An Advanced Energy Efficient Lightweight ElGamal Cryptography Technique for IoT Device

Deepika Rani Sona [1,a)], Regulapati Amulya [2, b)], Navina K.[3,c)], Kalapraveen Bagadi[4,d)]

[1,2,3]School of Electronics Engineering, Vellore Institute of Technology, Vellore, India-632014
[4]School of Electronics Engineering, VIT–AP University, Amaravati, India-522237
[a)]deepika.rs@vit.ac.in, [b)]regulapati.amulya2020@vitstudent.ac.in, [c)]navina.k2020@vitstudent.ac.in, [d)]Corresponding author: kpbagadi@gmail.com

Abstract: These days, both industry and academics have paid significant attention to the Internet of Things (IoT). It enables connections between people and things at anytime, anywhere, with anything, and with everyone, preferably via any path, network, or service. One vision for the future is that IoT develops into a utility with improved sensing, actuation, communication, control, and knowledge creation from massive data. Additionally, these device's computation, memory, and power consumption are constrained. How to provide security in such resource constrained devices is a significant challenge. This research aims to propose an improved energy efficient lightweight cryptography technique (EELCT) for IoT devices. The authors used the ElGamal algorithm to generate public and private keys, input encryption, and decryption. The authors also compare the performance of ElGamal, RSA, and Paillier approaches using MATLAB. The proposed method uses an 8-bit manipulation concept, which requires less power and memory, making it suitable for energy-limited IoT devices. The outcomes show that the suggested solution performs better in terms of power consumption, memory usage, and execution time, making it a viable choice for protecting IoT devices.

Keywords: Cryptography, Internet of Things (IoT), Lightweight, Encryption, Decryption, Security.

INTRODUCTION

Recently, the IoT technology has become popular with the availability of low cost and efficient wireless sensors [1–3]. Nowadays, the IoT technology is used in many engineering applications [4–6]. The IoT is a typical organization comprising regular members who can recognise and communicate with similar devices over the Internet. Cyberattacks can seriously disrupt any industrial setup if the server receives inaccurate information, leading to poor management as the outcome of the inadequate analysis. This is a serious security problem that has to be resolved. Our research goal is to create a cryptography technique that can effectively encrypt and decrypt data being delivered across a variety of IOT devices. Recent research has more of an emphasis on security challenges than on making things simpler. Numerous hardware devices and sensors are accessing and transferring information gathered from the Internet due to the broadband web's organization with high speed and low cost. This technological development offers the best plan for advancing IoT as the Internet of Everything (IoE) in the future. The complexity of IoT has also substantially increased because anything may send data to other devices online from anywhere in the world. This extremely useful data sharing over an IoT platform must be transmitted more securely to another device. The following are the three main causes of IoT being easily attacked by online criminals.

(a) IoT lacks a management system or an intelligent way to recognise intruders.
(b) Because IoT uses a wireless channel, spying is relatively easy.
(c) The Internet of Things accepts low computational capabilities and low energy usage

The science of cracking codes for secure communication is known as cryptography. In order to guarantee total security in IoT systems, the symmetric cryptography method, which uses the same key for both the encryption and decryption processes, must be used.

An encryption technique with little computational effort or both is known as lightweight cryptography. Its goal is to expand the use of cryptography on limited devices, and its international standardization and compilation of guidelines are now underway. A technical competition called CAESAR has been launched to support verified encryption that meets confidentiality and integrity requirements. In order to pass the second round of CAESAR selection, NEC developed a compact TWINE block cypher and an authorised OTR encryption method.

Symmetric key and public key (asymmetric key) are the two basic subcategories of cryptography. Symmetric key cryptography encrypts and decrypts data using the same secret key. Data encryption and authentication is done using processing that is reasonably lightweight. Conversely, public key cryptography employs a public key that is distinct from the secret key that is used for encryption and the secret key that is used for decryption, making it extremely difficult to extract the secret key from the public key. Public-key cryptography is used to share the secret key used in both symmetric-key cryptography and digital signatures, while having a computational complexity that is typically 1000 times greater than that of symmetric-key encryption.

Wide applications of symmetric key cryptography are available for hardware with significant resource limitations. The methods used to apply a fundamental function for encryption or authentication to a packet are referred to as a block cypher's mode of operation. Stream cyphers and block cyphers are two instances of fundamental symmetric key cryptography operations. Lightweight cryptography – The two-way key rule allows end devices to consume less power. Even for nodes with limited resources, lightweight cryptography provides the benefit of providing secure encryption devices. Factors to consider when deploying lightweight cryptography are energy, power consumption, size, latency, and processing speed.

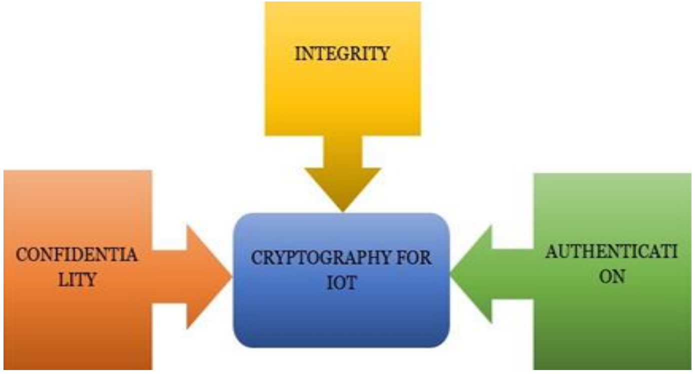


FIGURE 1. A Cryptographic system for IoT

Figure 1 provides the blocks of Cryptography fot IoT devices. This shows confidentiality, where the data isn't shared with any outsiders, Integrity and Authentication, where proper security should be done before giving access to data.

RELATED WORK

A power diffusion strategy is proposed in light of NASH bargaining arrangements to exploit the most inaccessible burgeons [7] effectively. In addition, available receive wire innovations are reviewed, and an ideal plan is suggested for maximum energy extraction from a low-power RF signal. Utilizing these approaches, battery powered sensor hubs can meet the planned goals of life expectancy, absolute cost, extraordinary performance, transmission inclusion, and consistency. For the Internet of Things (IoT), simple cryptographic techniques are examined in [8]. This overview compares many block cypher versions and covers a range of security measures, including lightweight cryptographic techniques. Advanced Encryption Standard (AES) works well as a security solution for constrained IoT devices. The authors in [9] focus on IoT devices with minimal resources because they can be challenging to protect under these circumstances (such as RFID tags, sensors, smart cards, etc.). There are more than fifty lightweight cryptography (plain encryption) algorithms available in the market that concentrate on a specific usage or application, and researchers have submitted another 57 techniques to the NIST competition. This evaluation compares various block cypher variations and lightweight cryptographic techniques, among other security measures. The study initiated that lightweight AES works well as a security solution for constrained IoT devices [10, 11]. This work discusses the security threats, requirements, and patterns related to IoT cryptography, technologies, and trends. The study also looks at the challenges faced and a comparison of existing IoT security solutions. This study in [12] focused on the performance of LoRaWAN, an open standard that specifies a communication protocol for Low-Power Wide Area Network (LPWAN) technology and Lightweight cryptographic(LWC) algorithms for intelligent IoT devices implementation, difficulties, and potential uses.

Authors in [13] examine some recent advancements in the development of lightweight algorithms as well as a variety of techniques to replace conventional cryptography in the context of the Internet of Things. The study in [14, 15] featured two components using formulas, and the rectangle method was conducted using the mathematical performance tests (MAT) and the trigonometric diagnostic test (TDT). The purpose of the study was to determine student's errors in learning trigonometry. Fifty-two block cyphers and 360 implementations are reviewed for security, effectiveness, and cost. They are then grouped based on how well they function with different types of embedded devices, and the most notable cryptanalysis relevant to these cyphers is given [16]. With a 64-bit block length and 128-bit key length, it suggests a new HIGHT block cypher [17]. It offers a hardware solution with cheap resources that is built into a ubiquitous computing device, like an RFID tag or a sensor in a USN. HIGHT is made up of simple operations and is extremely lightweight, yet it also has solid encryption and is a sufficiently secure algorithm**.**

The proposed solution used variable block sizes to make it easier to apply on different IoT devices with different memory capacities [18]. A novel lightweight encryption technique dubbed LRBC was presented in this study [19] that can guarantee data security at the sensing level. To improve security, LRBC combines the structural benefits of the Feistel structure and substitution permutation network (SPN). The suggested algorithm uses a very little amount of power—11.40 W—and takes up only 258.9 GE.

Furthermore, a detailed security study in [20] demonstrates that the proposed approach offers solid security against a variety of assaults. Additionally, it is discovered that for plaintext and key, respectively, the average avalanche effect of LRBC is 58% and 55.75. Authors in [21] compare NIST's well-defined LWC (cost, performance, and security) features and identify additional research gaps and open research problems. According to a literature review, NIST approved PRESENT and CLEFIA as two block cyphers due to security concerns as well as claimed performance and cost. However, SIMON and SPECK stand out because their implementations are as small as possible. None of the LWC algorithms generally meet all necessary performance benchmarks for hardware and software, but all perform optimally in a given environment. FlexCrypt, an automated lightweight cryptographic protocol, is introduced for WSNs, in [22]. A completely new dynamic clustering method was created for the FlexCrypt scheme, which supports the mobility of sensor nodes.

Lightweight and ultralight block cyphers are being developed by researchers [23, 24] for various applications that are resource constrained in nature. Evaluation results reveal that Kryptein performs two orders of magnitude better than cutting-edge systems like CryptDB and Talos in terms of compute time and power consumption on embedded client devices, are projected in [25]. In terms of increasing the battery life of IoT devices by about 35%, it performs better than cutting-edge IoT cyphers (Simon and Speck). Only a fairly simple formula was needed to calculate the statistics. Kryptein calculated statistics for one data segment (one matrix multiplication) with high accuracy (96%) without having to decode the original data.

With the introduction of 5G, the Internet of Things (IoT), which has a wide range of applications across numerous areas, has essentially become the focus of all organizations [26, 27]. Focusing on lightweight block cyphers, this study compares performance alongside reported cryptanalysis and identifies new research opportunities for developing unique algorithms that strike the ideal balance between cost, performance, and security properties [28]. The study in [29] compares ten practical cryptographic algorithms and provides a fair overview of their memory usage and speed. Based on the balance between the ideal methods. The IoT platform has constrained physical dimensions, internal storage capacity, other storage allocations like RAM/ROM, and transfer rates [30]. Devices are often powered by batteries; therefore, it is crucial to keep the energy charged for at least a few years. However, it is difficult to provide adequate security because the IoT cannot use current cryptographic techniques due to their weight. As a result, there has been a current interest in the development of new cryptographic algorithms on a small scale, even as initiatives are still trying to be more resilient to the advanced risks and dangers of the IoTs. There are not enough studies in the literature to provide comprehensive and up-to-date information on lightweight cryptography.To avoid any unwanted access or unnecessary interruptions in healthcare systems, it is important to guarantee the trust and privacy of the data from the beginning of the sensors throughout the medical treatment [31]. Therefore, encryption of data from the very first sensors is required, but due to the limitations of computational complexity, energy consumption, and communication bandwidth, the use of standard cryptographic algorithms currently available is absolutely impractical. Authors in [32] recommend quantum cryptography as a longterm security option for IoT. This article discusses the necessity of an IoT security system. It shows that quantum cryptography (QC) is the best choice for long-term IoT security. The currently used methods are doomed to failure in the long term. All expected security threats can be handled through quality control.

METHODOLOGY

Elgamal Algorithm

Data communication and data protection depend heavily on security. It helps prevent unwanted access to sensitive data that could lead to data loss or alteration by unidentified parties, making data transmission unsafe.

Figure 2 shows the workflow of the ElGamal algorithm. Public key cryptography is used in ElGamal encryption. For two-party communication, it encrypts the message and employs asymmetric key encryption. This cryptosystem is based on the fact that, even with knowledge of g_k and g_a, the discrete logarithms in the cyclic group, it is difficult to calculate g_{ak}.

If we want to understand the whole picture, we have to go step by step by actually encrypting and decrypting the messages. We will use the example of two peers willing to exchange data using the ElGamal technique securely. Consider that User–1 and User–2 wish to transmit information covertly, in which case the steps below will be performed.

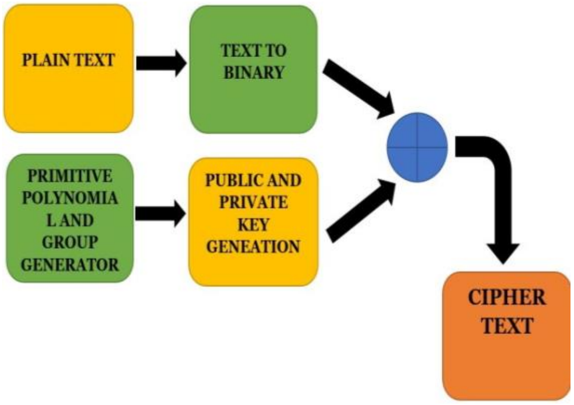

PLAIN TEXT
TEXT TO BINARY
PRIMITIVE POLYNOMIA L AND GROUP GENERATOR
PUBLIC AND PRIVATE KEY GENEATION
CIPHER TEXT

FIGURE 2. Process flow of ElGamal algorithm.

Step 1: Public and Private Key Generation.

User–1 attempts to choose a cyclic group and a very lengthy or large integer, x. Additionally, it will choose component b and the subsequent element c from this cyclic group. The values will be selected in a way that, when the desired function is employed, the outcome equals to 1.

The value will be calculated following the value selection process and used to create the private key. The equation f_m=b_c will be used to calculate the value. In this instance, User 1 selects F as his public key, where f_m = bc, a, and b. A private key composed of the values of a will be retained and utilised in future.

Step 2: User–2 encrypts the data using user1's public key.

There are specific settings that User–2 must select in order to begin encrypting a message. Additionally, the User–2 will need to select one of the cyclic group's p values. A cyclic group will be utilised, similar to User–1. It is important to choose the value so that it passes through and produces a 1 in the designated function.

The message will be encrypted with the public key using some additional values generated by User–2. $P_m = b_p$ is the value that will be created. b_c and b_{ap} will be equal after the second reevaluation. This calculation's outcome will be multiplied by the second variable Z to gain a closer estimate of the encryption method. The value will eventually be utilising the computations' results to b_p, $Z\times b_{ap}$.

Step 3: Decrypt the message at user 1's end.

Computing the values selected in the first and second phases, User–1 eventually determines the proper number that will be utilised to decrypt the encrypted message. User–1 processes bap and divides the result by Z to obtain the decrypted value. In the second stage, something was encrypted, and that something was the value that was decrypted. The algorithm's heart and soul are the private and public keys, which User–1 calculated to start the process in the example above. In the following stage, User–2 continues to encrypt the method using the key. The message is encrypted so it can be decrypted using the value calculated in the initial phase. In the third stage, it was seen that after dividing the full value by the number generated in the third step, the message was completely decrypted, allowing the end user to read it. The same procedure is used every time the impulse arises to send a message securely.

Mathematical Model of ElGamal Algorithm

The ElGamal algorithm is a public-key encryption method that encrypts and decrypts messages using the characteristics of discrete logarithms in a finite field. Here is the mathematical equations and execution process for the ElGamal algorithm:

Key Generation:
Select a high prime number p.
For the cyclic group Z_p, select a generator g. Pick a secret random number a, such that $1 \leq a \leq p - 2$.
Determine $A = g \times a \bmod p$ and publish it as the public key.
As the private key, keep A secret.

Encryption:
The message m should be transformed into an integer between $[0, p - 1]$.
Pick a random integer k, such that $1 \leq k \leq p - 2$.
Calculate $c_1 = g \times k \bmod p$ and $c_2 = m \times A \times k \bmod p$.
The pair (c_1, c_2) is the cypher text.

Decryption:
Compute $m = c_2 \times c_1^{-a} \bmod p$
The plaintext is m.

Keep in mind that the strength of ElGamal encryption depends on how challenging is $Z_p \times s$’ discrete logarithm issue, which means that given p, g, and A, it is difficult to compute a. Also, the use of a random k for each encryption provides additional security by making it difficult to recover m even if a is known.

Algorithm for the code Generation

(a) Find a group generator and primitive polynomial. Create a repeating outcome by changing the seed of the random number generator.
(b) Then, create the public and private keys. Then the original text is entered and displayed
(c) The message should be converted to binary, then grouped every m bit. ASCII characters are used in the message. Seven bits per character are adequate because there are 128 characters in the ASCII table.
(d) Using the binary data, encrypt the data text.
(e) Decrypt the encrypted text using the supporting function de2char, which is used to convert binary bits of data and then convert to char.
(f) The encrypted
(g) text is displayed.
(h) The decrypted data, which is the original text, is displayed

Comparison with existing methods

Public-key cryptography techniques like ElGamal, RSA, and Paillier are used for digital signatures, encryption, and decryption.

RSA: Ron Rivest, Adi Shamir, and Leonard Adleman, who created the RSA algorithm, are honoured with their names. It also takes into account how challenging factoring big numbers is. RSA is frequently used for digital signatures, encryption, and decryption. The algorithm has the advantage of being relatively fast and easy to implement.

Paillier: The Paillier algorithm is based on the difficulty of the decisional composite residuosity problem. It is a probabilistic algorithm that provides both encryption and homomorphic properties, which means that computations can be performed on cypher texts without decrypting them first. Paillier is often used in secure multiparty computation and privacy-preserving data analysis.

The choice of the algorithm relies on the particular use case and security requirements. All three approaches have merits and limitations. The most popular public-key cryptography algorithm is RSA. However, if the keys are not sufficiently long, it can be attacked. Elgamal and Paillier are less widely used but provide different security properties, such as resistance to quantum attacks and homomorphic encryption.

TABLE 1. Parameters for comparison of algorithms

Metric	Elgamal Algorithm	RSA Algorithm	Pailler Algorithm
Frequency	250 MHz	200 MHz	500MHz- 2GHz
Throughput	7.5 Gbps	5 Gbps	0.128Gbps
Area	12000 gates	20000 gates	10000 gates to 100000
Key Size	256 bits	2048 bits	2048-4096 bits
Power Consumption	200 mW	400 mW	100 mW

Table 1 represents a comparison among three algorithms. Different key values are tabulated to show the outcomes. The throughput of Elgamal Algorithm outperforms RSA and Pailler. It performs better for the lightweight key size and validates our research. While the other two algorithms can be referred for a wide range of key sizes.

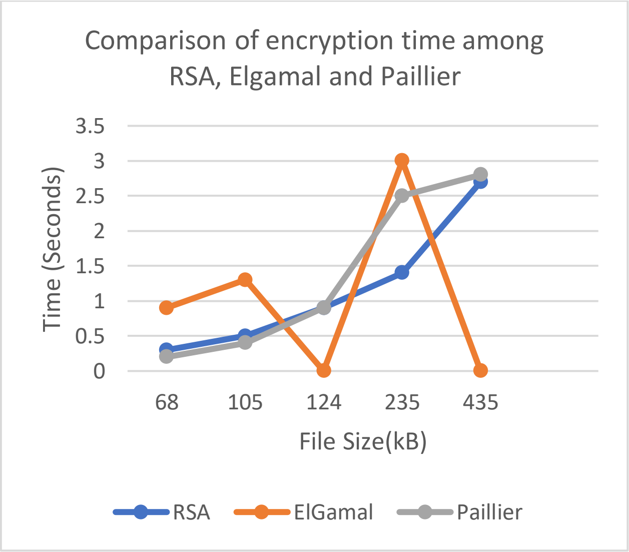


FIGURE 3. Throughput of RSA, ELGamal and Paillier Process

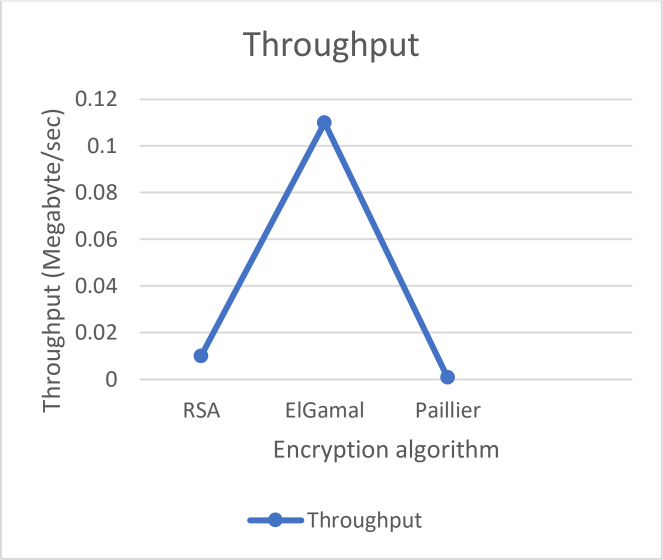


FIGURE 4. Throughput of encryption scheme

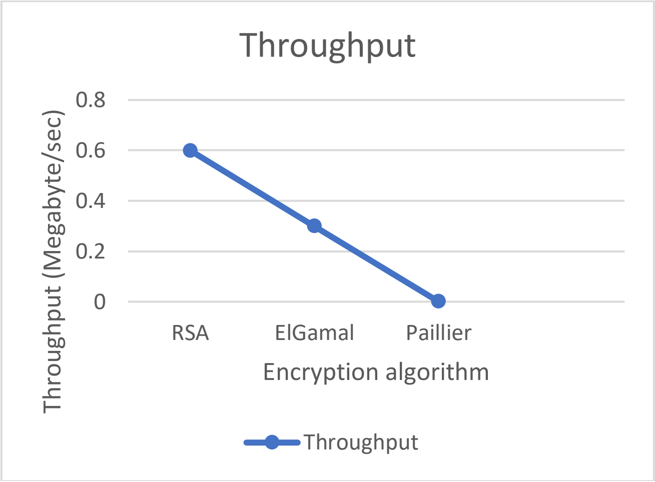
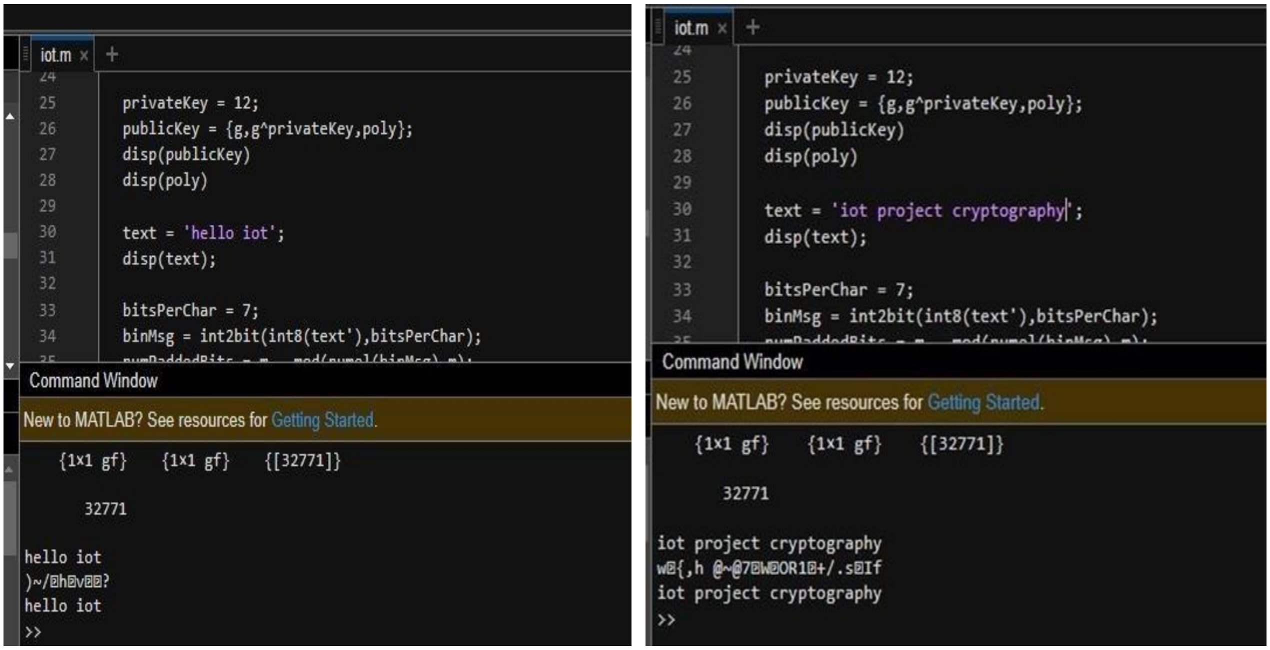


FIGURE 5. Throughput of the decryption scheme

From the results of Fig. 3,4, and 5, the ElGamal method showed better performance over RSA and Paillier in terms of encryption time. Time plays a crucial role cryptography domain. Because info has to be encrypted and decrypted before sending to the receiver, this process has to be fast to make it user friendly. So, our proposed method is more efficient than existing works.

RESULTS AND DISCUSSIONS


iot.m
Command Window
New to MATLAB? See resources for Getting Started.

```
privateKey = 12;
publicKey = {g,g^privateKey,poly};
disp(publicKey)
disp(poly)

text = 'hello iot';
disp(text);

bitsPerChar = 7;
binMsg = int2bit(int8(text'),bitsPerChar);
```

```
    {1x1 gf}    {1x1 gf}    {[32771]}

       32771

hello iot
)~/□h□v□□?
hello iot
>>
```

(a)

iot.m
Command Window
New to MATLAB? See resources for Getting Started.

```
privateKey = 12;
publicKey = {g,g^privateKey,poly};
disp(publicKey)
disp(poly)

text = 'iot project cryptography';
disp(text);

bitsPerChar = 7;
binMsg = int2bit(int8(text'),bitsPerChar);
```

```
    {1x1 gf}    {1x1 gf}    {[32771]}

       32771

iot project cryptography
w□{,h @~@7□W□OR1□+/.s□If
iot project cryptography
>>
```

(b)

FIGURE 6. (a) Encrypted message retrived as Text data 'hello iot' and (b) Text data' iot project cryptography'

The probabilistic nature of ElGamal encryption allows a single plaintext to be encrypted to a huge number of different cypher texts. The size of the cypher text over the plaintext is therefore expanded by a factor of 2:1 as a result of a general ElGamal encryption. Two exponentiations are essential for ElGamal encryption, but they are independent of the message and can be computed in advance if necessary. Despite their ease of integration into a single exponentiation, decryption only needs one exponentiation and one computation of a group inverse. Figure 6 shows the outcome of our method and screenshots of cryptic messages.

CONCLUSION

This paper suggested a more advanced lightweight, energy efficient ElGamal encryption method. For two-party communication, asymmetric key encryption is combined with public-key cryptography to encrypt the message. The difficulty of locating discrete logarithms in the cyclic group serves as the foundation for this cryptography method. The suggested method was examined and tested using text data. It has also been examined and confirmed using modern cartographic methods. The comparison and outcomes demonstrate that the suggested strategy provides the best throughput and area of performance with the least delay. Because of its low weight and great security, the suggested ElGamal cybertext block encryption method can be used in highly secure real-time applications such e-money transmission, authentication schemes, time stamps, Whats App encryption, histogram, etc. In the near future, the suggested approach can be tested, evaluated, and validated for a variety of real-time applications to improve its performance metrics.

REFERENCES

1. Visalakshi Annepu and Rajesh A., “Implementation of an Efficient Artificial Bee Colony Algorithm for Node Localization in Unmanned Aerial Vehicle Assisted Wireless Sensor Networks”, *Wireless Personal Communications,* Springer, vol. 114, no. 3, pp. 2663–2680, May 2020.
2. Visalakshi Annepu and Rajesh A., “An Unmanned Aerial Vehicle Aided Node Localization Using an Efficient Multilayer Perceptron Neural Network in Wireless Sensor Networks”, *Neural Computing and Applications*, Springer, vol. 32, no. 15, pp. 11651–11663, August 2020.
3. V. Annepu, A. Rajesh and K. Bagadi, “Radial basis function-based node localization for unmanned aerial vehicle-assisted 5G wireless sensor networks”, *Neural Computing and Applications*, 33, 12333-12346, 2021.
4. V. Annepu *et al.*, "Review on Unmanned Aerial Vehicle Assisted Sensor Node Localization in Wireless Networks: Soft Computing Approaches," *IEEE Access*, vol. 10, pp. 132875-132894, 2022
5. N. K. Vaegae, K. K. Pulluri, K. Bagadi and O. O. Oyerinde, "Design of an Efficient Distracted Driver Detection System: Deep Learning Approaches," *IEEE Access*, vol. 10, pp. 116087-116097, November 2022.
6. K. Bagadi, C. V. Ravikumar, M. Alibakhshikenari, Ch. Nagaraj, A. Rajesh, S. Aïssa, I. Dayoub, F. Falcone and E. Limiti, “Precoded Large Scale Multi-User-MIMO System Using Likelihood Ascent Search for Signal Detection”, *Radio Science*, vol. 57, no. 12, December 2022.
7. Goyal, Tarun Kumar, Vineet Sahula, and Deepak Kumawat. "Energy efficient lightweight cryptography algorithms for IoT devices." *IETE Journal of Research* 68, no. 3 (2022): 1722-1735.
8. Thakor, Vishal A., Mohammad Abdur Razzaque, and Muhammad RA Khandaker. "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities." *IEEE Access* 9 (2021): 28177-28193.
9. Dutta, Indira Kalyan, Bhaskar Ghosh, and Magdy Bayoumi. "Lightweight cryptography for internet of insecure things: A survey." In *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 0475-0481. IEEE, 2019.
10. Okello, Wanican Julian, Qingling Liu, Faizan Ali Siddiqui, and Chaozhu Zhang. "A survey of the current state of lightweight cryptography for the Internet of things." In *2017 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 292-296. IEEE, 2017.
11. Rao, Vidya, and K. V. Prema. "A review on lightweight cryptography for Internet-of-Things based applications." *Journal of Ambient Intelligence and Humanized Computing* 12 (2021): 8835-8857.
12. Hong, Deukjo, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee et al. "HIGHT: A new block cipher suitable for low-resource device." In *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8*, pp. 46-59. Springer Berlin Heidelberg, 2006.
13. Gunathilake, Nilupulee A., William J. Buchanan, and Rameez Asif. "Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications." In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 707-710. IEEE, 2019.
14. Buchanan, William J., Shancang Li, and Rameez Asif. "Lightweight cryptography methods." *Journal of Cyber Security Technology* 1, no. 3-4 (2017): 187-201.
15. Beaulieu, Ray, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. "The SIMON and SPECK families of lightweight block ciphers." *cryptology eprint archive* (2013).
16. Borghoff, Julia, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezevic, Lars R. Knudsen, Gregor Leander et al. "PRINCE–a low-latency block cipher for pervasive computing applications." In *Advances in Cryptology–ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings 18*, pp. 208-225. Springer Berlin Heidelberg, 2012.

17. Usman, M. H., and M. M. Hussaini. "Analysis of students' error in learning of trigonometry among senior secondary school students in Zaria Metropolis, Nigeria." *IOSR Journal of Mathematics* 13, no. 2 (2017): 1-4.
18. Ilori, Alade E., Bulus A. Sawa, and Abdullahi A. Gobir. "Application of cause-and-effect-analysis for evaluating causes of fire disasters in public and private secondary schools in Ilorin Metropolis, Nigeria." *Archives of Current Research International* 19, no. 2 (2019): 1-11.
19. Hong, Deukjo, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee et al. "HIGHT: A new block cipher suitable for low-resource device." In *Cryptographic Hardware and Embedded Systems-CHES 2006: 8th International Workshop, Yokohama, Japan, October 10-13, 2006. Proceedings 8*, pp. 46-59. Springer Berlin Heidelberg, 2006.
20. Mohd, Bassam Jamil, Thaier Hayajneh, Zaid Abu Khalaf, and Khalil Mustafa Ahmad Yousef. "Modeling and optimization of the lightweight HIGHT block cipher design with FPGA implementation." *Security and Communication Networks* 9, no. 13 (2016): 2200-2216.
21. Al-Husainy, Mohammed Abbas Fadhil, Bassam Al-Shargabi, and Shadi Aljawarneh. "Lightweight cryptography system for IoT devices using DNA." *Computers and Electrical Engineering* 95 (2021): 107418.
22. Biswas, A., A. Majumdar, S. Nath, A. Dutta, and K. L. Baishnab. "LRBC: a lightweight block cipher design for resource constrained IoT devices." *Journal of Ambient Intelligence and Humanized Computing* (2020): 1-15.
23. Thakor, Vishal A., Mohammad Abdur Razzaque, and Muhammad RA Khandaker. "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities." *IEEE Access* 9 (2021): 28177-28193.
24. Khashan, Osama A., Rami Ahmad, and Nour M. Khafajah. "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks." *Ad Hoc Networks* 115 (2021): 102448.
25. Bhardwaj, Isha, Ajay Kumar, and Manu Bansal. "A review on lightweight cryptography algorithms for data security and authentication in IoTs." In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)*, pp. 504-509. IEEE, 2017.
26. Hasan, Mohammad Kamrul, Shayla Islam, Rossilawati Sulaiman, Sheroz Khan, Aisha-Hassan Abdalla Hashim, Shabana Habib, Mohammad Islam et al. "Lightweight encryption technique to enhance medical image security on internet of medical things applications." *IEEE Access* 9 (2021): 47731-47742.
27. Sallam, Suzan, and Babak D. Beheshti. "A survey on lightweight cryptographic algorithms." In *TENCON 2018-2018 IEEE Region 10 Conference*, pp. 1784-1789. IEEE, 2018.
28. Rana, Muhammad, Quazi Mamun, and Rafiqul Islam. "Current lightweight cryptography protocols in smart city IoT networks: a survey." *arXiv preprint arXiv:2010.00852* (2020).
29. Shah, Ankit, and Margi Engineer. "A survey of lightweight cryptographic algorithms for iot-based applications." In *Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS-2018*, pp. 283-293. Springer Singapore, 2019.
30. Katagi, Masanobu, and Shiho Moriai. "Lightweight cryptography for the internet of things." *sony corporation* 2008 (2008): 7-10.
31. Madushan, Hasindu, Iftekhar Salam, and Janaka Alawatugoda. "A Review of the NIST Lightweight Cryptography Finalists and Their Fault Analyses." *Electronics* 11, no. 24 (2022): 4199.
32. Dhanda, Sumit Singh, Brahmjit Singh, and Poonam Jindal. "Lightweight cryptography: a solution to secure IoT." *Wireless Personal Communications* 112 (2020): 1947-1980.