Modified ElGamal Algorithm Using Three Paring Functions

Eman Hatem Omran and Rana Jumaa Sarih Al-Janabi

Abstract Cryptography defines different methods and technologies used in ensuring that communication between two parties over any communication medium is secure, especially in presence of a *third* part. This is achieved through the use of several methods, such as encryption, decryption, signing, generating of pseudo-random numbers, among many others. Cryptography uses a key or some sort of a password to either encrypt or decrypt a message that needs to be kept secret. This is made possible using two classes of key-based encryption and decryption algorithms, namely symmetric and asymmetric algorithms. The best known and the most widely used public key system is ElGamal. This algorithm comprises of three phases, which are the key generation phase, encryption phase, and the decryption phase. Owing to the advancement in computing technology, ElGamal is prone to some security risks, which makes it less secure. The following paper previews combination of three paring function used to enhance the ElGamal algorithm and increase its security. The results showed that the modified algorithm gives 93% accuracy.

Keywords Cryptography · ElGamal algorithm · Encryption · Decryption · Cryptosystem · Security · Public key · Private key · Paring functions

1 Introduction

Cryptography is the study of algorithms that provides a security service and protects the integrity of data, algorithms that guarantee the authenticity of the source of data, and algorithms that provide confidentiality for data (encryption algorithms). Privacy is at the heart of cryptography. Coding is a functional means to achieve data privacy [1]. Cryptography played a vital role in many aspects of our world today, such as online banking and E-commerce operations and E-mail. Understanding the principles

E. H. Omran (✉) · R. J. S. Al-Janabi
Computer Science Department, University of Alqadisiyah, qadisiyah, Iraq
e-mail: com.post15@qu.edu.iq

R. J. S. Al-Janabi
e-mail: rana.aljanaby@qu.edu.iq; rana.aljanaby@gmail.com

R. Kumar et al. (eds.), *Next Generation of Internet of Things*, Lecture Notes in Networks and Systems 445, https://doi.org/10.1007/978-981-19-1412-6_35

of encryption depends on the knowledge of many topics such as complexity and pure mathematics [2]. Encryption is separated into two basic forms (symmetric encryption also named private key encryption uses the similar key to encode and decode like stream cipher and block cipher), and asymmetric encryption also named public key coding uses two couples of key, one to code the message and the other to the encode, the first is identified as public key because it is identified to operator in the chosen situation, it is utilized to code messages, while the next is known as private key so termed because he is recognized to only one operator which is the owner and is utilized to decode encrypted messages public key. The goals of cryptography can be descripted as the following:

(a) **Confidentiality**: It confirms that only official personnel can access data. Hiding data by encrypting information is one method to provide secrecy.
(b) **Data integrity**: It confirms that it is possible to identify unauthorized adjustments to the information. It also saves against an attacker changes documents through transportation, like interrupting an E-mail message and changing the message before sending it to the receiver.
(c) **Authentication**: It confirms that data is created from the operator or computer that claims to have sent the data. It also saves against imposters and man-in-the-central attacks.
(d) **Non-repudiation**: It certifies that an operator cannot deny acting a job or transfer data. For sample, non-repudiation confirms that a party to an agreement cannot refute having signed the agreement.
(e) **Anti-replay protection**: Avoids an attacker from interrupting a message and transfers it later. For example, an attacker can detention a logon sequence and then replay the system packs to logon at a later time. Anti-replay protections, like addition encrypted time brands to information, stop such attack.

2 Related Works

Galindo and Großschädl [3], they said that leakage-flexible cryptography purposes to expand the rigorous promises succeeded over the verifiable safety example to physical applications. The structures planned on based of this different method necessarily hurt from an Achilles foot: A restricted outflow supposition is required. At present, a massive gap occurs amid the concept of many projects and their application to approve the outflow flexibility in training. The current job efforts to thin this hole for the outflow-tough interconnected ElGamal key encapsulation device (BEG-KEM) offered in 2010. Their main influence in the different of a restricted seep and first-calculation-seepages ideal that is nearer to training. We deteriorate the limit on the document extent of the leak jobs in all types.

Siahaan and Elviwani [4], an asymmetric process is a coding method that utilizes alternative solutions on the procedure of coding and decoding. This process utilizes two answers, open key and special key. The open key is openly divided, whereas the user keeps the special key privately, and answer needs the period for decoding procedure. RSA and ElGamal are dual processes that appliance an open key cryptosystem. The power of the process dishonesties in the while distance utilized. The gradation of struggle in RSA is located in the separating of big peaks, whereas ElGamal is located in a computation of separate algorithms. In later experimentation, it is confirmed that RSA completes a quicker coding procedure than ElGamal, while ElGamal decoding procedure is quicker than RSA. All of these processes are cryptographic open key processes, then got purposes in various techniques. RSA is an imperative process, whereas ElGamal is a potential process.

Magsino and Arboreta [5], they supposed that the credit card amount could be protected by hiding the main figures to a ciphertext. Altered techniques of encryption could be utilized, but several of individuals are disposed to each physical strength offense particularly and have been utilized through various. This suggests into mixture of the ElGamal coding system and RSA and chaos process. The originality of scheme and haste has been proved to show the competence of the fresh scheme. The tests have proved that the algorithm of the new cryptosystem is more secure than its parent cryptosystems (RSA and ElGamal). But, the speed of the new system is slightly slower than its parents. The RSA algorithm can be slower depending on the chosen encryption key. Overall, the new cryptosystem is found efficient to use in credit card number encryption.

Jia1 et al. [6] ElGamal cryptography is unique of the greatest significant public key cryptography (PKC), meanwhile it was suggested while these PKCs which are grounded on solid issue that separate process issue and numeral factorization issue are weak with improvements in volume CPUs. So, selected replacements must be suggested two ElGamal-like open key coding systems grounded on big abelian subcategory of official linear collection over a remainder ring, but the two structures were not extended; earlier, it was verified risky through us. Then, in (2016), they projected a better-quality cryptosystem, which contains resistance of my occurrence on 'NEURAL COMPUTING & APPLICATIONS.' Through examining the safety of the open key cryptography, we suggest an enhanced technique of arithmetical answer-resuscitation offense in the mathematical calculation difficulty despising the inventors' right that the cryptosystem is best safety. In addition, they deliver consistent applied attack instance to show the offense process in our cryptanalysis, whereas disruptions examples are demanding 10 bytes of safety fewer than 60 s on a solo PC workstation.

Mani and Begam [7], in their paper, they supposed that the possible weakness of ElGamal cryptosystem is the ciphertext shaped which is continuously doubled as extended to the normal text to the communication development via a feature of dual earnings location through coding. After the letter is very lengthy, the ciphertext formed by the ElGamal cryptosystem is also extended for example; once the ciphertexts are conveyed over the message station, which goes to deliver fewer safeties cause, if the opponent interrupts anybody of the ciphertext after dual ciphertexts for

both charm of the Normal text, the additional might be saved simply because there is a connection in the middle of the dual ciphertexts. Doubt dual ciphertexts are descending by one; the opponent might not be talented to expect the dual ciphertexts from single. To improve the safety of ElGamal algorithm, the dual Cantor purpose, Rosenberg pairing purpose, and Elegant pairing purposes are utilized in this research. Once the supposed meanings are utilized, the dual ciphertexts shaped through each normal text charm are decline by one, so that the opponent will not simply be improved by the normal text. New outcomes obviously exposed improving the safety of ElGamal algorithm afterward joining the combination jobs in it.

3 Asymmetric Cryptography

Once it arrives to the term 'Encryption,' we celebrate it as a method that guards documents employing a cryptographic answer, and there is nothing incorrect with this. Nevertheless, what greatest people do not understand is that there are a lot of types of coding systems. Asymmetric coding, also named as public key cryptography, is an illustration of one kind. Different 'standard' (symmetric) coding, asymmetric encryption code and decode the information by dual isolated exactly linked cryptographic answers. These answers are called as a 'Public Key' and a 'Private Key.' Both are named as 'Public and Private Key pair. Let us show how these dual keys action with each other to make the difficult power that is asymmetric coding [8].

Asymmetric coding usages dual different, yet connected keys. First key, the open key, is applied for coding, and the second, the special Key, is for decoding. As indirect in the term, the private answer is proposed to be secret so that just the certified receiver could decode the letter.

Let us know this with a asymmetric encryption sample. Imagine you are a snooping action and you want to plan an apparatus for your managers to transfer it safely. You do not want double-method statement, they got their instructions, and you only want normal itemized reports upcoming in from them. Asymmetric coding would let you to make public answer for the operator to code their data and a private answer back at control center that is the just method to decode it all. This offers a solid system of first-technique connection (Fig. 1).

At the main of asymmetric coding drops a cryptographic process. This procedure uses a main group procedure (a type of scientific purpose) to produce a key pair. All these keys are arithmetically related with one another. This connection in these keys is different from one system to other. The process is a mixture of dual jobs—coding purpose and decoding purpose. To state the clear, the coding mean codes the information and decodes meaning decode it [9].

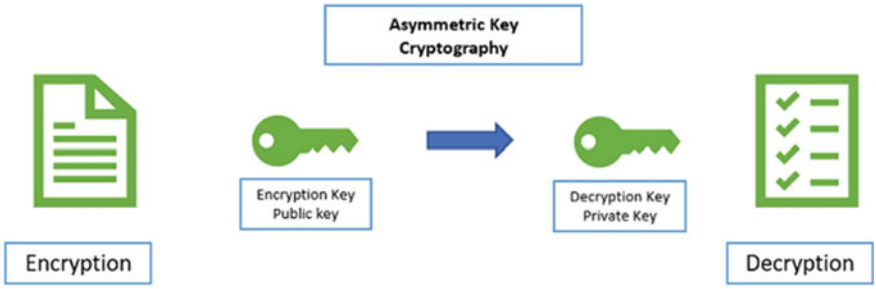

Fig. 1 Asymmetric key cryptography

4 Proposed System

The proposed system in this paper is to encrypt and decrypt the texts by adding three paring functions to ElGamal algorithm. Their paring functions are Cantor pairing function, Rosenberg-Strong pairing algorithm, and Elegant pairing algorithm, the goal of this algorithm is to check if their functions are getting better encryption and decryption results than the original ElGamal algorithm, and the steps of the proposed algorithm are showed in Algorithm 1 and in Fig. 2.

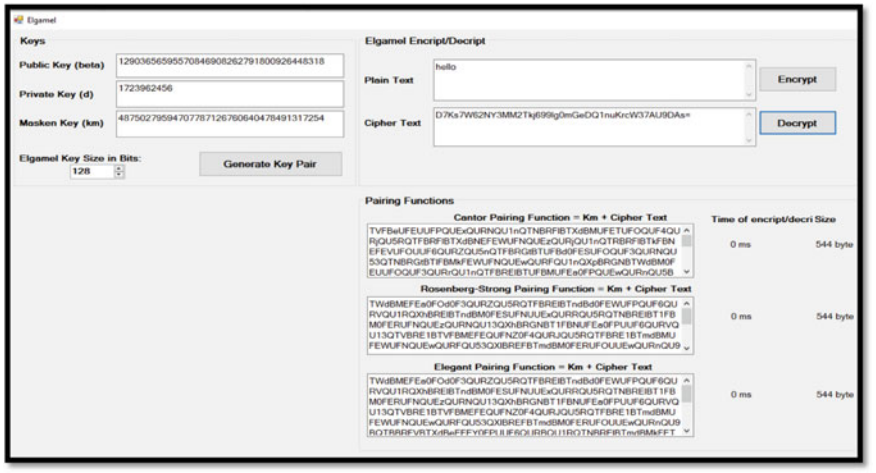

Fig. 2 Execution of the combination algorithms

Algorithm 1: the combination of ElGamal with 3 paring functions
Input: plaintext
Output: ciphertext (encryption and decryption)
Begin **Step1**: generate random keys for cipher in ElGamal and for that we use this method to generate large primary random number for the key (p) **Step2**: generate other random number by bit number **Step3**: start cipher using ElGamal algorithm **Step4**: start cipher using main method named Cantor Pairing Function **Step5**: now cipher using next method named Rosenberg-Strong Pairing Function **Step6**: Start cipher using third method named Elegant Pairing Function **Step7**: display the result of ciphering on monitor **Step8:** finally decrypt the ciphertext to get the plaintext once again **End**

(a) Cantor Pairing Function

Assume some group B, a pairing purpose for B is a 1–1 message of the group of orderly pairs B^2 to the group B. The usual B is supposed to remain limited with pairing purposes; it consumes less from dual features. A pairing purpose aimed at B essentially occurs, if B is unlimited. The Cantor's pairing purpose [10, 11] to the numbers is of the method

$$c(x, y) = z = 1/2(x^2 + 2xy + y^2 - x - 3y + 2) \tag{1}$$

(b) Rosenberg-Strong Pairing Function

The Rosenberg-Strong pairing algorithm [12] to the undesirable numbers is clear via the formulation

$$r(x, y) = (\max(x, y))^2 + \max(x + y) + x - y \tag{2}$$

In the setting of the Rosenberg-Strong pairing function, the amount max(x, y) is supposed to be the seashells integer of the point (x, y). The opposite of the Rosenberg-Strong combination purpose r(x, y) is specified by the formulation

$$r^{-1} = \begin{cases} (z - m^2, m) & , if\ z - m^2 < m \\ (m, m^2 + 2m - z)\,, \text{ otherwise} \end{cases}$$

(c) Elegant Pairing Function

If x and y are undesirable numbers of Elegant pairing algorithm. Formerly, E(x, y) outcome is only undesirable number that is exclusively related with that pair [13].

$$E(x, y) = z = \begin{cases} y^2 + x & x \neq \max(x, y) \\ x^2 + x + y & x = \max(x, y) \end{cases}$$

Table 1 ElGamal algorithm enhanced with pairing functions experimental results of ten times the sentence for 128 key sizes

Algorithm name	Encryption time (MS)	Decryption time (MS)	Total time (MS)	Encryption speed (kb/s)	Decryption speed (kb/s)	Total speed (kb/s)	Block size (bits)
ElGamal (default)	0.001	0.01	0.011	1648.43	164.84	1813.27	128
Cantor	0.005	0.031	0.036	4227.343	681.82	4909.163	128
Rosenberg-Strong	0.003	0.025	0.028	7045.57	845.46	7891.03	128
Elegant	0.009	0.074	0.083	2348.52	285.63	2634.15	128

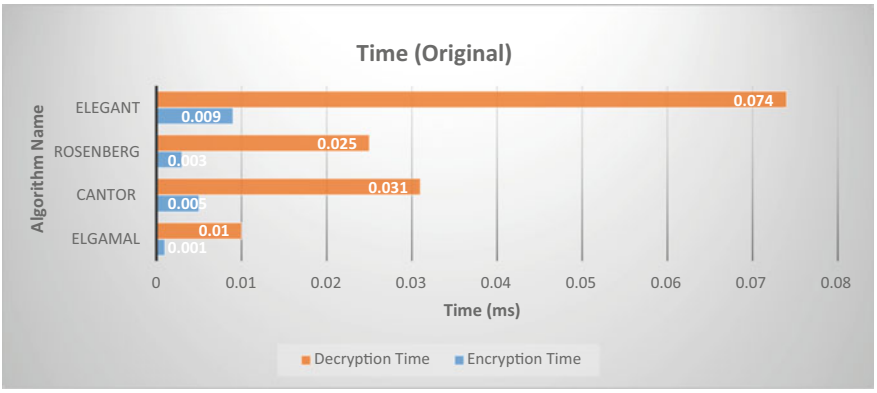

Fig. 3 Encryption and decryption time across the proposed algorithms for 128-bit key size

5 Experimental Results

This is the enhanced version of our proposed system where a plaintext goes through two ciphering operations; the first one is the default ElGamal algorithm, while the second encryption is through one of the pairing functions (Cantor, Rosenberg-Strong, and Elegant). Hence, there are three ciphertexts. The experimental results of ciphering ten times the sentence '**the quick brown fox jumps over the lazy dog**' are shown in Table 1 and are for 128 key sizes in bits, respectively, (Figs. 3 and 4).

6 Conclusion

An improved form of ElGamal coding with triple alternative pairing algorithm is supposed of and applied them effectively. The trial outcomes obviously designated to rise in the safety rank of ElGamal coding when pairing algorithm are applied into it. The purposes of getting the right evaluation results of applying the plaintext on different algorithms giving ElGamal key size a fixed value each time makes it easier

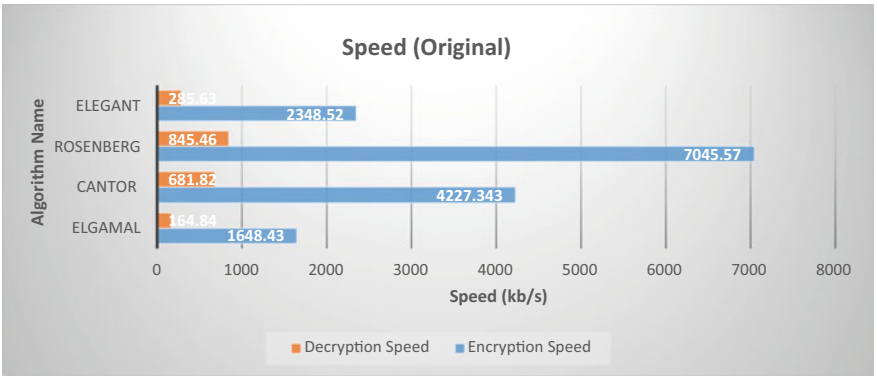

Fig. 4 Encryption and decryption speed across the proposed algorithms for 128-bit key size

to monitor the change in encryption measurement parameters as shown in Table 1 above by setting the key size to 128. The results show that with a fixed block size and key size, the encryption and decryption speed of Cantor pairing function is faster than ElGamal default algorithm and both Rosenberg-Strong and Elegant pairing functions. With that is said, the encryption and decryption time of both Rosenberg-Strong and Elegant pairing functions is less than others. On the other hand, the ciphertext size of all pairing functions is greater that ElGamal default algorithm in multiple times. Of course, all of that has to do with how each algorithm works especially that each algorithm has different number of mathematical operations.

References

1. Dent AW, Mitchell CJ (2005) User's guide to cryptography and standards, Artech House. INC, USA
2. Talbot J, Welsh D (2006) Complexity and cryptography an introduction. Cambridge University Press, UK
3. Galindo D et al (2014) Implementation of a leakage-resilient ElGamal key encapsulation mechanism Springer special section on proofs
4. Siahaan APU, Elviwani, Octavian B (2018) Comparative analysis of RSA and elgamal cryptographic public-key algorithms EAI
5. Magsino JP, Arboleda ER, Corpuz RR (2019) Enhancing security of El Gamal encryption scheme using RSA and chaos algorithm for E-commerce application. Int J Sci Technol Res
6. Jia J, Wang H, Zhang H (2019) Cryptanalysis of an ElGamal-like cryptosystem based on matrices over group rings, Springer Nature Singapore Pte Ltd
7. Mani K, Begam BA (2020) Enhancing the security in ElGamal cryptosystem using paring functions. Int J Innov Technol Exploring Eng (IJITEE), 9(4)
8. Tarnish AH (2000) Designing and implementing a stream cipher image cryptography system. (M.Sc. Thesis, University of Technology at Computer Science)
9. Kiraz MS, Uzunkol O (2018) Still wrong use of pairings in cryptography. Appl Math Comput, Elsevier 333:467–479
10. Mrabet MJ (2017) Guide to pairing-based cryptography, 1st edn. Chapman and Hall/CRC, New York

11. Cegielski P, Richard D (2001) Decidability of the theory of the natural integers with the cantor pairing function and the successor. Theor Comput Sci, Elsevier 57:51–77
12. Szudzik MP (2019) The rosenberg-strong pairing function. Discrete mathematics
13. Matthew S (2006) An elegant pairing function. Wolfram Research, Inc.