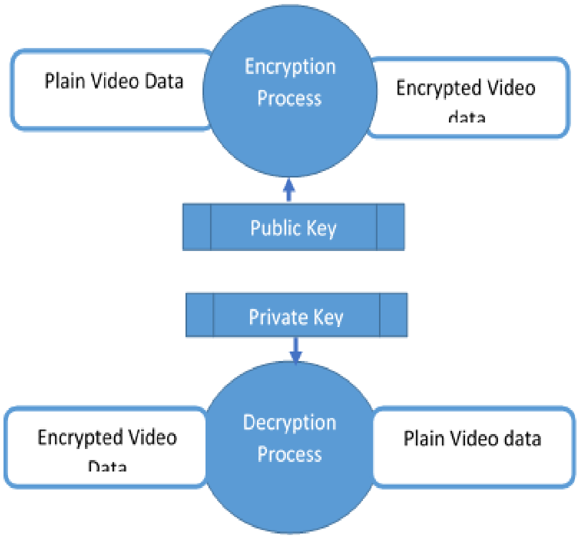

Figure 2: Asymmetric Algorithm

Computational complexity is the measure of the amount of resources needed to run a system or program. It is the execution time and storage space required to perform a computational task. We carry out complexity study of algorithms to find out how algorithms behave in different situations. An algorithm is shown to be effective when the parameters of its component are minimal or rise slowly relative to an increase in the input size. Different inputs of the same length which allow the algorithm to have distinct characteristics, so best, worst and average case definitions may all be of realistic importance to the user.

The RSA Cryptographic Algorithm

The public key cryptography RSA was from Diffie and Hellman, who invented the exponential key exchange process. In 1976, Ronald Rivest, Adi Shamir and Leonard Adleman, all young graduate students of the Masschusettes Institute of Technology, started working on a new method of cryptographic architecture [15]. Rivest and Shamir were computational scientists at the MIT, while Adleman was a numerical researcher at the MIT. Ronald and Adi would create concepts in their project, while Leonard would try to knock the ideas down by breaking them down. Leonard had been able to break them again and again until one night, when Ronald created an algorithm that Leonard could not crack. The Algorithm was called RSA, named after Rivest, Shamir, and Adleman [16],[17],[18]. The heart of RSA has withstood any assault by the finest cryptographic minds. RSA has played a critical role in the area of electronic media. As the very first example in the existence of the public key cryptography, and worth little, the only form that has survived more than 30 years of attacks, the RSA has now become a preferred algorithm for features such as phone call authentication, Internet credit card encryption, e-mail protection, and various other Internet security features. RSA continues to increase its functions and to reward its contributions, Rivest, Shamir and Adleman won one of the most prestigious prizes in the field of mathematics, the Alan Turing Award of the Association for Computing Machinery in 2002. It is no wonder that RSA security remains a core subject of cryptographic studies in both theoretical and functional applications [19],[20].

ElGamal Cryptographic Algorithm

The ElGamal cryptographic algorithm is closely connected to the Diffie Hellman key exchange protocol because the users can exchange a private key over an unsecured channel and then use this key to encrypt a message and send to the other [21]. The security of this cryptosystem is based solely on the difficulty of solving the Diffie-Hellman problem. ElGamal cryptosystem is a non-deterministic algorithm which is based on the discrete logarithm problem [22]. ElGamal cryptography is among the encryption schemes that uses randomization in the encryption algorithm, while others include McEliece encryption and Goldwasser-Micali and Blum-Goldwasser probabilistic encryption. The underlying principle driving randomized encryption strategies is to use randomization to improve the privacy protection of the encryption process via one or all of the following approaches – maximizing the effective size of the clear text file space – prescribing or reducing the efficacy of selected plaintext attacks by one-to-many cipher-text modeling; and – Preventing or lowering the efficacy of predictive attacks by reducing the a priori probabilistic model of inputs.

Nwe & Phyo [23], in their paper discussed about the performance study of RSA and ELGamal cryptographic algorithms for audio security depending on the execution time. The study also acknowledged the fact that due to significant improvement in hardware specification, cryptographic computation can be performed faster, but this also means that attackers can attack faster. Therefore, there is a need for longer key size and fast security services, so public key cryptography is the best. Their experimental result showed that the RSA cryptographic algorithms was significantly faster than the ELGamal cryptographic algorithms in terms of encryption and decryption of the audio files. The study made further suggestions that more analysis should be carried out in other file formats such as (.txt, .jpg etc) for performance comparison.

Abari et al, [24] in their paper examined the speed of encryption and decryption as well as the size of the ciphertext of both RSA and ELGamal cryptographic algorithm. From the study's results, it was stated that the RSA takes longer time to generate its key than the ELGamal algorithm. It was also stated that the ELGamal takes longer time in term of encryption and decryption of plain file and cipher text respectively. The study also highlighted that the ciphertext generated by the ELGamal algorithm was twice as large as the ciphertext generated by the RSA algorithm, therefore establishing the fact that the ELGamal consumed more storage space than the RSA algorithm. The study concluded that the ElGamal is proven to be mathematically safer than the RSA, but the RSA is significantly faster than the ELGamal cryptographic algorithm. It was further recommended that mathematical approach is to be made in carrying out comparative analysis of the two cryptographic algorithms.

Siahaan et al, [1], in their paper carried out a comparative analysis of both RSA and ELGamal cryptographic algorithm. According to the analysis of the results, the encryption and decryption time of the RSA is better than the ELGamal. The study stated that the cipher text of the RSA had fewer numbers then the ELGamal, it also further discussed the ELGamal algorithm whose cipher text was a pair (each encrypted plain text will generate two cipher text values). It was also discussed that for security reasons, the ELGamal algorithm (which lies in calculation of discrete logarithms) has proven to be more secure than the RSA (which lies in factorization of large prime) due to the challenge in solving discrete logarithms in real time.

Kyaw et. al., [25] discussed the encryption and decryption time performance analysis of RSA and ElGamal public-key cryptosystems. The researcher encrypted the plaintext (text, image and audio) file with a public key RSA and ElGamal and show the comparison of encryption time for the two algorithms. The result shows that RSA is about four times faster than ElGamal during the encryption process and also RSA is faster than ElGamal during the decryption process.

2. MATERIALS AND METHOD

This study implements RSA and ElGamal Asymmetric Cryptographic Algorithms on video dataset to determine the time and space complexities of both algorithms for proper infrastructure design, decision making and resource allocation. The encryption time, decryption time and memory usage of both algorithms were obtained and analyzed with tables and graphs. Figure 3 and Figure 4 depicts the flowchart design for RSA and ElGamal asymmetric algorithms respectively.

RSA Key Generation, Encryption and Decryption Techniques

This section discuss how RSA algorithm encryption, decryption, and key generation are performed in theory, along with some real implementations, and diagrams

Key Generation

Detailed below is the Key Generation process;

Randomly pick two big, distinct prime numbers p and q.

Calculate n, the multiplication of p and q; n = p * q

Calculate the phi function ϕ(n) = (p - 1) * (q - 1)

Select a random numbere, such that 0 < e < ϕ(n) and the GCD of e and ϕ(n) is 1.

Compute d, such that e * d mod ϕ(n) = 1, using the Extended Euclidean Algorithm

The private key is given as (n,d) and the public key as (n,e)

Encryption

Given the message to be M and the Cipher C

Encryption is done using the public key (n,e)

Compute C, such that C =M^e mod n

Decryption

Given the message to be M and the Cipher C

Decryption is done using the private key (n,d)

Obtain the cipher file C.

Compute M, such that M = C^d mod n

Design of the RSA Algorithm (next page)

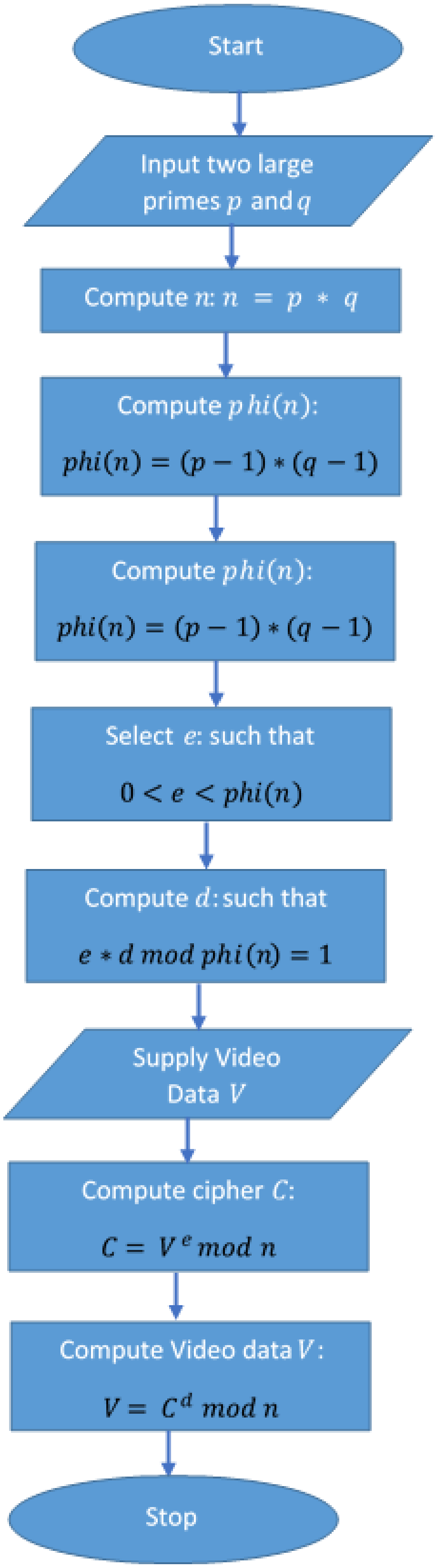

Figure 3: Flowchart for the RSA Algorithm Design

ElGamal Key Generation, Encryption and Decryption Techniques

The ElGamal cryptographic algorithm is based on a discrete logarithm. The security strength of the cipher is a function of the sizes of the modulus. It requires module exponentiation operation for the encryption and decryption processes. This section outline how encryption, decryption, and key generation for the ElGamal algorithm are performed in theory, along with some actual implementations.

Key Generation

Detailed below is the Key Generation process;

i. Randomly pick a big, distinct prime p.

ii. Choose a generator number g.

iii. Select an integer x, such that 0 < x < p-2, x becomes the secret number.

iv. Compute y, such that y = gx mod p.

The private key is given as (p, x) and the public key as (p, g, y)

Encryption

Given the message to be M and the Cipher C

i. Encryption is done using the public key (p, g, y)

ii. Select an integer k, such that 1 < k < p-2.

iii. Compute C1, such that a = gk mod p.

iv. Compute C2, such that b = (yk * M) mod p

The cipher file C is given as C = (C1, C2)

Decryption

Given the message to be M and the Cipher C

i. Decryption is done using the private key (p, x)

ii. Obtain the cipher file C = (a, b)

iii. Compute a, such that a = (C1x) p-2 mod p

Compute M, such that M = (a * C2) mod p

Design of the ElGamal Algorithm

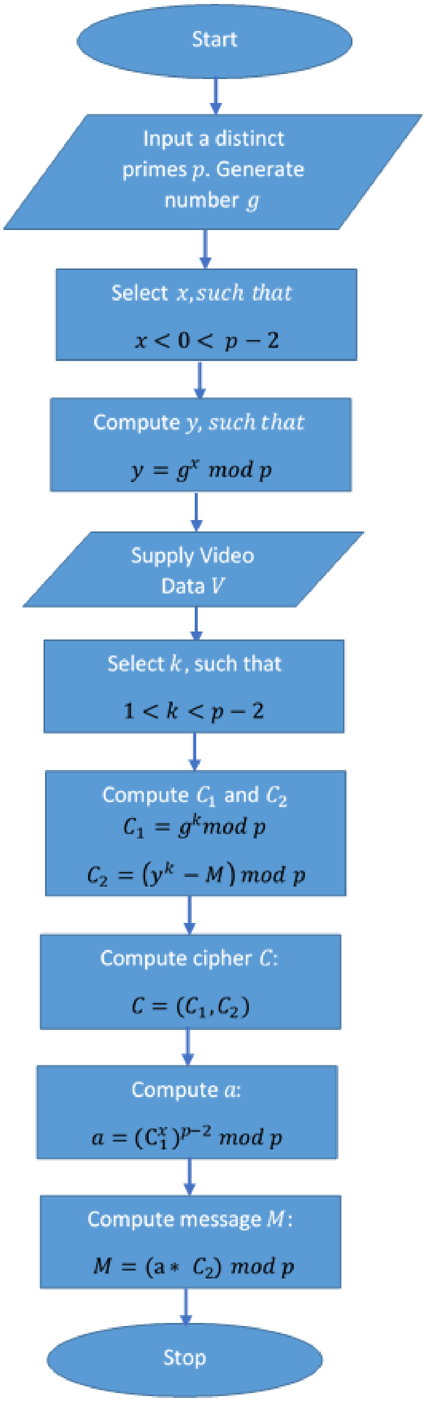
Start
Input a distinct primes p. Generate number g
Select x, such that $x < 0 < p - 2$
Compute y, such that $y = g^x \; mod \; p$
Supply Video Data V
Select k, such that $1 < k < p - 2$
Compute C_1 and C_2 $C_1 = g^k mod \; p$ $C_2 = (y^k - M) \; mod \; p$
Compute cipher C: $C = (C_1, C_2)$
Compute a: $a = (C_1^x)^{p-2} \; mod \; p$
Compute message M: $M = (a * C_2) \; mod \; p$
Stop

Figure 4: Flowchart for the ElGamal Algorithm Design

3. RESULTS AND ANALYSIS

This section provides a comprehensive overview of comparative study of the RSA and ElGamal cryptographic algorithms on video data, its features and how it functions. Information regarding the various methods used in designing this software application, as well as, how the software functions are discussed.

Results

The time taken to encrypt, and decrypt is given in seconds (s), while the original size and space used of the video data is given in kilobytes (kb). Table 1 to Table 4 display the tabular representation of comparative study of time and space used for both encryption and decryption of video data using RSA and Elgamal Cryptographic Algorithms.

Table 1: Encryption Time Taken for Video Data

S/N	Video Size (kb)	RSA Encryption Time Taken (s)	ElGamal Encryption Time Taken (s)
1.	282	10.525	22.114
2.	295	11.234	24.076
3.	733	26.077	55.411
4.	743	27.310	58.463
5.	848	31.363	72.252
6.	1740.8	33.501	93.143
7.	5120	86.124	245.332

Table 2: Encryption Space Used for Video Data

S/N	Video Size (kb)	RSA Encryption Space Used (kb)	ElGamal Encryption Space Used (kb)
1.	282	6786.44	848.29
2.	295	7096.51	887.04
3.	733	17841.30	2199.07
4.	743	17943.80	2230.14
5.	848	20358.91	2544.86
6.	1740.8	23924.38	4379.15
7.	5120	35546.20	10437.62

Table 3: Decryption Time Taken for Video Data

S/N	Video Size (kb)	RSA Decryption Time Taken (s)	ElGamal Decryption Time Taken (s)
1.	282	107.41	17.83
2.	295	113.49	19.58
3.	733	252.44	51.38
4.	743	261.61	56.43
5.	848	292.69	52.60
6.	1740.8	302.32	99.41
7.	5120	423.51	225.54

Table 4: Decryption Space Used for Video Data

S/N	Video Size (kb)	Space Used for RSA Decryption on Video data (kb)	Space used for ElGamal Decryption on Video data (kb)
1.	282	848.29	848.29
2.	295	887.04	887.04
3.	733	2230.14	2199.07
4.	743	2249.45	2230.14
5.	848	2544.81	2544.87
6.	1740.8	2832.74	4379.15
7.	5120	3479.80	10437.63

Graphical Analysis of the each Data Table

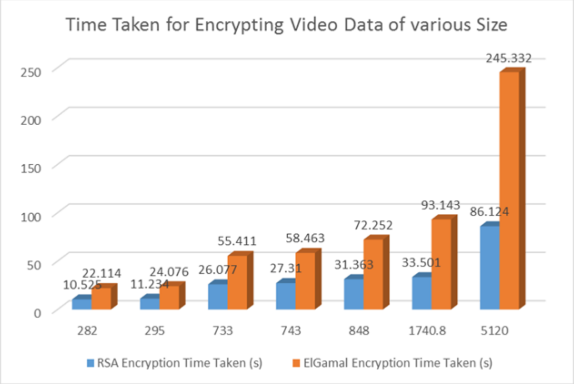

Figure 5: Graphical Display of Encryption Time of RSA and ElGamal on Video Data

From Table 1 and Figure 5, it can be deduced that RSA used lesser time during the encryption of video data while Elgamal Algorithm uses larger time for encrypting video data.

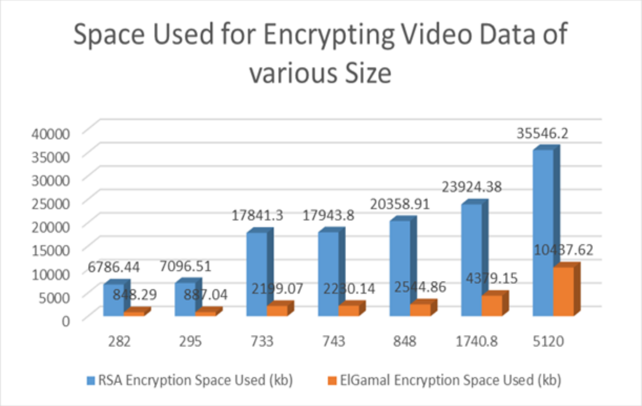

Figure 6: Graphical representation of Space Used for Encrypting Video Data

The Table 2 and Figure 6, shows that RSA algorithm generate larger files during encryption process, thus used large space for the cipher data while the cipher file ElGamal generate during encryption process is relatively low compare to RSA algorithm.

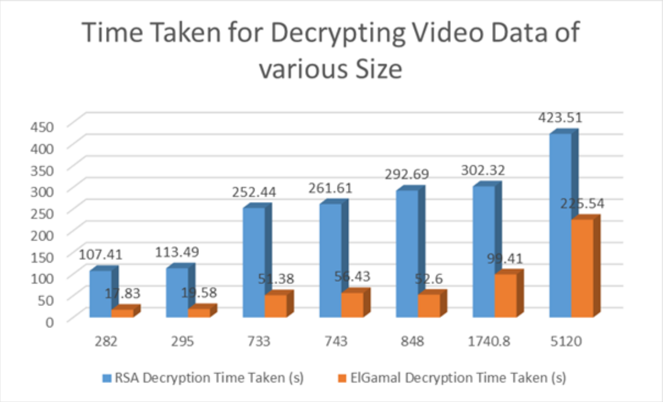

Figure 7: Graphical Display of Decryption Time Taken of RSA and ElGamal Algorithms on Video Data.

The Figure 7 and Table 4 shows that ElGamal used lesser time in decrypting video data of various file size while the time taken by RSA algorithm in decrypting video data pf various file size is relatively high.

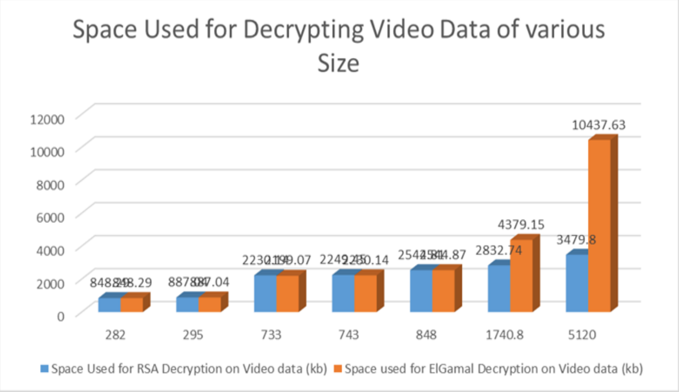

Figure 8: Graphical Display of Space Used by RSA and ElGamal Algorithms for Decrypting Video Data.

The Table 4 and Figure 8 shows that there is no significant difference between the space used by RSA and ElGamal algorithms a smaller file size during video data decryption but as the video file size increases RSA uses smaller space of memory compare to ElGamal algorithm that the space used increases as the video file size increases.

Result Interpretation

Based on the statistics in the tables as well as the graphical representation of each table, it can be deduced that the RSA performs better than the ElGamal while capturing the time used in encrypting video data, while the ElGamal algorithm performs better in terms of decrypting time of video data. It can also be deduced that ElGamal algorithm performs better in terms of space usage while encryption video data, while RSA algorithm performs better in terms of space usage while decryption video data.

4. CONCLUSION

The study conducted a comparative study on RSA and ElGamal cryptographic algorithm to determine the time and space complexities of both algorithms on video data. The study were able to compare and results of both algorithms and produce a result that suggests which of the algorithms is more efficient on video data. It was deduced that the RSA cryptographic algorithm is superior in terms of encryption time to the ElGamal cryptographic algorithm, and the ElGamal cryptographic algorithm superior in terms of decryption time to the RSA cryptographic algorithm. Also, it was observed that when the data sizes become bigger, both algorithms take a longer time to perform encryption and decryption of video data. From this study, it was concluded that RSA algorithm is time efficient for video data while ElGamal algorithm is memory efficient for video data. Moreover, with the amount of data that is being generated daily, it is therefore imperative that algorithms that can comprehend larger data sizes at a lesser time and memory usage should be developed to help improve infrastructure design, decision making and allocation of resources.

REFRENCES:

[1] Putera Utama Siahaan, A., Elviwani, E., & Oktaviana, B. (2018). Comparative Analysis of RSA and ElGamal Cryptographic Public-key Algorithms. In Proceedings of the Joint Workshop KO2PI and the 1st International Conference on Advance & Scientific Innovation (pp. 163-172). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

[2] Leger, S., Zwanenburg, A., Pilz, K., Lohaus, F., Linge, A., Zöphel, K., ... & Sak, A. (2017). A comparative study of machine learning methods for time-to-event survival data for radiomics risk modelling. Scientific reports, 7(1), 1-11.

[3] Yousri, D., Abd Elaziz, M., Oliva, D., Abualigah, L., Al-qaness, M. A., & Ewees, A. A. (2020). Reliable applied objective for identifying simple and detailed photovoltaic models using modern metaheuristics: Comparative study. Energy Conversion and Management, 223, 113279.

[4] Vigo, M., & Harper, S. (2017). Real-time detection of navigation problems on the World 'Wild'Web. International Journal of Human-Computer Studies, 101, 1-9.

[5] Panda, M. (2016). Performance analysis of encryption algorithms for security. In 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (pp. 278-284). IEEE.

[6] Whitman, M., & Mattord, H. (2005). Principles of information security.[University of Phoenix Custom Edition e-text]. Canada, Thomson Learning, Inc. Retrieved May, 4, 2009.

[7] Seth, S. M., & Mishra, R. (2011). Comparative analysis of encryption algorithms for data communication 1.

[8] Heinrich, F., & Morina, D. (2017). U.S. Patent No. 9,577,996. Washington, DC: U.S. Patent and Trademark Office.

[9] Siahaan, A. P. U. (2018). Comparative analysis of rsa and elgamal cryptographic public-key algorithms.

[10] Singanjude, M. D., and Dalvi, R. (2020). Secure and Efficient Application of Manet Using RSA Using Vedic Method Combine With Visual Cryptography and Identity Based Cryptography Technique. Available at SSRN 3570567.

[11] Suguna, S., Dhanakoti, V., and Manjupriya, R. (2016). A Study on Symmetric and Asymmetric Key Encryption Algorithms. International Research Journal of Engineering and Technology (IRJET), 2395-0056.

[12] Maqsood, F., Ahmed, M., Ali, M. M., & Shah, M. A. (2017). Cryptography: A comparative analysis for modern techniques. International Journal of Advanced Computer Science and Applications, 8(6), 442-448.

[13] Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., and Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. International Journal of Advanced Computer Science and Applications, 8(11), 333-344.

[14] Muneer B. Y., Shadi A., Ethar Q. et. al. (2017). Comprehensive Study of Symmetric Key and Asymmetric Key Encryption Algorithms. ICET2017, Antalya, Turkey. 978-1-5386-1949-0/17/$31.00 ©2017 IEEE

[15] Costello, C., Longa, P., and Naehrig, M. (2016, August). Efficient algorithms for supersingular isogeny Diffie-Hellman. In Annual International

Cryptology Conference (pp. 572-601). Springer, Berlin, Heidelberg.

[16] Aryanti, A., & Mekongga, I. (2018). Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher In Web Based Information System. In E3S Web of Conferences (Vol. 31, p. 10007). EDP Sciences.

[17] Sann, Z., thi Soe, T., Knin, K. W. M., and Win, Z. M. (2019). Performance comparison of asymmetric cryptography (case study-mail message). APTIKOM Journal on Computer Science and Information Technologies, 4(3 November), 105-111.

[18] Okeyinka, A. E. (2015) "Computational Speeds Analysis of RSA and ElGamal Algorithms on Text Data" Proceedings of the World Congress on Engineering and Computer Science 2015 Vol I WCECS 2015, October 21-23, 2015, San Francisco, USA.

[19] Bos, J., Kaihara, M., Kleinjung, T., Lenstra, A. K., & Montgomery, P. L. (2009). On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography (No. REP_WORK).

[20] Dindayal M and Dilip K.Y. (2018). Performance Analysis of RSA and Elliptic Curve Cryptography. International Journal of Network Security, Vol.20, No.4, PP.625-635, July 2018 (DOI: 10.6633/IJNS.201807 20(4).04).

[21] Vassilev, T. S., & Twizell, A. (2012). Cryptography: A Comparison of Public Key Systems.

[22] Kumar, M. G. V., & Ragupathy, U. S. (2016). A Survey on current key issues and status in cryptography. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 205-210). IEEE.

[23] Nwe, T. Z., & Phyo, S. W. (2014). Performance Analysis of RSA and ElGamal for Audio Security. International Journal of Scientific Engineering and Technology Research, 3(11), 2494-2498.

[24] Abari Ovye John, P.B. Shola, & Simon Philip (2015). Comparative analysis of discrete logarithm and RSA Algorithm in data cryptography. International Journal of Computer Science and Information security. (ISSN 1947-5500 Volume 13–No.2, 2015).

[25] Kyaw Myo Thu | Kyaw Swar Hlaing | Nay Aung Aung "Time Performance Analysis of RSA and Elgamal Public-Key Cryptosystems" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.448-450, URL: https://www.ijtsrd.com/papers/ijtsrd28096.pdf