Academic Science Journal

Hybrid Cryptosystem Using Polybius and Elgamal Algorithm Over the Gaussian Integers

Hiba A. Khalaf, Rifaat Z. Khalaf

Department of Mathematics, College of Science, University of Diyala

hibbaahmaed@gmail.com

Received: 2 November 2022 **Accepted: 22 February 2023**

DOI: https://doi.org/10.24237/ASJ.02.01.707B

Abstract

In composition theory, computer security, and engineering are all closely related fields under which cryptography, a technology that deals with data security, falls. However, the complexity of cryptographic systems must be increased due to the attackers' use of powerful computers. El Gamal encryption and the Polybius square were bypassed in this study's attempt to increase data security. As this hybridization was done in a Gaussian environment. The ciphertext produced by the Polybius box aims to strengthen the hybrid cipher. The simulation results show that the proposed technique creates a unique ciphertext that is immune from brute force or repeated attacks since it does not resemble any pattern of plaintext.

Keywords: Polybius, Elgamal Algorithm, Gaussian integer.

نظام تشفير هجين يستخدام بولييوس وخوارزمية الجمال على الأعداد الصحيحة الغاوسية

هبه احمد خلف و رفعت زيدان خلف

قسم الرياضيات –كلية العلوم – جامعة ديالى

الخلاصة

في نظرية التكوين وأمن الكمبيوتر والهندسة بمجالاتها المختلفة ,مرتبطة ارتباطا وثيقا يندرج تحتها التشفير ,التشفير هوتقتينة تتعامل مع امن البيانات .ومع ذلك ,يجب زيادة تعقيد أنظمة التشفير بسبب استخدام المهاجمين أجهزة حاسوب متطورة وقوية . حيث قمنا في هذا البحث بدراسة تشفير هجين (خوارزمية الجمال مع مربع بولييوس) محاولة منا في هذه

Academic Science Journal

الدراسة للحصول على نظام تشفير اكثر امنية للحفاظ على سرية المعلومات ,حيث انه تم التهجين في بيئة غاوسية . يهدف نص التشفير الذي ينتجه مربع بوليبيوس الى زيادة امن التشفير الهجين . حيث أظهرت نتائج المحاكاة ان التقنية المقترحة تخلق نصا مشفرا مميزا محصنا من هجمات القوة الغاشمة او الهجمات المتكررة نظرا لانها لا تشبه أي نمط من النص العادي.

الكلمات المفتاحية : خوارزمية الجمال ,مربع بوليبيوس , اعداد غاوسين .

Introduction

Due to the tremendous growth in communication technology today, security becomes one of the top priorities, where in data security is still a challenge. For most organizations, crucial data is very important and must not be changed or used for illegal purposes. In defense, data security is prioritized. The unauthorized broadcast of data in the defense system is extremely disastrous and can cause damage. Likewise, data in banking systems must be adequately secured where authentic data, under no circumstances, should go to perpetrators [1]. Data can be secured by being transformed into an unreadable form and then returned to its original format after it has reached the intended recipient. The method of securing data is the fact that a file may only be accessed by authorized individual cryptography. Cryptography is a method and branch of research that uses mathematical ciphers to conceal information [2]. A cipher is a set of algorithms that converts plaintext into ciphertext. The encryption procedure is an unintelligible format with reverse decryption, which turns ciphertext back into plaintext back into plain text [3] in its original form. Symmetric and asymmetric key cryptography are the two main categories of cryptography. The same key, which is used for both encryption and decryption, is shared by the sender and receiver in symmetric-key cryptography. In contrast to symmetric key cryptography, which assigns a pair of keys to each user, asymmetric key cryptography introduces the idea of handling public and private keys. Two keys are used: one for encryption and the other for decryption [4].

A public-key approach called the Elgamal algorithm is based on the challenging calculation of discrete logarithms in a finite field; for more information, see [4] and [5]. Because each plaintext letter is encoded in two interdependent ciphertexts, the beauty algorithm is vulnerable

to various ciphertext attacks. In other words, if you know the ciphertext, you will also know the plaintext [6] without the key information.

To increase the security of the Elgamal algorithm, several investigations have been done. For instance, to make the ciphertext larger during the encryption process, the numerical form of the letter M is represented in terms of I primes, as shown in [6]. Additionally, the beauty algorithm uses the square matrix as a private key to increasing the method's security against brute force attacks (see [7]).

In number theory, Gaussian integers of the form x + yi, where x and y are integers of the type [8] & [9]. The use of Gaussian integers in cryptography can enhance the speed and security of the algorithms used in these systems. When the length of integral floating point types is defined, Gaussian integers, for instance, can be utilized to increase the security of an elliptic curve encryption system [10]. Based on the difficulties of interpreting huge complex numbers, Gaussian integers are also utilized to enhance the Fiat and Shamir diagram approach [11].

Polybius Algorithm

Polybius cipher is also known as Polybius square, which is an alternate cipher using a square grid. Each letter in the regular letter is replaced by an equal number according to Table 1.

A substitution cipher called the Polybius cipher was created by the ancient Greek historian Polybius. [12-15] To represent the character set with a lesser number of symbols, the Polybius cipher fractionates it. The alphabet's letters are organized in a 5x5 Polybius square, and each letter is identifiable by its grid location, or more simply by its row and column positions or coordinates. Simple substitution of appropriate pairs of integers for plain text letters results in encryption. The square is used to symbolize the English alphabet, and the positions of the letters I and J coincide, making it simple to discern when the text is decoded. The Polybius cipher can also be keyed, in which case the key letters are entered into the square first without repeating themselves, and the other letters are inserted in turn. . By using a long key, a square, and a sum with the plain text message that has been encrypted, the Polybius cipher may be used as a polyalphabetic substitution cipher. See [16]

Table 1: The Table Show Character in Polybius

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Exampal:Hiba=23 24 12 11

ElGamal Algorithm

Elgamal encryption technology, one of the public key cryptosystems, is widely used since it depends on the difficult computation of discrete logarithms in finite fields (see [4] & [5]). The algorithm is carried out between two parties—the sender, Alice, and the receiver, Bob by following these steps :

1.Generating the Keys

A. Bob chooses a large prime number p.

B. Bob chooses random numbers c and g, such that, $c, g < p$.

C. calculates

$d \equiv g^c \ (mod\ p)$

Then, the private key is c and the public key is d, g, and p.

2. The Encryption Process

To transmit Bob the message (sent)=S, Alice encrypts the message. Then,

A. Alice chooses a positive integer t randomly, such that, $1 < t < p - 1$.

B. Alice calculates the formulas below.

$$E \equiv g^t \ (mod\ p) \text{.....(1)}$$

$$F \equiv d^t * S \ (mod\ p) \text{ ....(2)}$$

The ciphertext s then sent to Bob as the pair (E , F).

3.The Decryption Process

After obtaining the ciphertext (E, F), Bob completes this procedure by computing the formula shown below.

Either:

$$S \equiv \frac{F}{(E)^C} \ (mod\ p) \ldots\ldots\ldots\ldots\ldots (3)$$

OR:

$$S \equiv F * z(\ mod\ p)$$

$$z \equiv d^{p-1-C}(mod\ p)$$

$$d = g^t(mod\ p\ )$$

4. The Gaussian Integers

A fascinating area of number theory is the study of the Gaussian integers. Theorems and definitions for the Gaussian integers are provided in this section; for further information, see [8] and [9].

Definition 4.1: (The Gaussian Integers)

The Gaussian integers are given as

$$Z[i] = \{x + yi : x, y \in \mathbb{Z}, i = \sqrt{-1}\}$$

Definition 4.2: (The Conjugate)

Let $\alpha = x + yi$ be a Gaussian integer, then the conjugate of α is

$$\bar{\alpha} = x - yi.$$

Note 4.1: Under the common addition and multiplication, Z[i] is a commutative ring of the complex number field.

Definition 4.3 (The Norm) The norm of $\alpha = x + yi$ if we assume that x+yi is a Gaussian integer is given as

$$N(\alpha) = \alpha\bar{\alpha} = (x + yi)(x - yi) = x^2 + y^2.$$

Table 2: The table shows the letters and their corresponding values of Gaussian integers.

THE LETTER	THE POLYBIUS	THE CORRESPONDING GAUSSIAN INTEGERS	THE LETTER	THE POLYBIUS	THE CORRESPONDING GAUSSIAN INTEGERS
A	11	11	N	33	14
B	12	12	O	34	15
C	13	$3 + 2i$	P	35	$4i$
D	14	14	Q	41	$4 + 5i$
E	15	15	R	42	42
F	21	21	S	43	43
G	22	22	T	44	44
H	23	23	U	45	$3 + 6i$
I	24	24	V	51	51
J	24	$3 + 4i, 5i$	W	52	$6 + 4i$
K	25	31	X	53	$2 + 7i$
L	31	$4 + 4i$	Y	54	54
M	32	32	Z	55	55

And we got this table 2 through an application from the norm definition 4.3

Proposition 4.1:

1. If $\alpha, \beta \in Z[i]$, then $N(\alpha\beta) = N(\alpha)N(B)$
2. If $\gamma \in \mathbb{Q}$, then $N(\gamma) = \gamma^2$.

Theorem 4.1: (Division Theorem): Let α,β∈Z[i], where β≠0, then there are q,r ∈Z[i], such that, α= bq + r and N(r)<N(β).

Theorem 4.2: (Euclidian Algorithm): Let $\alpha, \beta \in Z[i]$ be two Gaussian integers, then by the division theorem, we have

$$\alpha = \beta\gamma_1 + \rho_1, \quad N(\rho_1) < N(\beta)$$

$$\beta = \rho_1\gamma_2 + \rho_2,\ N(\rho_2) < N(\rho_1)$$

$$\rho_1 = \rho_2\gamma_3 + \rho_3, \qquad N(\rho_3) < N(\rho_2)$$

$$\vdots$$

$$\rho_{k-2} = \rho_{k-1}\gamma_k + \rho_k, \qquad N(\rho_k) < N(\rho_{k-1})$$

$$\rho_{k-1} = \rho_k\gamma_{k+1}.$$

The last non-zero remainder ρ_k is the greatest common divisor of α and β, and it is denoted by $\gcd(\alpha, \beta)$.

The proposed method

The proposed method includes the following process:

The encryption method

1. Alice uses a Polybius square to encrypt the message using the gaussian integer setting.
2. To obtain the corresponding (E, F), Alice uses the formulae (1) and (2) to encrypt each letter of S using the Elgamal method.

5. The Decryption Method

Bob performs the actions listed below after receiving each ciphertext S.

1. Bob uses Formula (3) to decode the pair (E, F) and obtains the appropriate S letter.

2. Bob decodes the pair (E, F) using formula (3) and determines the value of the correct letter S. The message then appears in Table 2 as a result.

Example 5.1: Suppose that $t = 31$, the public key is $p = 71, g = 33, d = 10$, and the private key is $c = 62$. Also, suppose that Alice's message is $S =$ "CAKE", then from Table 2, S is converted to the corresponding Gaussian integers as

$$S = \{s_j\}_{j=1}^{n} = \{3 + 2i, 11, 4 + 3i, 15\}, \text{ where } i = \sqrt{-1}.$$

$$E \equiv g^t \ (mod\ p)$$

$$\equiv 33^{31} \ (mod\ 71)$$

$$\Longrightarrow E \equiv 62 \ (mod\ 71).$$

Also,

$$F \equiv d^t * s_1 \ (mod\ p)$$

$$\equiv 10^{31} * (3 + 2i) \ (mod\ 71)$$

$$\Longrightarrow F \equiv 32 + 45i \ (mod\ 71).$$

Then, $(E, F) = (62{,}32 + 45i)$.

Alice calculates $(62{,}32 + 45i)$. By Formula (3),

$$S \equiv \frac{F}{(E)^c} \ (mod\ p)$$

$$\equiv \frac{32 + 45i}{(62)^{62}} \ (mod\ 71)$$

$$\Longrightarrow S \equiv (13) \ (mod\ 71)$$

Therefore, from Table 2 Bob gets the original letter "C".

$$E \equiv g^t \ (mod\ p)$$

$$\equiv 33^{31} \ (mod\ 71)$$

$$\Longrightarrow E \equiv 62 \ (mod\ 71).$$

Also,

$$F \equiv d^t * s_2 \ (mod\ p)$$

$$\equiv 10^{31} * (11)\ (mod\ 71)$$

$$\Longrightarrow F \equiv 70\ (mod\ 71).$$

Then, $(E, F) = (62{,}70)$.

Alice calculates $(62{,}70)$. By Formula (3),

$$S \equiv \frac{F}{(E)^c}\ (mod\ p)$$

$$\equiv \frac{70}{(62)^{62}}\ (mod\ 71)$$

$$\Longrightarrow S \equiv (11)\ (mod\ 71)$$

Therefore, from Table 2 Bob gets the original letter "A".

$$E \equiv g^t\ (mod\ p)$$

$$\equiv 33^{31}\ (mod\ 71)$$

$$\Longrightarrow E \equiv 62\ (mod\ 71).$$

Also,

$$F \equiv d^t * s_3\ (mod\ p)$$

$$\equiv 10^{31} * (4 + 3i)\ (mod\ 71)$$

$$\Longrightarrow F \equiv 19 + 32i\ (mod\ 71).$$

Then, $(E, F) = (62\ , 19 + 31i)$

Alice calculates $(62{,}19 + 32i)$. By Formula (3),

$$S \equiv \frac{F}{(E)^c}\ (mod\ p)$$

$$\equiv \frac{19+32i}{(62)^{62}} \ (mod\ 71)$$

$$\Rightarrow S \equiv (4+3i)\ (mod\ 71)$$

Therefore, from Table 2 Bob gets the original letter "K".

$$E \equiv g^t\ (mod\ p)$$

$$\equiv 33^{31}\ (mod\ 71)$$

$$\Rightarrow E \equiv 62\ (mod\ 71).$$

Also,

$$F \equiv d^t * s_4\ (mod\ p)$$

$$\equiv 10^{31} * (15)\ (mod\ 71)$$

$$\Rightarrow F \equiv 18(mod\ 71).$$

Then, $(E, F) = (62,18)$.

Alice calculates $(62,18)$. By Formula (3),

$$S \equiv \frac{F}{(E)^c}\ (mod\ p)$$

$$\equiv \frac{18}{(62)^{62}}\ (mod\ 71)$$

$$\Rightarrow S \equiv (15)\ (mod\ 71)$$

Therefore, from Table 2 Bob gets the original letter "E".

Security analysis

The Elgamal Public-Key cipher system in the field of Gaussian integers provides an extension of the beauty algorithm in the field of Gaussian integers. The extension deals with modulo

real Gaussian Primes (primes p: mod 4 = 3). The proposed cipher is supposed to be more secure because the order of the Gaussian Prime generator is $p^2 - 1$ as opposed to p for real integers. This is likely to be a huge advantage as this allows the use of smaller primes, which greatly improves efficiency.

For security testing, the Baby-step Giant-step algorithm was used. The authors found that the Gaussian integer beauty algorithm was probably more powerful than the original because the discrete logarithm took twice as long to compute the Gaussian integers. This is by no means proof that it is robust, However, it is an indication that it can be stronger than the original and we have done this research by applying the Polybius square algorithm to the Gaussian integer beauty algorithm to make the encryption algorithm more difficult

This algorithm increases the difficulty of the cipher, as the Polybius algorithm is an array and each letter consists of two numbers (a row and a column), so it is difficult for the attacker to decipher.

Thus, the encryption system that we worked on in this research is more secure.

Conclusion

In this research, a novel approach to boosting algorithm security is suggested. On the usage of Gaussian integers and Polybius square, the optimization is based. The Polybius square can be applied using the suggested manner. In comparison to the traditional Elgamal method, the findings indicated that the Elgamal algorithm employing Polybius on the Gaussian integer domain was more secure. Additionally, the suggested approach is more secure than the traditional Elgamal algorithm since the proposed algorithm's order is $(p^2 - 1)$, where as the traditional Elagamal algorithm's order is p. That is, the use of lower prime numbers makes the suggested approach more effective than the conventional method, which speeds up the encryption and decryption processes. Therefore, as compared to the traditional Al-gamal algorithm, the suggested technique is secure, efficient, and safe.

References

1. S. Dey, J. Nath, and A. Nath, An Integrated Symmetric Key Cryptographic Method – Amalgamation of TTJSA Algorithm, Advanced Caesar Cipher Algorithm, Bit Rotation, and Reversal method: SJA Algorithm, Int. J. Mod. Educ. Comput. Sci., vol. 4, no. 5, pp. 1–9, 2012. https://doi.org/10.5815/ijmecs.2012.05.01
2. W. Stallings, Cryptography and Network Security Principles and Practices. Prentice Hall, 2015.
3. M. S. Hossain Biswas et al., A systematic study on a classical cryptographic cipher to design the smallest cipher, Int. J. Sci. Res. Publ., vol. 9, no. 12, pp. 507–11, 2019.
4. Have I. Hussein & Wafaa M. Abdullah (2021) An efficient ElGamal cryptosystem scheme, *International Journal of Computers and Applications*, 43:10, 1088-1094, DOI: 10.1080/1206212X.2019.1678799
5. Rajitha Ranasinghe & Pabasara Athukorala (2021) A generalization of the ElGamal public-key cryptosystem, *Journal of Discrete Mathematical Sciences and Cryptography*, DOI: 10.1080/09720529.2020.1857902
6. Dissanayake, W. D. M. G. M. (2018). An Improvement of the Basic El-Gamal Public Key Cryptosystem. *International Journal of Computer Applications Technology and Research*, 7(02), 40-44.
7. Irawadi, S. (2020, October). Discrete Logarithmic Improvement for ElGamal Cryptosystem Using Matrix Concepts. In *2020 8th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-5). IEEE.
8. Stillwell, J. (2003). The Gaussian integers. *In: Elements of Number Theory. Undergraduate Texts in Mathematics*. Springer, New York, NY. https://doi.org/10.1007/978-0-387-21735-2_6
9. Koval, A. (2016). Algorithm for Gaussian Integer Exponentiation. *In: Latifi, S. (eds) Information Technology: New Generations. Advances in Intelligent Systems and*

Computing, vol 448. Springer, Cham. https://doi.org/10.1007/978-3-319-32467-8_93

10. Naganuma, K., Suzuki, T., Tsuji, H., & Kimura, T. (2020). Study of Safe Elliptic Curve Cryptography over Gaussian Integer. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 103(12), 1624-1628.

11. Zahhafi, L., Khadir, O. (2021). A Secure Variant of the Fiat and Shamir Authentication Protocol Using Gaussian Integers. *In: Melliani, S., Castillo, O. (eds) Recent Advances in Intuitionistic Fuzzy Logic Systems and Mathematics. Studies in Fuzziness and Soft Computing*, vol 395. Springer, Cham. https://doi.org/10.1007/978-3-030-53929-0_14

12. D. Salomon, "Data Privacy and Security: Encryption and Information Hiding," Springer, (2003).

13. C. Christensen, "Review of Secret History: The Story of Cryptology by Craig P. Bauer," Cryptologia, vol. 38 no. 2, (2014), pp. 192-193.

14. D. Salomon, "Elements of Cryptography," Foundations of Computer Security. Springer London, (2006), pp. 263-284.

15. D. Salomon, "Coding for data and computer communications," Springer, (2006).

16. Chandan Kumar, Sandip Dutta, Soubik Chakraborthy, A Hybrid Polybius-Playfair Music Cipher, International Journal of Multimedia and Ubiquitous Engineering,2015.