JNNCE Journal of Engineering & Management, Volume 6, No.1, Jan – June 2022 ISSN 2582-0079
This paper is presented at National Workshop on Cryptology NWC 2021, held at JNN College of Engineering, Shimoga during 18-20 Nov 2021

Available online @ https://jjem.jnnce.ac.in
https:www.doi.org/10.37314/JJEM.2022.060113
Indexed in International Scientific Indexing (ISI)
Impact factor: 1.395 for 2021-22
Published on: 31July 2022

LightWeight Public Key Cryptography Based on Cyclic Group of 6^x Mod 11 and its Application to Image Encryption

Deeksha[1*], Manisha Shalini Mascarenhas[2], Raghavendra A[3]

[1*,2,3] Poornaprajna College, Udupi, Karnataka,

deekshamaj@gmail.com, manishashalini200026@gmail.com, ragavendra.bhat.a@gmail.com

Abstract

One of the popular fields for research work is the Internet of Things(IoT). The security of this is one of the most challenging one. Almost all IoT devices are having very few memories and processing powers. Powers for these are to be consumed in an efficient way. The existing security algorithm needs more processing powers and memories, Hence Lightweight cryptography is one of the emerging areas in Iot's.

In this paper it is suggested a novel method of using lightweight public key cryptography by using an equation 6^x *mod 11. This is used in this work for the encryption of an image standard image Lena. This image is step down to mod 11 and encrypted for the convenient purpose. The performance of the encryption is measured by evaluating the values of standard deviation, entropy, histogram and visual process*

Keywords: *Group, Cyclic Group, Generator*

1. Introduction

The Internet of Things (IoT) has enormous potential to change the world. Security of IoT is also a challenging one. This challenge is met in many ways. These are mentioned as follows. Symmetric-key cryptosystems and public key cryptosystem provides more security, but it is having high computational complexity. Therefore IoT security is major challenge for public key cryptosystems as well as complex security.[3]

Commonly used cryptography algorithms such as AES, RSA are one-to-one communication encryption techniques so it requires lots of steps to share data with many users and it creates problems when sharing data. By using the idea of item sensors,constant handling and intellectual capacities, the Internet of Things(IoT) networks are developed.
In lightweight cryptography AES is more convenient than RSA. Since AES uses asymmetric key cryptography it uses a small size of keys and it has only one for encryption as well as description process. Public key cryptography allows authentication without pre-sharing the secrets and solves key management issues [1, 2].

Internet of Things (IoT) technology is a platform for research work. IoT's devices and sensors are accessed and send the information to users by using the single internet network [4].

RAM and ROM are used to store and run the application. The size of the memory is very small which occupies limited resources. IoT devices deal with the real-time application which gives quick and accurate response. Essential security, energy security and data security are challenging tasks for designers [5].

Block chain requires extensive resources and high computational capabilities for communication processes. It evaluates and tests the lightweight hash functions such as spongent photon and quark on FPGA platforms to check which is more suitable for block chain IoT devices. SPONGENT hash function performs best on security and throughput. QUARK hash function performs as a least power and energy but it has a lowest security. PHOTON acts as less area, energy and security [6].

E^3LCM method is proposed for the operation of the encryption and decryption process and to evaluate several performance of latency, memory required etc. This method has less power consumption and less memory occupation. For electronic money transfer, authentication scheme, time stamping, encryption in WhatsApp etc. we are using E^3LCM cyber text method. It can be integrated in real time high security applications [4].

Elliptic Curve are used in various key exchange technique which includes the Diffie-Hellman key scheme. When we are giving the security to gadgets, Elliptic Curve Diffie-Hellman[EC-DH] algorithm is received the significance of its features such as low power and it is reasonable for the IoT gadgets. Text messages are not included in this algorithm so we exploit this by using the key exchange techniques. Elliptic Curve Diffie Hellman[EC-DH] is an attractive and effective public-key cryptosystem. We utilize this cryptography for key generation [7].

Liang C et al [8], introduced the hybrid encryption algorithm is a developed method on RSA algorithm and it is combined with AES. Hybrid encryption algorithm proposed to improve the efficiency of generating large primes. But this algorithm is mainly used for enhancing the data. M-SSE proposed by Chongzhi Gao al. is different from symmetric encryption algorithm. It provides privacy in forward as well as backward direction using techniques of multi-cloud computing [8].

Dahshan proposed a distributed key management protocol which is based upon the Elliptic Curve Cryptography (ECC). During initialization phase the authority generates public key and private key which is provided to all IoT entities. These two keys are private key for each entity. After the network deployment each entity executes the key generation protocol and produces its session key pair [9].

To make IoT solutions safer, we have to consider security requirements. Lightweight cryptography's are requested to use for devices which possess less memory and poor capabilities [10].

There is limitation for homomorphic encryption Since it takes long run time over complex algorithm. Hence, we used partially homomorphic algorithm [11].

Objects are connected to the network. The network location of these objects is an major issue. Currently we are using the locating method which is based on IPV4/IPV6. Named Data Networking(NDN) is proposed as a naming infrastructure of Future Internet Architecture(FIA). NDN is method which is based on the object names [12].

We are using several kinds of sensors for sensing different kinds of data. For example camera sensors, smoke detection sensors etc. To sense the physical environment we are using mechanical, electronic or chemical sensors. IoT application like RFID,GPS are depends on the sensing layer technology [13].
The safety review and symmetric testing of the system using the AVISPA method as showed the protection quality of the systems [14].

It is necessary to improve security to ensure privacy, confidential matters and end-to-end security. We needed to invest new technologies in order to overcome open research challenges in IoT [15].
All these methods are based on the existing methods and its extensions. However the time

and the power consumptions in these types are always high.

2. Mathematical Preliminaries

In this chapter the paper deals with two main parts

1. Basic algebraic structure based on **groups**
2. Cyclic group based on 6^x mod 11

Algebraic structure based on groups [1]:

Let algebraic structure (Ɠ,×) is the non-empty set [2], with respect to × be considered as groups, if it obeys the following conditions.

Closure: Let ȿ, ɏ ∈ Ɠ, such that (ȿ × ɏ) ∈ Ɠ. Where × be the binary operator

Associativity: The binary operator × on set Ɠ is associative if,

(ȿ × ɏ) × ʐ = ȿ × (ɏ × ʐ)∀ȿ, ɏ, ʐ ∈ Ɠ.

Let Ş be a set containing at least a single element, and × is an operation that satisfies associative property in Ş; then, an ordered pair (Ş, ×) is referred to as a semi group.

Example: $(N,\times), (Z,\times), (Q,\times), (R,\times), (C,\times)$ are semi groups under ×. Since all these mentioned sets are nonempty sets and binary operation × is associative.

A semigroup (Ɱ,×) is said to be a monoid if an element ε exist in Ɱ, such that ȿ × ε = ε × ȿ = ȿ , where ∀ ȿ ∈ Ɱ,.

Identity: We know that if (Ɱ, ×) is a monoid and an element ε in Ɱ, satisfying the condition ȿ × ε = ε × ȿ = ȿ for each ȿ ∈ Ɱ, is unique. This unique element ε of the monoid is termed as the identity element of (Ɱ,×).

A monoid (Ɠ,×) with identity element ε is said to be a group, for every ą there exists a unique ḅ in Ɠ such that,

$$ą \times ḅ = ḅ \times ą = ε \qquad (1)$$

Example:$(N,\times), (Z,\times), (Q,\times), (R,\times), (C,\times)$ are all monoid under × (multiplication), with 1 as the identity element.

Inverse: In a group (Ɠ,×) ε be an identity element, then ∀ą ∈ Ɠ there is uniqueḅ ∈ Ɠ, satisfying the above condition (1). This unique element ḅ ∈ Ɠ is called inverse of ą which is represented through $ą^{-1}$.

Commutative: In group (Ɠ,×), if the × binary operation satisfies commutative property. i.e. ą × ḅ = ḅ × ą ∀ ą, ḅ ∈ Ɠ, the group Ɠ is considered as an Abelian.

Example: Under binary operation × ,
$(Q^*,\times), (R^*,\times), (C^*,\times)$ are said to be abelian groups

The order of the group is the number of elements contained in (Ɠ,×).

Finite group:

A finite group Ɠ contains exactly ŋ distinct elements, then Ɠ becomes finite group of order ŋ represented as Oɍɗ(Ɠ) = ŋ. In finite group, when one operates on two elements ą × ḅ, where ą, ḅ ∈ Ɠ, and if the resultant goes beyond the limit ŋ, then these numbers wrap around within the limit mentioned. To limit this within the given order, modular arithmetic plays an important role, which is explained next.

Modular Arithmetic:

Let ą, ḅ are integers and ɱ ∈ Z^+. If ɱ divides ą − ḅ, then this can be mathematically written as,

$$ą \equiv ḅ \; mod \; ɱ. \qquad (2)$$

Where, ɱ be the modulus and ḅ be the reminder.

Let $x, y \in Z$ and $x \times y$ also $\in Z$ can be demonstrated using the following examples.

Example: $3 \times 2 \equiv 6 \; mod \; 9$=6 and 6∈ Z
$4 \times 3 \equiv 12 \; mod \; 9$=3 and 3∈ Z

Let Oɍɗ(Ɠ) $< A$ be the results of an operation of two elements of Z. The result A can be written in terms of elements of Z , which are reminder (ȹ), divisor (ɱ) and quotient (q) as

$$A = q \times ɱ + ȹ, \quad (3)$$

Example:

Let $A = 43$ and $Orđ(Ǵ)$ or $ɱ = 9$, using equation (3) write it as $43 \equiv 4 \times 9 + 7$ and therefore we can write 43 as $43 \equiv 7 \; mod \; 9$.

Generator:

If an element ą produces all the elements of set Ǵ under×, then ą is called the generator of set Ǵ. Let (Ǵ,×) is a group, and r be a positive integer. An element $ą \in Ǵ$ generates all other elements of set Ǵ can be written as,

$$Ǵ = < ą > = \{ą^r | r \in Z\} \quad (4)$$

Order of the elements:

Let ƙ is smallest positive integer, if it results as $ą^{ƙ} = 1$, identity element, this ƙ is called the order of the element.

$$ą^{ƙ} = ą \times ą \times ą \ldots\ldots \times \underbrace{ą}_{ƙ \; times} = 1 \quad (5)$$

In equation (5) ą is an element.

Example:

Consider the set $H = \{2,4,8\} \subset Z_7^*$ under multiplication, where ą =2.

$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8 \equiv 1 \; mod \; 7.$$

Therefore, the number of elements (order of the element) in H is 3.

Cyclic Groups: If $Ǵ = < ą >$ for $ą \in Ǵ$, then Ǵ is considered cyclic. For example elements of $Z_5^* = \{1,2,3,4\}$ is considered as cyclic, with the generators 2 and 3 under multiplication.

Cyclic group based on 6^x mod 11:

Next the paper defines a cyclic group based on 6x mod 11. A group < 6x, mod 11> can be defined as a cyclic group 6^x (mod 11) , where x belongs to positive integers. Then A={1,2,3,4,5,6,7,8,9,10}
Above set contains 1 to 10 numbers if we take power more than 10, then we get the same set i.e A.

Example,
6^{11}(mod 11) = 6^1(mod 11) ,6^{12}(mod 11) = 6^2(mod 11) and so on.

- *Closure Law:*

Let 6^a(mod 11), 6^b(mod 11)∊A that is (6^a(mod 11))(6^b(mod 11))∊A ∀a,b∊A

Example
6^2(mod 11), 6^3(mod 11)∊A that is (6^2(mod 11)(6^3(mod 11))
=3.7=21≡6^5(mod 11) ∈6^x(mod 11)

- *Associative Law:*

Let 6^a(mod 11), 6^b(mod 11), 6^c(mod 11) ∊A that is 6^a(mod 11)[(6^b(mod 11)) (6^c(mod 11))]= [(6^a(mod 11))(6^b(mod 11))] 6^c(mod 11) ∀a,b,c∊A

Example:
6^2(mod 11), 6^3(mod 11), 6^3(mod 11) ∈A that is 6^2(mod 11)[(6^3(mod 11)) (6^4(mod 11))]= [(6^2(mod 11))(6^3(mod 11))] 6^4(mod 11) 3*(7*9)=(3*7)*9

- *Identity Law:*

Let 6a (mod 11)∊A then there is an element e∊A such that (6^a(mod 11)) (6^e(mod 11)) = 6^a(mod 11) ∀a∊A
Example:
(6^2(mod 11)(6^{10}(mod 11))=6^2(mod 11) that is 6^{10}(mod 11) is identity.

- *Inverse Law*:

If 6^a(mod 11) ∈A then there exist $6^{a'}$(mod 11) ∈A such that (6^a(mod 11))($6^{a'}$(mod 11)) = 6^e(mod 11) ∀a∊A
Example:
(6^2(mod 11)(6^8(mod 11))=6^{10}(mod 11)
∴ 6^8(mod 11) is inverse.

3. Methodology

This work is based on the cyclic group using 6^x mod 11. Hence the maximum integer value taken for the process will be eleven.

Work considers an image which is a grey scale; in this case it is taken as a standard Lena image. Each pixel of this is represented in the range zero to 255. Since there is a limitation of maximum integer as eleven, Now we have to convert the standard image into an equivalent level of eleven division of 0 to 255. That is table 1 shows the rearranged pixel levels of the image

Table 1 : Rearrangements of the pixel level for the construction of images in different resolutions for adapting the cryptographic technique from 0 to 255 to 0 to 10.

Pixel levels of 0 to 255 of original image	0-23	24-46	47-70	71- 93	94-117	118-140	141-163	164-186	187-210	211-232	233-255
Pixel level converted image	0	1	2	3	4	5	6	7	8	9	10

After converting the image into a scale of 11. This will be encrypted by using an algorithm based on (1.1).

$$cypher\ Text = 6^{(plaintext \times key)mod\ 11} mod\ 11 \qquad (1.1)$$

Similarly for decryption algorithm is also explained as equation (2.2)

$$plain\ text = 6^{(ciphertext \times key)mod11} mod\ 11 \qquad (2.2)$$

During encryption the product of plain text and key is the exponent for six. And during decryption the exponent is the product of cipher text and key and it should be such that the resultant will be the original plain text. Indicates the product of key and cipher text should results in the inverse of the product of plain text and key.

In this case the group A contains {1,2,3,4,5,6,7,8,9,10} inverse of this is A^{-1}={1,6,4,3,9,2,8,7,5,10}

Result and analysis: The experiment is conducted based on the above procedure. An image Lena as shown in figure 1 is taken as a reference

Figure 1: A monochrome standard image

Figure 2: reconverted image of the figure1 based of the scale 11

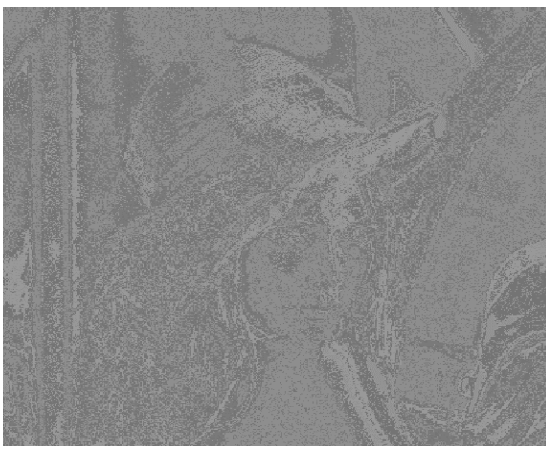

Figure 3: Encrypted image

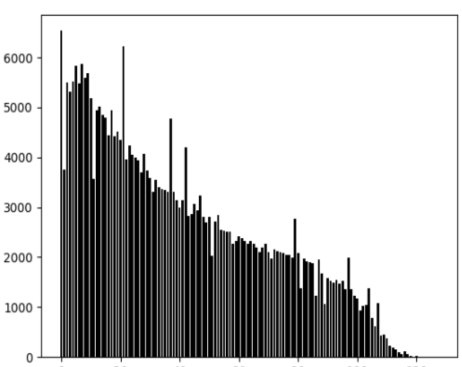

Figure 4: Histogram of the original image

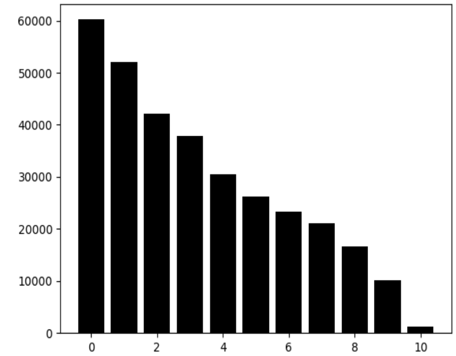

Figure 5: Histogram of the converted image

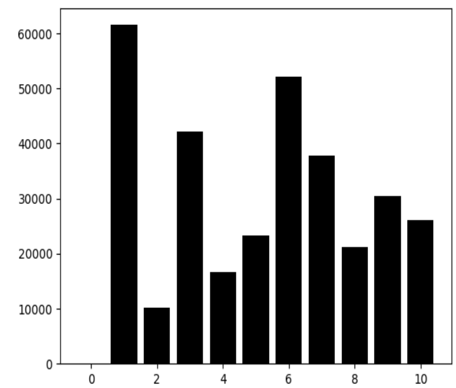

Figure 6: Histogram of the encrypted

Figure 2 is the converted image and will be a blurred image since it is scaled down from 0 to 255 to 0 to 10. This scaled image is encrypted based on the equation (1) that is shown in figure 3. In this figure it is a bit difficult to identify the image traces. Next for these figures the paper applies a histogram approach to measure the strength of the cryptography. Histograms of the figure 1,2,3 are shown in the figures 4,5 and 6 respectively. The figure 6 shows the quality of encryption, indicating a flatter histogram.

Following are some of the measures of cryptography they are

1. Entropy. 2. Standard deviation. 3.coraletion

The readings of these are given in the table 2.

Table 2: Measures of cryptography

Standard deviation	Entropy	Correlation
2.723652	2.141902	0.797702

4. Conclusion

Even though the traces are noted in the encrypted image the encryption is comparatively good for the modular operation taken. This can be extended for the value 257 to get good results of encryption and the results of table 2. Further extension can be possible based on the modular number which is taken as 11 in this work.

References

1. Véronique Cortier, Stéphanie Delaune, Pascal Lafourcade, A Survey of Algebraic Properties Used in Cryptographic Protocols. Journal of Computer Security, IOS Press, Vol. 14, No. 1, 2006,pp.1-43.

2. Džamonja, Mirna. Set Theory and its Place in the Foundations of Mathematics: A New Look at an Old Question. Journal of Indian Council of Philosophical Research. Vol. 34, No. 2, 2017, pp.415–424.

3. A. M. Qadir and N. Varol, A Review Paper on Cryptography, 7th International Symposium on Digital Forensics and Security (ISDFS), 2019, pp. 1-6.

4. Norhidayah Muhammad, Jasni Mohamad Zain, Conceptual Framework for Lightweight Ciphertext Policy-attribute based Encryption Scheme for Internet of Thing Devices, Malaysian Journal of Computing, Vol.4, Issue 1, pp.237-245.

5. Vidyotma Thakur,Gaurav Indra, Nitin Gupta, Pushpita Chatterjee, Omar Said, Amr Tolba, Cryptographically secure privacy-preserving authenticated key agreement protocol for an IoT network: A step towards critical infrastructure protection, Peer-to-Peer Networking and Applications, Vol.15, 2022, pp.206-220.

6. Shuang sun ,Rong du, Shudong chen, and Weiweili, Blockchain-Based IoT Access Control System: Towards Security, Light-weight, and Cross-Domain, IEEE Access, Vol. 9, 2021, pp.1-10.

7. Sa'ed Abed , Reem Jaffal, Bassam J. Mohd, Mohammad Al-Shayeji, An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices., Cluster computing,The author (s),under exclusive licence to springer Science+Business Media, LLC,part of springer Nature 2021,31 May 2021,pp.4-16.

8. Vishal a. Thakor, Mohammad Abdur Razzaque, (Member, IEEE),and Muhammad R. A. Khandaker , (Senior Member, IEEE), Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Oppurtunities, Vol. 9, 2021,pp.3-9.

9. Prakasam P.a, Madheswaran M.b, Sujith K.P.c, Md Shohel Sayeedd,An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices, ICT Express (2021),14 March 2021, pp.28177-28180.

10. Tarun Kumar Goyal, Vineet Sahula, Light-weight Security Algorithm for Low Power IoT Devices, Proceedings of the Internatinal Conference on Advances in Computing, Communications and Informatics (ICACCI), Sept.21-24, 2016, Jaipur ,India, pp.1725-1729.

11. Sreeja Rajesh , Varghese Paul , Varun G. Menon, and Mohammad R. Khosravi, A Secure and Efficient Lightweight Symmetric Encryption Scheme for Transfer of Text Files between Embedded IoT Devices., Symmetry, Vol.11, No. 2, 2019, pp.1-21. https://doi.org/10.3390/sym11020293

12. Samia Belattaf, Mohamed Mohammedi,

Mawloud Omar ,Rachida Aoudjit, Reliable and Adaptive Distributed Public-Key Management Infrastructure for the Internet of Things, Wireless Personal Communications, Vol.120, 2021, pp. 113–137.

13. Vidya Rao , K. V. Prema, A review on lightweight cryptography for Internet-of-Things based applications., Journal of Ambient Intelligence and Humanized Computing, Vol. 12, 2021, pp. 8835–8857.

14. P. Devi, S. Sathyalakshmi,D. Venkata Subramanian, An optimal metaheuristic optimization based ElGamal public key cryptosystem for privacy in an IoT environment, International Journal of System Assurance Engineering and Management, 2021,pp.1-11.

15. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh," IoT Security: Ongoing Challenges and Research Opportunities, Proceedings of the IEEE 7th International Conference on Service-Oriented Computing and Applications, 17-19 November 2014, Matsue, Japan.

16. Vikas Hassija, Vinay Chamola , Vikas Saxen, Divyansh Jain,Pranav Goyal, and Biplab Sikdar, (Senior Member, IEEE), A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures., IEEE Access, Vol. 7, 2019, pp.1-18.
DOI: 10.1109/ACCESS.2019.2924045

17. Vidyotma Thakur, Gaurav Indra, Nitin Gupta, Pushpita Chatterjee, Omar Said,Amr Tolba, Cryptographically secure privacy-preserving authenticated key agreement protocol for an IoT network: A step towards critical infrastructure protection., Peer-to-Peer Networking and Applications, Vol. 15, Issue 3, 2022, pp. 206–220.

18. Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, Internet of Things (IoT) Security:Current Status, Challenges and Prospective Measures, Proceedings of the 10th International Conference for Internet Technology and Secured Transactions (ICITST), 14-16 December 2015, London, UK