International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-13 Issue-5, April 2024

A Novel Cycle Leader Permutation with Elgamal Algorithm for Image Encryption

Boggana. Vandana, Kanusu. Srinivasa Rao, Buduri. Reddaiah, Bodi. Susheel Kumar

Abstract: ***As more people use networks in whatever capacity, security-related issues come up more frequently. These issues could be external to the network or internal to it. To address the security-related problems, the science of cryptography and network security enables the protection of resources, data quality, and network infrastructure. Firewalls and filters are utilized across many workstations to safeguard the resources. However, security services are required to protect the data during transmission to prevent unauthorized access. To guard against attacks, these services must be changed often. This paper integrates Cycle Leader permutation with Elgamal algorithms to construct such a system. These hybrid solutions can be used to prevent hackers from gaining unauthorised access to different commercial applications.***

Keywords**:** ***Encryption, Decryption, Key, Cycle Leader Permutation, Elgamal.***

I. INTRODUCTION

Electronic commerce is becoming the norm for most corporate organisations, and they are encouraging users to adopt this approach. The widespread usage of networks and the internet has made this possible. Currently, the most important thing for industry is to securely communicate via secure communication channels to transmit confidential information about individuals engaged in commercial activities. The hackers must transfer sensitive data in an unexplainable way [4]. To accomplish this kind of secure communication, one technique and field of study that contributes to security is cryptography. This sequence of events and activities provides the security services in the secured communication channel. In places where data is sent across networks, security services are required. Unauthorized users attempt to have control over moving data. Confidentiality, authenticity, and data integrity may be compromised if unauthorised access is obtained to data. A suitable protection method must be employed to transfer data securely and guard against such security breaches.

Manuscript received on 30 March 2024 | Revised Manuscript received on 05 April 2024 | Manuscript Accepted on 15 April 2024 | Manuscript published on 30 April 2024.

**Correspondence Author(s)*
Boggana Vadana, Department of Computer Science and Technology, Yogi Vemana University, Kadapa-516005, India. Email: bbogganavandana@gmail.com, ORCID ID: 0009-0006-5090-2792
Kanusu. Srinivasa Rao, Associate Professor, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: kanususrinivas@gmail.com
Buduri. Reddaiah*, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: prof.reddaiah@yvu.edu.in, ORCID ID: 0000-0002-5851-2194
Bodi. Susheel Kumar, Department of Computer Science and Technology, Yogi Vemana University, Kadapa, India. Email: bjayakarunya@gmail.com

The study of cryptography focuses on protecting data during transmission from unauthorised access. This science utilises mathematical concepts to both encode and decode data. The strength of each newly constructed system depends on the encryption that is created during encoding [5]. This science aids in the investigation and creation of novel cryptosystems that may help prevent unauthorised users from taking action. Elgamal algorithms and Cycle Leader permutation are used in this study to develop a novel hybrid system. These techniques facilitate the development of complex cryptosystems. These kinds of systems are particularly challenging to understand and need more effort to break.

A. Types of Attacks in the Network

A threat is something that has the potential to harm the user's data. A threat can be an object, a unit, or a program that characterises a scheme of risk. Due to the widespread use of the internet these days, a sizable number of people are connected, and their data is stored on internet servers. Likewise, social, personal, and professional activities rely on the internet. These factors enable unauthorised users to compromise resources and impact the availability of internet services. Network security becomes essential considering the numerous anomalies, attacks, and threats. Attacks are classified as either passive or active, as they cause the most significant harm to interconnected systems. In terms of passive attack, it simply involves data flow analysis, traffic analysis, eavesdropping, and monitoring [6]. Active attacks include stopping data while moving, as it travels from one place to another, as well as altering, fabricating, and stopping data [7].

II. BACKGROUNG STUDY

Moatsum Alawida proposes a novel picture encryption technique with minimal processing time, based on an improved chaotic map. They introduced a unique hybridised forward-backwards perturbation map, based on a novel perturbed logistic chaotic map.

Compared to other chaotic systems already in use, it exhibits superior chaotic qualities, including a wide chaotic range, increased sensitivity, and unpredictability. Based on this, a novel image encryption method is described that uses two substitution operations and a special permutation operation to achieve superior encryption speed and efficiency. They used a chaotic data sequence as its basis; the unique permutation operation generates 8-bit values by using all chaotic states. The last 8-bit number's indexes are combined into a single block [1].

Sandip Kumar Bhowmick et al. suggested a modified version of ElGamal encryption that offers high information rate digital signatures and data secrecy.

ElGamal's security is solely dependent on how difficult it is to factor discrete logarithm problems, where it is highly challenging to determine discrete logarithms over finite fields using statistical or brute force methods. This suggested technique improves the algorithm by adding a key and an arbitrary number to the standard one, increasing the deciphering difficulty and decreasing the time complexity to decode the message, in response to the ongoing challenges to the security of the ElGamal scheme [2].

Alejandro Freyre Echevarrıa provided a graph description of S-boxes along with optimization techniques to generate complete cycles per cryptographically secure mutations [3].

Rajesh P. Singh presented a permutation polynomial-based multivariate encryption technique that is effective across finite fields. The authors developed a trapdoor function for the cryptosystem by using polynomials in L(2,m), where m = 2k for any k > 0 [8].

To increase security, Rahmadi Asri et al. suggested using the split-merge approach with the El-Gamal algorithm. The paper explains the design and analysis of the system. Large prime number computations are used in the combination, which makes it more difficult for cryptanalysts to decipher the plaintext [9].

Akash Thakkar and Ravi Gor presented a technique for cryptography that utilises the Kamal Transform and ElGamal algorithm to enhance communication security. Further security for information communication cannot be achieved by encryption and decryption systems based on the Kamal Transform applications. The discrete logarithm issue is the foundation of the public key ElGamal algorithm [10].

III. PROPOSED SCHEME

This proposed system is primarily based on cycle leader permutation, which permutes the values generated from the input image. Along with the cycle permutation Elgamal algorithm, it is also used in encryption and decryption.

A. Cyclic Permutation

In group theory in particular, a cyclic permutation is a permutation consisting of a single cycle [11,12]. Cyclic permutations are sometimes called cycles [13]. A cyclic permutation may be referred to as a k-cycle if it has k elements. More than just one non-trivial cycle, a few authors expanded this idea to include permutations with fixed points [13, 14]. Cycles are also the separate cyclic components of a permutation. Cyclic permutations are represented in cycle notation by a list of their elements, permuted in the order indicated by the parentheses around the elements. A cyclic permutation's orbit is the collection of items that it does not fix. It is possible to break down every permutation on a limited number of components into cyclic permutations on disjoint orbits.

B. Elgamal Algorithm

ElGamal's security is solely dependent on how difficult it is to factor discrete logarithm problems, where it is exceedingly challenging to use statistical or brute force attacks to determine discrete logarithms over finite fields. ElGamal, developed by Taher ElGamal in 1985 as a successful implementation of the Diffie-Hellman algorithm, gained prominence as one of the most well-known public-key cryptography algorithms after the Diffie-Hellman key exchange algorithm. Diffie and Hellman initially proposed the idea of asymmetric key cryptography, sometimes known as public key cryptography, in 1976.[15]. It is a modified version of the Diffie-Hellman algorithm that offers a digital signature for message authentication in addition to allowing the exchange of messages rather than simply keys [16][17].

Among the widely used encryption algorithms is the El-Gamal algorithm. Generally, communications are encrypted using the El-Gamal algorithm. A straightforward and effective cryptographic technique is part of the El-Gamal algorithm [18]. Since this technique can perform multiple factorisations, calculating key creation using random values is relatively secure. El-Gamal is thereby able to withstand cryptanalyst assaults while maintaining communication security.

IV. PROPOSED SYSTEM

A. Framework of Key Generation

In this framework, the key for the encryption and decryption process is generated using primitive roots, as shown in Figure 1.

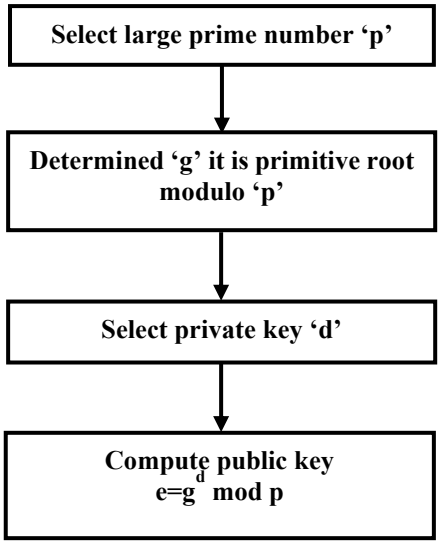

Fig. 1. Block Diagram of Key Generation Process

B. Key Generation Algorithm

The proposed algorithm (Figure 1) illustrates a step-by-step procedure for key generation using primitive roots.

Proposed Key Generation Algorithm-1

Step 1. Select a huge prime number denoted by p
Step 2. Determine 'g' and it is a primitive root of modulo 'p'
Step 3. Select **private Key** denoted by d '
Step 4. Compute the **public key** denoted by **'e'**
$e = g^d \bmod p$

C. Framework of Encryption Process

The proposed framework outlines a step-by-step procedure for encryption, which involves converting original images into encrypted images, as illustrated in Figure 2.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

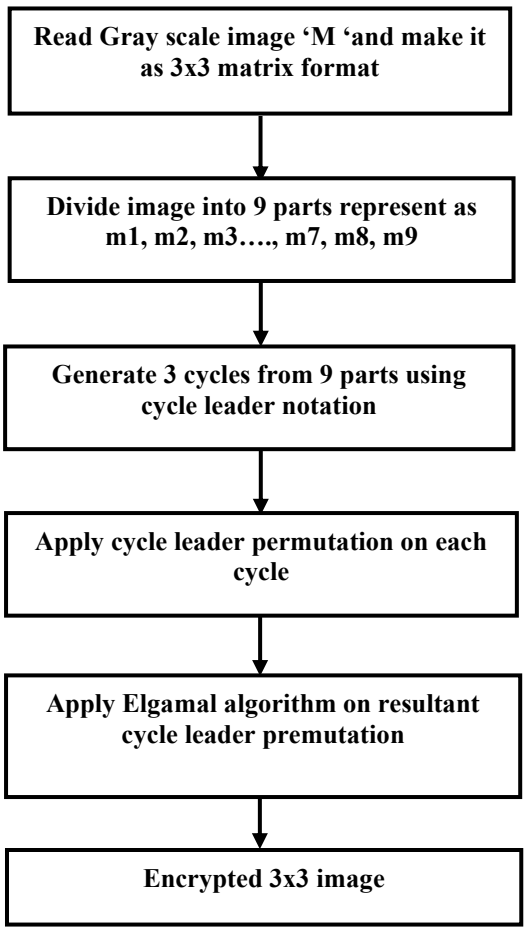

Fig. 2. Block Diagram of Encryption Process

D. Encryption Algorithm

The proposed algorithm 2 illustrates a step-by-step procedure for encryption, which involves converting the original image into an encrypted image, as shown in Figure 2.

Proposed Encryption Algorithm-2

Step 1. Read gray scale image
Step 2. Convert a grey-scale image into a 3x3 matrix format
('M'), With nine parts.
Step 3. Among nine parts, three cycles are generated using
cycle leader notation.
Cycle 1 – (1 3 5)
Cycle 2 – (2 4 6 9)
Cycle 3 – (7 8)
Step 4. Apply the cycle leader permutation on each cycle
Step 5. Apply the ElGamal technique on the newly generated
3x3 matrix.
Step 6. The resultant is the Encrypted image

E. Framework of Decryption Process

The proposed framework outlines a step-by-step procedure for decryption, which involves converting encrypted images into their original form, as illustrated in Figure 3.

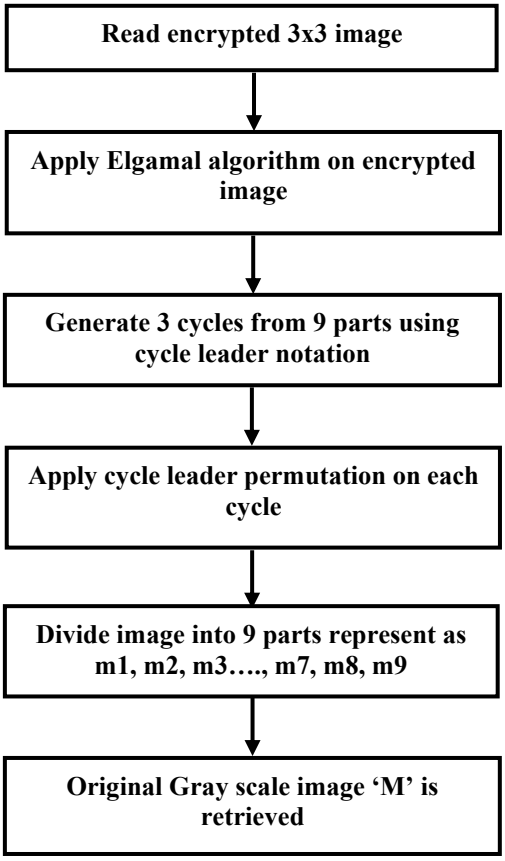

Fig. 3. Block Diagram of Decryption Process

F. Decryption Algorithm

The proposed algorithm 3 illustrates a step-by-step procedure for decryption, which involves converting encrypted images into their original form, as shown in Figure 3.

Proposed Decryption Algorithm-3

Step 1. Read the encrypted image represented as a 3x3 matrix
Step 2. Apply the ElGamal algorithm on the encrypted image
Step 3. Among nine parts, three cycles are generated using
cycle leader notation.
Cycle 1 – (8 7)
Cycle 2 – (2 9 6 4)
Cycle 3 – (1 5 3)
Step 4. Apply the cycle leader permutation on each cycle
Step 5. Generate 3x3 matrices with nine parts represented as
m1, m2, m3, m7, m8, m9.
Step 6. The resultant is the original grey-scale image

V. RESULT AND DISCUSSION

The key generation algorithm uses a prime number and its primitive root. The key for encryption and decryption is derived as shown in Table I.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table I: Outcome of Key Generation Process

Choose a Random Prime Number 'p'	Primitive Root Modulo 'p'	Choose a Random Private Key	Compute Public Key 'e' using Primitive Root 'g', Prime Number 'p', and Primitive Key'd $e = g^d \bmod p$
P=23	g=5	D=6	E=8

The original image's encryption technique, which utilises a 3x3 matrix of its ASCII code, is shown in Table I to produce the encrypted image.

Table II: Outcome of Encryption Process

3x3 Matrix Pixel Values for Original Grey Scale Image	Cycle Permutation On the original Grey Scale Image	Elgamal Algorithm on Cyclic Leader Permutation	Encrypted Grey Scale Image Pixel Values
100 150 200 50 75 125 25 175 225	100 150 75 125 200 225 175 25 50	4,200 4,300 4,150 4,250 4,400 4,450 4,350 4,50 4,100	4,200 4,300 4,150 4,250 4,400 4,450 4,350 4,50 4,100

The decryption algorithm used on the encrypted image is considered in a 3x3 matrix, as shown in Table II, to obtain the original image.

Table III: Outcome of Decryption Process

Encrypted Grey Scale Image Pixel Values	Inverse Elgamal Algorithm on Cyclic Leader Permutation	Inverse Cycle Permutation On the Original Grey Scale Image	3x3 Matrix Pixel Values for Original Grey Scale Image
4,200 4,300 4,150 4,250 4,400 4,450 4,350 4,50 4,100	100 150 75 125 200 225 175 25 50	100 150 200 50 75 125 25 175 225	100 150 200 50 75 125 25 175 225

VI. CONCLUSION

This study proposes an enhanced security version of the Elgamal cryptosystem for signature creation and encryption. This paper provided a novel approach to experimental mathematics that blends the Elgamal algorithm, cyclic leader permutation-based computing, and traditional mathematical progress. Since the suggested method outperforms the original ElGamal scheme in terms of information rate, it is anticipated that digital data transmissions would be safe. Due to the discrete logarithm problem and the difficulty of factoring large numbers to obtain the private keys, the security of the modified method depends entirely on the difficulty of obtaining the private keys. The strength and efficiency of cyclic permutation-based cryptography systems should be enhanced as part of future research to make them competitive choices in the rapidly evolving fields of data security and secure communications.

DECARATION STATEMENT

Funding	No, I did not receive.
Conflicts of Interest	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval or consent to participate, as it presents evidence that is not subject to interpretation.
Availability of Data and Materials	Not relevant.
Authors Contributions	All authors have equal participation in this article.

REFERENCES

1. Moatsum Alawida, "A novel chaos-based permutation for image encryption", Journal of King Saud University-Computer and Information Sciences, 35 (2023) 101595, pp. 1–21. https://doi.org/10.1016/j.jksuci.2023.101595
2. Sandip Kumar Bhowmick et al., "Modified Elgamal Cryptosystem for Public-Key Encryption and Digital Signature", International Journal of Pharmacy & Technology, Dec-2016, Vol. 8, Issue No. 4, pp. 26578-26583.
3. Alejandro Freyre Echevarria et al., "A graph theory approach to heuristic generation of cyclic permutations", Springer Nature 2021, pp. 1-16.
4. A. H. Zahid, E. Al-Solami, and M. Ahamad, A Novel Modular Approach Based Substitution-Box Design for Image Encryption", IEEE Access, vol. 8, pp. 150326-150340. 2020. https://doi.org/10.1109/ACCESS.2020.3016401
5. R. Bhanot, and R. Hans, "A Review and comparative Analysis of Various Encryption Algorithms:, International Journal of Security and Its Applications, vol. 9, No. 4, pp. 289-306, 2015., to be published. https://doi.org/10.14257/ijsia.2015.9.4.27
6. Neha Khandelwal, Prabhakar. M Kuldeep Sharma, "An Overview of Security Problems in MANET".
7. Stallings. W (2006), Cryptography and Network Security, Fourth Edition, Prentice Hall.
8. Rajesh P. Singh et al., "A Public Key Cryptosystem Using a Group of Permutation Polynomials", Mathematical Institute, Slovak Academy of Science, pp. 139-162.
9. Rahmadi Asri et al., " Modification of Ciphertext Elgamal Algorithm using Split Merge", The 3rd International Conference on Computing and Applied Informatics-2018, Journal of Physics: Conference Series, 1235 (2019) 012054, pp. 1-7. https://doi.org/10.1088/1742-6596/1235/1/012054
10. Akash Thakkar, Ravi Gor, "Cryptographic method to enhance the Data Security using ElGamal algorithm and Kamal Transform", IOSR Journal of Computer Engineering, vol. 24, Issue. 3, pp. 08-14.
11. Gross, Jonathan L. Combinatorial Methods with Computer Applications. Discrete mathematics and its applications. Boca Raton, Fla.: Chapman & Hall/CRC. P.29 (2008).
12. Knuth, Donald E. The Art of Computer Programming. Addison-Wesley. P. 35 (2002).
13. Bogart. Kenneth P. Introductory combinatorics (3rd ed). London: Harcourt Academic Press. P. 554 (2000).
14. Rosen, Kenneth H. Handbook of discrete and combinational mathematics. Boca Raton, London, New York: CRC Press.
15. Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126. https://doi.org/10.1145/359340.359342
16. Merkle, Ralph, and Martin Hellman. "Hiding information and signatures in trapdoor knapsacks." IEEE transactions on Information Theory 24.5 (1978): 525-530.4 4 https://doi.org/10.1109/TIT.1978.1055927
17. P. M. Durai Raj Vincent, Sathiyamoorthy E, " A Novel and efficient public key encryption algorithm" International Journal of Information and Communication Technology, Vol. 9, No. 2, pp 199-211, 2016. https://doi.org/10.1504/IJICT.2016.10000121
18. Z Wu, D Su, G Ding. 2014. ElGamal Algorithm for Encryption of Data Transmission. In Proc. of Int. Conf. on Mechatronics and Control (ICMC)

AUTHORS PROFILE

Boggana Vandana is studying for an M.C.A. in the Department of Computer Science and Technology at Yogi Vemana University, Kadapa, Andhra Pradesh. She is passionate about learning new technologies and developing new methods. She has a strong interest in developing new techniques and exploring new technologies. She is keen on conducting security-related research with real-world applications and hopes to expand into a comprehensive security service provider. She also aspires to be a software developer in the security sector. Her leadership in several projects demonstrates her commitment to resource management and the growth of technological innovations. Sasikala's contributions to this study provide a comprehensive understanding of the scalability challenges facing the security sector.

Kanusu. Srinivasa Rao is working as an Associate Professor in the Department of Computer Science and Technology at Yogi Vemana University, Kadapa, Andhra Pradesh. He has published 40 papers related to Image Processing and Security. His research interests include Image Processing, Cryptography, and Network Security. Kanusa's commitment to investigating the nexus between security and technology is essential to the creation of reliable solutions. His research highlights the value of using systematic techniques to create models for security and upkeep. He symbolizes the collaborative attitude of this study team as the corresponding author.

Buduri. Reddaiah is working as an Associate Professor in the Department of Computer Science and Technology at Yogi Vemana University, Kadapa, Andhra Pradesh. His research interests are in security and Artificial Intelligence. With a focus on network security and Artificial Intelligence, his research endeavours to enhance data integrity and access control mechanisms. Reddaiah's dedication to exploring the intersection of technology and security plays a crucial role in the development of robust systems. His work emphasises the importance of methodical approaches to developing models in security and maintenance. As the corresponding author, he embodies the collaborative spirit of this research team.

Bodi. Susheel Kumar is working as an Academic Consultant in the Department of Computer Science and Technology, Kadapa, Andhra Pradesh. His research areas include Cryptography and Network Security, and he has published numerous papers in these fields. He is a significant contributor to this study due to his expertise and commitment to programming with new technologies, as well as his efforts to promote a deeper understanding of the role of technology in this work. He has a strong desire to work as a developer. His dedication to his career is evident in his leadership of various activities. Susheel's contributions to this work provided a thorough understanding of the scalability issues associated with security-related online applications.