Global Journal of Engineering and Technology Advances

eISSN: 2582-5003

Cross Ref DOI: 10.30574/gjeta

Journal homepage: https://gjeta.com/

(Research Article)

A proposed method for encrypting and sending confidential data using polynomials

Sana Ahmed Kadhim * and Saad Abdual Azize abdual Rahman

Al_Ma'moon University College, Computer science dept, Baghdad, Iraq.

Global Journal of Engineering and Technology Advances, 2021, 08(02), 082–087

Publication history: Received on 26 July 2021; revised on 29 August 2021; accepted on 31 August 2021

Article DOI: https://doi.org/10.30574/gjeta.2021.8.2.0133

Abstract

With the improvements of cyberspace and communications, an essential problem was raised and that is how to secure the transmitted data and keep it confidential. Many techniques have been used for this purpose, some of them were broken but others were stayed immune against different attacks. Complexity of the used technique is one of the major reasons that kept it secure. To increase complexity, mathematics was used. In this paper, a method for encrypting and sending confidential data was proposed. The method depends on mathematical equations for encrypting data, sending and decrypting it. The method is complex, secure and workable.

Keywords: Cryptography; Transmission; Mathematical equations; Polynomials

1. Introduction

In the last decades, transmitting data was one of the most important fields which concerns data security researchers. The extreme development and usage expansion of Internet caused a huge problem, which is, protecting transmitted data from unauthorized manipulation like modifying, damaging or even just reading transmitted data [1]. Cryptography was invented to secure data from any outsiders. Many methods and techniques were invented and improved through time. Complexity is one of the essential concepts in creating any new cryptography method [2]. El-Gamal cryptosystem was invented to encrypt and decrypt confidential messages with specific equations and numbers to be chosen carefully and mathematically [3]. Sending specific data by mathematical equations to construct polynomials was also one of the powerful mathematical methods used in cryptosystems [4]. Shamir and Lagrange are two related equations that could be used for sending information in cryptosystems [5].

In this paper a combination of the previous methods will be used to encrypt a secrete message then use the result in Shamir's polynomial, sending few numbers to the receiver who is going to reconstruct a polynomial with Lagrange to find out the encrypted data which is going to be decrypted to reproduce the plain text.

The next section will explain the methodology of Shamir, Lagrange and El-Gamal. Section three will explain the proposed method. Section four will explain the implementation of the proposed method and finally, the conclusions and the references.

2. El-Gamal, Shamir, and Lagrange Techniques

Each technique used in the proposed method will be explained below [6]:

* Corresponding author: Sana Ahmed Kadhim

Al_Ma'moon University College, Computer science dept, Baghdad, Iraq.

2.1. El-Gamal cryptosystem

El-Gamal encryption is a public key system. Its complexity depends on the difficulty of finding logarithm of modules numbers. The keys of El-Gamal found by a person (receiver) by:

- Choosing a prime number P.
- Choosing random number g.
- a is a primitive number g.
- Compute Y ≡ ga mod P.
- Choosing random number K, such that: 2<= K <= P-2.

The public key is (P, a, g), and the private key is K.

For encrypting the message M:
Compute C1 ≡ gK mod P.
Compute C2 ≡ YK * M mod P
Send (C1, C2) to the receiver.

After encrypting a message, K could be left and use another number for the next transmission. This is an advantage for El-Gamal system since the same message may have different cipher text in each different transmission.

For decrypting the received cipher (C1, C2):

S = C1K mod P
M= C2 * S-1 mod P

2.2. Shamir's polynomial

Shamir's algorithm was used in sharing secrete data by first choosing k different values known as xi, where i between 1 and k, then, the distribution of shared data [7]:

- If the secrete data is N, then N-1 value will be chosen randomly (a1, a2, ., an-1).
- Compute yi = a (xi) for all i <= k, and

$a(x) = \sum_{j=0}^{n-1} ajx^{j} \bmod p$ …… [1]

Where p is a prime number.

- Each person Pi will be given yi.
- The secrete data for Shamir's system is the constant value in the polynomial
- The polynomial couldn't be constructed unless all distributed values are joined in the polynomial.

f (x) = a0 + a1x + a2x2 + _ _ _ + ak-1xk-1 ……… [2]

2.3. Lagrange's Method

Lagrange interpolation formula gives a unique polynomial of degree k-1 for k known points y1, y2, …, yk where yi = a (xi) and [8]:

$$a(x) = \sum_{i=1}^{k} yi \prod_{1 \le j \le k.j \ne i} \frac{x - xj}{xi - xj} \ldots..[3]$$

For a given set of n + 1 nodes xi; the Lagrange polynomials are the n + 1 polynomials defined by

$$\mathrm{Li(xi)} = \begin{cases} 0 \text{ if } i \neq j \\ 1 \text{ if } i = j \end{cases}$$

Then, the interpolating polynomial is defined as

$\mathrm{Pn(x)} = \sum_{i=0}^{n} \mathrm{Li(x)yi}$ …….. [4]

If each Lagrange Polynomial is of degree of at most n; then Pn also has this property. The Lagrange polynomials can be characterized as follows:

$$\mathrm{Li(xi)} = \prod_{j=0, i\neq j}^{n} \frac{x - xj}{xi - xj} \ldots\ldots [5]$$

3. The suggested method

In this paper, the method suggested is combining the previous techniques in one process, where the data to be transmitted has to be encrypted first to ensure the secrecy of the confidential data. The encryption is done using El-Gamal cryptosystem. Then, for each cipher text, Shamir's algorithm is applied and three points are sent.

The suggested method has one common step between the sender and the receiver that step is the keys of El-Gamal. Then, there are five steps for the sender and four steps for the receiver.

3.1. The sender steps

- The sender will encrypt the message using El-Gamal algorithm. For each character (M) of the message, two output will be obtained (C1, C2).
- C1, C2 will be used in Shamir equation, five points will be obtained.
- Using the same random function for sender and receiver, select randomly three points only (for example: (x0, y0), (x1, y1), (x2, y2) → (1, y0), (2, y1), (3, y2))
- Send (y0, y1, y2) to the receiver.

3.2. The receiver steps

- Using the same random function, the receiver knows the sequence of the selected points (1, 2, 3) which means (x0=1, x1=2, x2=3).
- Apply Lagrange equation to find L0, L1, L2.
- Find the interpolating polynomial P (x).
- Extract C1 and C2 from P (x).
- Use C1 and C2 to decrypt the message using El-Gamal algorithm.

4. The Implementation of the suggested method

To implement the proposed method, the consecutive steps of the proposed method will be followed as below:

4.1. The keys of El-Gamal

Each part (sender and receiver) should have his public and private key; let's suppose that the sender has the following keys:

Let a = 6, g = 11, a is primitive of P
Let K = 7, K is a random number
Let P = 23, P is a prime number
Y = ak mod P = 6
Public key = (g, a, Y); private key = K

4.2. The encryption process

Let the message is the letter "M" = 13 (the sequence number in alphabetic)

Y= ga mod p = 116 mod 23 = 9

C1 = gk mod p = 117 mod 23 = 7

C2 = m*yk mod p = (13*97) mod 23 = 6

(C1, C2) = (7, 6)

For each two pairs (C1, C2), three points will be produced using Shamir's polynomial and the Y's are sent.

Construct Shamer's polynomial:

F (x) = C2 + C1x + gx2
= 6 + 7x + 11x2

Compute some points:

F (0) = 6
F (1) = 6 + 7 + 11 = 24
F (2) = 6 + 7*2 + 112 = 64
F (3) = 6 + 21 + 99 = 126
F (4) = 14675
F (5) = 161092

Choose three points randomly:

x0 = 1, x1 = 2, x2 = 3
(x1, y1) = (1, 24)
(x2, y2) = (2, 64)
(x3, y3) = (3, 126)

Send (y1, y2, y3)

4.3. The decryption process

The receiver will use these Y's in Lagrange interpolation to reconstruct the pair (C1, C2) which are going to be decrypted by El_Gamal decryption algorithm to find out the original message.

For decryption use Lagrange equations to extract C1, C2

$$\mathrm{L0} = \frac{\mathrm{x - x1}}{\mathrm{x0 - x1}} * \frac{\mathrm{x - x2}}{\mathrm{x0 - x2}}$$

$$\mathrm{L0} = \frac{\mathrm{x} - 2}{1 - 2} * \frac{\mathrm{x} - 3}{1 - 3}$$

$$\mathrm{L0} = \frac{\mathrm{x}^2 - 5\mathrm{x} + 6}{2}$$

$$\mathrm{L1} = \frac{\mathrm{x - x0}}{\mathrm{x1 - x0}} * \frac{\mathrm{x - x2}}{\mathrm{x1 - x2}}$$

$$\mathrm{L1} = -\,(\mathrm{x}^2 - 4\mathrm{x} + 3)$$

$$\mathrm{L2} = \frac{\mathrm{x - x0}}{\mathrm{x2 - x0}} * \frac{\mathrm{x - x1}}{\mathrm{x2 - x1}}$$

$$L2 = \frac{x^2 - 3x + 2}{2}$$

Then:

$$P(x) = \frac{x^2 - 5x + 6}{2} * 24 - (x^2 - 4x + 3) * 64 + \frac{x^2 - 3x + 2}{2} * 126$$

P (x) = (12 x2 – 60 x + 72 – 64 x2 + 256 x – 192 + 63 x2 – 189 x + 126)

P (x) = 6 + 7x + 11x2

So,

(C1, C2) = (7, 6)

To decrypt the message:

S = C1a mod p

= 76 mod 23

= 4

M = C2 * S-1 mod p

= 13

So the decrypted message is the letter ‘M’

The benefit of El_Gamal algorithm is that if the sender use different random number in his process then C1 and C2 will be different even for the same letter. Let the message be the word “DOOR”, then, by applying the algorithm, the result will be as in table 1 below:

Table 1 Different results for the same letter

	D	**O**	**O**	**R**
Sender random key	60	112	37	7
Sequence number	3	13	13	17
C1	131	86	58	109
C2	32	28	46	40

The decryption will not affected by the choice of the different random numbers of the sender and the original letters will surly reconstructed successfully.

5. Conclusion

Transmitting secrete message between different parities required an attention to be sure that the data will not be manipulated or read by unauthorized outers. Cryptography system used to encrypt the data before transmission so that even if it is hijacked it won’t be readable. El-Gamal algorithm is one of the well known cryptosystems that had been used for decades. In the other hand, Shamir sharing system and Lagrange interpolation were proved to be complex, secure, and workable for data transmission. Combining the previous methods in one process (the suggested method) ensures having the benefits of all methods together. It provides encryption, secrete distribution, and complex reconstruction of the received data before decryption.

Compliance with ethical standards

Acknowledgments

The authors would like to thank the staff of Al_Ma'moon University college for their support.

Disclosure of conflict of interest

Both authors certify that they have participated sufficiently in the work to take public responsibility for the content.

References

[1] Cryptography and Network Security: Principles and Practice, William Stallings, Prentice Hall Press Upper Saddle River, NJ, USA. 2010.

[2] Goichiro Hanaoka. On the properties of public key encryption from group signatures, Publisher: ACM. May 2013.

[3] Jesse Russell, Ronald Cohn. Elgamal Encryption, Book on Demanid. 2012.

[4] James F. Epperson. An Introduction to Numerical Methods and Analysis, Wiley. ISBN 0-471-31647-4. 2001.

[5] Adi Shamir. On the generation of multivariate polynomials which are hard to factor, Publisher: ACM. June 1993.

[6] The nearest polynomial of lower degree, Robert M. Corless, Nargol Rezvani, Publisher: ACM. July 2007.

[7] Salomaa, Arto. Public-Key Cryptography", sipringers. 1990.

[8] S Patil, N Rana, D Patel, Prajol Hodge. Extended Proactive Secret Sharing using Matrix", International Journal of Scientific and Engineering Research, vol. 4, no. 6, 2024-2029. June 2013.

[9] S Salim, S Suresh, R Gokul, S Reshma. Application of Shamir Secret Sharing Scheme for Secret Data Hiding and Authentication, International Journal of Advanced Research in Computer Science and Technology. April - June 2014; 2 (2): 220-224.

[10] S Ahmed, S Abdualazize. Embedding Secrete Message in Transformed Voices File using a New Method for Position Selection, Electronic ISBN: 978-1-5386-9188-5, Print on Demand (PoD) ISBN: 978-1-5386-9189-2. 14 February 2019.

[11] S Ahmed, S Abdualazize. Preventing Unauthorized Access to Special Applications using Signed Audio, International Journal of Civil Engineering and Technology (IJCIET), CiteScore:2.76, SJR:0.246, SNIP:0.153, Impact Factor:9.7820, ISSN:0976-6316.

[12] S Ahmed, S Abdualazize. A Proposed Method for Image Verification by Encrypted Hidden Text using a Chaotic Polynomial and Random Locations, International Journal of Civil Engineering and Technology (IJCIET), CiteScore:2.76, SJR:0.246, SNIP:0.153, Impact Factor:9.7820, ISSN:0976-6316.