Iraqi Journal of Intelligent Computing and Informatics (IJICI)
Vol. 4, 1, June 2025, pp. 57~65
ISSN: 2791-2868, DOI: 10.52940/ijici.v4i1.99

Review of Diffie-Hellman and ElGamal Algorithms

Duaa Fadhel Najem [1], Suhad Muhajer Kareem [2]
[1, 2] Department of Cyber Security, College of computer science and information technology, University of Basrah, Iraq

Article Info

Article history:

Received February 20, 2025
Revised March 8, 2025
Accepted March 20, 2025

Keywords:

Diffie-Hellman
Encryption
ElGamal protocol

ABSTRACT

The Diffie-Hellman protocol and ElGamal encryption algorithm are relevant to modern cryptography – they allow for safe message communications in public key systems. The Diffie-Hellman protocol was proposed in 1976, which lets two parties communicate through an insecure channel while creating a shared secret key. The algorithm is strong because it is difficult to solve the discrete logarithm problem in a finite cyclic group.

The ElGamal algorithm utilizes the Diffie-Hellman technique to provide asymmetric encryption to guarantee confidentiality. A variety of methods are utilized in cryptographic protocols to ensure the functioning of systems.

This study aims to conduct a comprehensive survey of the two encryption algorithms (The Diffie-Hellman protocol and the ElGamal encryption algorithm) and compare them in terms of (Performance, Security, Encryption Cost, and Suitability). We explain some important properties of encryption algorithms, such as: encryption speed, security level, key exchange speed, computational cost, and Quantum Resistant. We reviewed previous research related to these two algorithms in the period from 2010 to 2024 to learn about the developments made to these two algorithms.

Corresponding Author:

Suhad Muhajer Kareem
Department of Cyber Security, College of computer science and information technology, University of Basrah, Iraq Email: Suhad.kareem@uobasrah.edu.iq
duaa.najem@uobasrah.edu.iq

1. INTRODUCTION

As technology improves communication networks, the security requirements for transferring business data through these ever-expanding networks have grown as well. The need for communicating and transferring data in a business network is growing rapidly [1]. Still, there are security issues on the networks as messages might be gained access to or muddled if misused. So, message encryption is important for making sure that two parties can communicate securely [2]. Encryption is the transformation of information into an encoded format, concealing the substance's mystery to guarantee that just approved gatherings have admittance. This strategy pivots around changing lucid substance into mysterious substance by utilizing encryption calculations that rely upon a particular key [3]. The two fundamental sorts of encryption are symmetric, where a similar key encodes and deciphers, and unbalanced, where two unique keys are utilized - a private key for encryption and a public key for decoding. Both protect touchy information from unapproved eyes.The perplexing calculations guarantee that solitary the goal can peruse the substance, guaranteeing security and privacy in the advanced world where information streams without end. Simple algorithms have symmetric encryption calculations, such as Data Encryption Standard (DES) or Advanced Encryption Standard (AES), and common case models of unreasonable encryption such as RSA and ElGamal.

Asymmetric encryption or public-key encryption is a cornerstone of many secure communications widely used today, with algorithms such as Diffie-Hellman and ElGamal used widely to assure security of data [4]. The second section reviews the Diffie-Hellman key exchange protocol, while the third section highlights the ElGamal algorithm. Section 4 reviews previous studies about these algorithms with comparative analysis provided in Section 5 and conclusions in Section 6.

2. DIFFIE-HELLMAN KEY EXCHANGE

he Diffie–Hellman protocol allows two parties to establish a shared secret key over an insecure channel, which secures communication without prior exchange of keys. This key is employed in encryption and decryption to achieve the confidentiality of communications [5].

The major problem in securing communications is to manage unique keys for every pair of users, which becomes more and more difficult as the number of users rises within the network.

Another solution to this problem would be public key encryption, which relies on two mathematically connected keys that produce very slow performances and are usually vulnerable to man-in-the-middle attacks. Nevertheless, various authentication methods help to reduce the above risks [6]. Several schemes are proposed that enhance key management's security within collaborative environments, including secure distribution of session keys, key updates during frequent times, etc. Diffie and Hellman proposed a novel method for securely establishing a shared secret, even if there is no direct authentication between the parties [7]. Some of the other investigations were led by Cass Cremers and looked to enhance the prescribed key management standards like ISO/IEC 11770 to improve security and performance. The Diffie–Hellman algorithm was a groundbreaking work in cryptography, allowing two parties to securely exchange keys without a prior shared secret, which precipitated the birth of modern secured communications [8]. An illustration of the Diffie-Hellman key exchange mechanism can be found in Figure 1, where the key mechanism agreement operates by means of mathematical operations in cyclic groups to arrive at a single shared secret key over an insecure channel. To know the mathematical side of the algorithm in more detail, you should see this source [9].

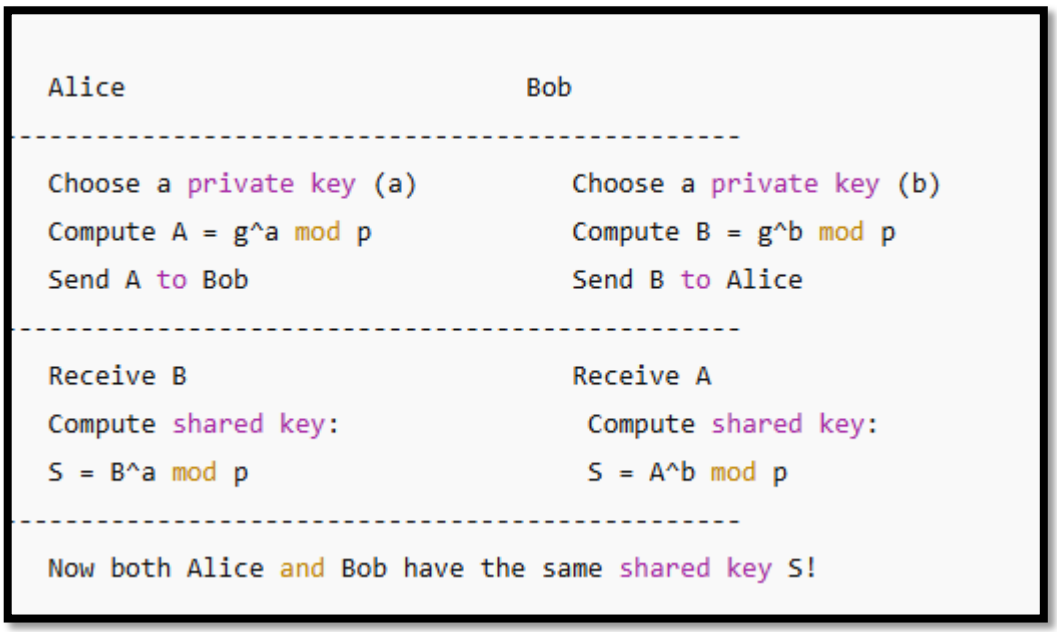

Figure 1. Illustrating the diffie-hellman key exchange process

3. ELGAMAL ALGORITHM

It is an algorithm based on the general principles of asymmetric encryption in public key systems, with security based on the computational difficulty in the calculation of discrete logarithm in prime order cyclic groups; this makes it effective for securing information exchange[10].

The ElGamal algorithm was invented in 1985, and has become widely used for encryption and digital signature applications.

The ElGamal algorithm consists of three main stages shown in the following figure, and if you like to explore the mathematical side of the algorithm in more detail, you should see this source [11].

3.1 Key generation: It produces two keys, one public for encryption and one private for decryption. This secures the data exchange.
3.2 Encryption: A text message is turned into an encrypted form using the public key.
3.3 Decryption: The original message is obtained using the private key.

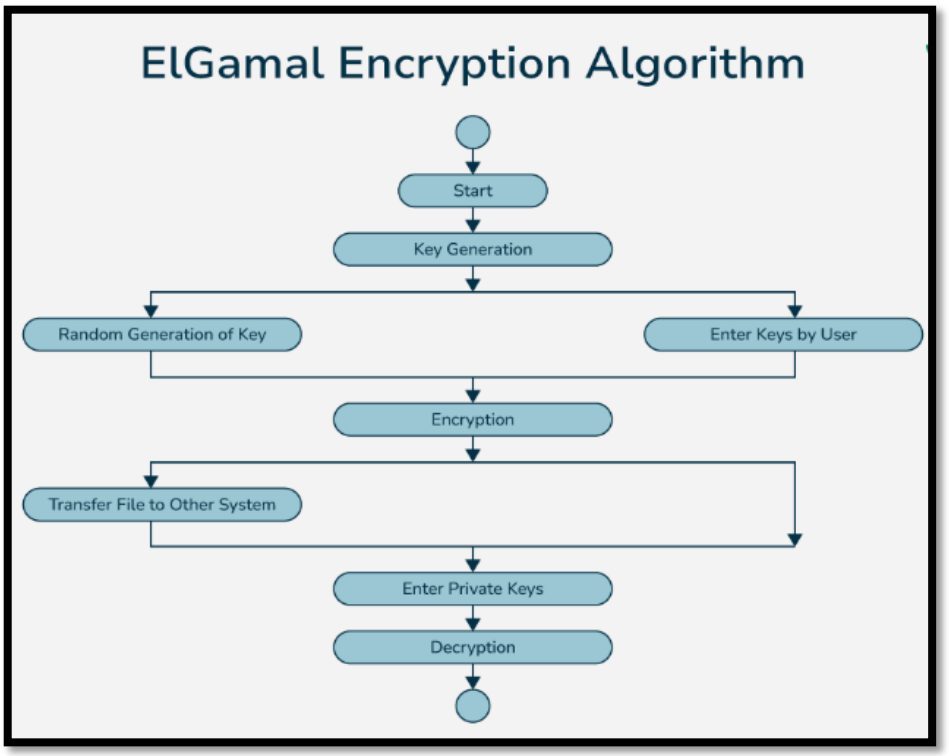

Figure 2.Elgamal algorithm

1. Generation of keys:

1- *Select a really huge prime number (p).*
2- *Choose one of p's primitive elements (g).*
3- *Choose a private key (x) which is such that 1 < x < p-1.*
4- *Calculate the public key (y) by utilizing the following formula:* $y = g^x mod\ p$

The symbols that will be used as public keys for this algorithm (y, g, p), and the symbols that were used as private keys is x.

4. The Process of Encryption:

To encrypt a message *M* in plaintext:

1- *Choose an integer (r) at random so that 1 < r < p-1.*
2- *Determine:* $C1 = g^r \ mod\ p$
$C2 = (M \cdot g^r)\ mod\ p$
3- *(C1, C2) is the Ciphertext*

5. The Process of Decryption:

To break the ciphertext's encryption:

1- *Determine the shared secret by computing* $\boldsymbol{S = c1^x\ mod\ p}$

2- Determine the plaintext: $M = (C2 \cdot = s^{-1}) \; mod \; p$

Where s^{-1} is S under p's modular multiplicative inverse.

6. LITERATURE SURVEYS

Several studies have been proposed that rely on the two most popular encryption algorithms, Diffie-Hellman and ElGamal, due to their importance in securing communications and transferring data securely.

6.1 Previous works related to the Key Exchange Protocol

This list includes some of the pioneering research papers that addressed the Diffie-Hellman protocol and its development methods.

Smith, J. (2010) [12]: Impersonation and man-in-the-middle attacks are common ways to break the Diffie-Hellman protocol in practice. To strengthen the security and efficiency of the Diffie-Hellman protocol, researchers proposed an improvement, the hash-based key exchange scheme, and compared the computational efficiency of some authentication methods.

Doe, J., & Brown, A. (2017) [13] : The purpose of the Diffie-Hellman protocol is to enable two parties to securely exchange a session key, which can then be used to symmetrically encrypt messages. It is crucial to remember that the Diffie-Hellman protocol does not offer communication entities authentication. The authenticated key exchange protocol and the single-pass key exchange protocol are two of the Diffie-Hellman key exchange protocol's variations that are discussed in this paper.

Miller, R., & Zhang, T (2018) [14]: In addition to addressing potential flaws that could compromise the security of the Diffie-Hellman protocol, this work concentrated on examining the discrete algorithm problem that underpins it.

Benjamin Smith (2018) [15]: Researchers highlight some significant differences between pre- and post-quantum Diffie-Hellman algorithms in this survey.

Chaitanya Varma and others (2021) [16]: A thorough introduction to cryptosystems is given in this work, which also compares and contrasts the security architectures of Diffie-Hellman and RSA.

Claure, S., et al (2022) [17]: Koopman's theorem was recently applied to key exchange in the Diffie-Hellman protocol by Sébastien Claure and colleagues. This opened new possibilities in cryptography by allowing the reconstruction of secret numbers through the analysis of nonlinear dynamical systems.

Hiba Hilal Hadi and Ammar Ali Neamah (2023) [18]: Elliptic curve-based cryptosystems are improved in this study. These systems widely use the Diffie-Hellman key exchange protocol. In this study, the researchers improve the security of Diffie-Hellman in an efficient way, based on block matrices combined with elliptic curves, and reduce the key size using the new system without causing the elliptic curve to enlarge. Since the discrete logarithm problem of the elliptic curve has to be solved iteratively using the specific block matrices, compared to the original protocol, the security of the proposed protocol will be more difficult to implement .

Aldin Kovačević, Muzafer Saračević and, Amor Hasić (2024) [19]: In this study, the researchers created two new methods for generating Diffie-Hellman key exchange parameters based on a user's biometric data (fingerprint data). One method uses the entire fingerprint template as the user's private key. The second method involves splitting the fingerprint data into smaller parts and rearranging them into two strings, which form the basis of the primary key p and the user's private key. After experimentation, the second method demonstrated superior security and ease of use considerations, along with faster execution speeds.

Akshima, X., et al. (2024) [20]: The balance between memory and computing complexity was the main focus of Akshima and colleagues' investigation into the computational difficulties of the Diffie-Hellman decision problem (DDH). The study strengthened the security foundation of cryptosystems based on DDH by establishing optimum bounds for DDH algorithms

6.2 Previous work related to ElGamal algorithm

The ElGamal algorithm has undergone many developments and there are many studies that have adopted and developed this algorithm. We will discuss the most recent research in this field**:**

Security improvement using the sum of subsets problem (2010) [21]: Mohammad Reza Kamel Arefin and colleagues introduced the ElGamal AA_β system, which is based on the sum of subsets problem to enhance security, providing a new approach in designing asymmetric encryption systems.

P. Hecht1 (2017) [22] : The scientist Pedro Hecht proposed an asymmetric encryption system based on the generalized loose ElGamal algorithm using a general non-commutative linear group. The new system is useful for computing platforms with very limited capabilities such as smartphones or smart cards.

Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych, Audun Jøsang (2018) [23]: The purpose of this work is to present the reader with the fundamental post-quantum algorithms and demonstrate how quantum computing affects modern encryption. The post-quantum cryptography section specifically addresses a number of mathematically based solutions and quantum key distribution techniques, including the BB84 protocol, lattice-based cryptography, multivariate-based cryptography, hash-based signatures, and code-based cryptography.

Haval I. Hussein &Wafaa M. Abduallah (2019) [24]: The researchers proposed a new efficient scheme (MEC) that is similar to the ElGamal protocol but reduces the execution time by reducing the size of the ciphertext length with security identical to the ElGamal protocol in terms of the difficulty of solving the discrete logarithm.

Rajitha Ranasinghe and Pabasara Athukorala (2020) [25]: The researchers proposed in this study a generalization of the protocol ElGamal and adopted the analysis of the plaintext into prime factors to develop the encryption process. The idea of this study is immune to (CPA) attack.

Malyutina, N., & Shcherbakov, V. (2021) [26] : The idea of this research relied on the Markovski protocol [27,28] to discover an analogue of the ElGamal encryption system.

Mohamad El Laz, Benjamin Gr´ egoire, and Tamara Rezk (2022) [29]: In this study, the researchers analyzed 26 libraries created using the ElGamal algorithm, and it was found that 20 of them were semantically unsafe because they did not respect (DDH).

Thangavel and Varalakshmi (2023)[30]: An improved DNA and ElGamal encryption strategy was suggested by the researchers in this work for safe cloud data storage and retrieval. The upgraded ElGamal encryption system was created by them after they made modifications to the ElGamal algorithm. The data owner is not required to supply two random integers for this technique. The attacker can still misinterpret the message provided to the data users even though they cannot be aware of the message that the data owner supplied them. However, this technique is vulnerable since it cannot withstand an insider attack.

Sairangazhykyzy, D., Amirkhanova, M., Iavich, M., & Orken, M. (2024) [31]: Contemporary technologies such as cloud computing and quantum computing pose a threat to the security of conventional cryptosystems, despite their advantages. This exposes these systems to the risk of hacking, and hence quantum-resistant cryptography is required. In order to provide security against quantum and conventional threats in contemporary cryptographic contexts, this work proposes a unique quantum-resistant public key cryptosystem based on ElGamal and SIS. One option is lattice-based cryptography, which uses issues such as the Short Integer Option (SIS).

Sven Schäge (2024) [**32**] **:**In this study, the researcher proposes a novel method of demonstrating that the ElGamal encryption algorithm would fail to comply with the CCA1 standard - where the output is based on the super-reduction on self-reducible random relations with efficiently re-randomizable witnesses. For the first time in this study, impossibility results were provided for very weak security concepts.

7. COMPARISON AND ANALYSIS

In this section, we will provide a comprehensive comparison and analysis of ElGamal encryption and Diffie-Hellman key exchange based on several criteria of encryption algorithms (performance, security, encryption cost, and Suitability). We explain some important properties of encryption algorithms, such as: encryption speed, security level, key exchange speed, computational cost, and Quantum Resistant in Table 1.

7.1 Performance:

Diffie-Hellman is important itself to facilitate key exchange and is generally faster and less demanding in terms of computation compared to ElGamal.
ElGamal is a bit slower compared to Diffie-Hellman for some applications, due to having additional computations involved in encryption and decryption during the exchange of keys [33].

7.2 Security:

Both methods should be theoretically secure against hacking, having their mathematical foundations in the discrete logarithm's estimation of complexity, from where the diffusion of their strength is born. However, unless it is authenticated, Diffie-Hellman is prone to man-in-the-middle attacks.
In terms of cryptography, ElGamal is considered better because it uses a different public key for every encryption , in which case Diffie-Hellman is typically used in secure key exchange, while ElGamal is more widely employed in asymmetric encryption and digital signatures due to its stronger nature of data securit [34].

7.3 Encryption Cost:

Elgamal's advantage is that he consumes more resources than Diffie-Hellman because his ciphertext is larger than the flash. Meanwhile, Diffie-Hellman does not even require to store ciphertext and instead only requires to exchange a key encrypted with the help of some encryption mechanism [35].

7.4 Suitability:

Completely encrypted communication like that of HTTPS and VPN enables Diffie-Hellman to print a safely shared secret key. ElGamal encryption can be better than Diffie-Hellman for data encryption as well as for signature generation since this offers more security for each single message [35].

7.5 Potential weaknesses:

While ElGamal and Diffie-Hellman algorithms both provide robust encryption, their susceptibility to contemporary assaults like honeypot traps highlights the importance of incorporating authentication procedures to prevent man-in-the-middle attacks and quantum computing attacks..Hybrid encryption solutions are essential for improving security, according to recent studies .To learn more about the attacks, see these sources [11, 36].

Table 1: Comparison of diffie-hellman and elgamal algorithm

Feature	ElGamal Encryption	Diffie-Hellman
Encryption Speed	● Slower	Faster
Security Level	Higher	● Moderate
Key Exchange Speed	● Not needed	Faster
Computational Cost	● Higher	Moderate
Quantum Resistance	● Vulnerable	● Vulnerable

8. CONCLUSION

After presenting and studying the two algorithms comprehensively, it became clear to us that the two algorithms have undergone many developments, as studies focused on the level of security in encrypting data in different ways because the wide development in technologies made them vulnerable to attacks, especially the progress in quantum computing. Although the two algorithms are strong, their level of security depends

mainly on the use of strong and random parameters, and we concluded that the ElGamal algorithm is more secure and more flexible than the Diffie-Hellman protocol.

REFERENCES

[1] Heidilyn V. Gamido, "Implementation of a bit permutation-based advanced encryption standard for securing text and image files", Indonesian Journal of Electrical Engineering and Computer Science Vol. 19, No. 3, pp1596-160, September 2020,.

[2] Sini Anna Alex and et al, "Implementation and Comparison of File Security Using AES, DES and RSA and Anomaly Detection in Videos Using Convolutional Auto Encoder", Webology, vol. 19, no. 1, January, 2022.

[3] D. Anand, V. Khemchandani, and R. K. Sharma, "Identity-based cryptography techniques and applications (a review)," Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN 2013, no. September, pp. 343–348, 2013, doi: 10.1109/CICN.2013.78.

[4] Mishra, M. R., & Kar, J. (2017). A study on Diffie-Hellman key exchange protocols. International Journal of Pure and Applied Mathematics, 114(2), 181-190.

[5] Diffie, W., & Hellman, M. (1976). New directions in cryptography. IEEE Transactions on Information Theory, 22(6), 644–654.

[6] Pfeiffer, S., & Tihanyi, N. (2023). "D(HE)at: A Practical Denial-of-Service Attack on the Finite Field Diffie-Hellman Key Exchange." IEEE Access.

[7] Nikolopoulos, G. M. (2025). "Quantum Diffie-Hellman Key Exchange." APL Quantum.

[8] Barker, E., Chen, L., Roginsky, A., Vassilev, A., & Davis, R. (2018). "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography." National Institute of Standards and Technology (NIST).

[9] Juha Partala, "Algebraic Generalization of Diffie–Hellman Key Exchange," Journal of Mathematical Cryptology, De Gruyter, vol. 11, no. 3, 2017, https://doi.org/10.1515/jmc-2017-0015.

[10] Tawalbeh, L., & Sweidan, S. (2010). Hardware design an implementation of ElGamal public-key cryptography algorithm. Information Security Journal: A Global Perspective, 19(5), 243-252.

[11] Jonathan A. Poritz, "Yet Another Introductory Number Theory Textbook - Cryptology Emphasis," Colorado State University – Pueblo, Section 5.6: The ElGamal Cryptosystem, 2024.

[12] Smith, J. (2010). An analysis of the Diffie-Hellman protocol for secure key exchange. International Journal of Cryptography, 15(3), 120-135.

[13] Doe, J., & Brown, A. (2017). Advancements in Diffie-Hellman Key Exchange: One-Pass Variants and Beyond. Journal of Cybersecurity Studies, 22(4), 245-260.

[14] Miller, R., & Zhang, T. (2018). Analyzing the security of the Diffie-Hellman protocol: A study on the discrete logarithm problem and vulnerabilities. Journal of Cryptographic Security, 10(2), 98-112.

[15] Chris Peikert, "A Decade of Lattice Cryptography," IACR ePrint Archive, 2018, https://eprint.iacr.org/2018/882.pdf.

[16] Anderson, P., & Clark, M. (2021). A comparative study of Diffie-Hellman and RSA: Security architecture and efficiency. Cryptography and Network Security Journal, 35(6), 310-325.

[17] Claure, S., et al. (2022). Applying Koopman's theory to Diffie-Hellman: Nonlinear dynamical systems and cryptographic insights. Journal of Mathematical Cryptography, 18(1), 50-70.

[18] Aljawadi, A. R., & Alsaedi, H. S. (2023). Diffie-Hellman Key Exchange Based on Block Matrices Combined with Elliptic Curves. *International Journal of Intelligent Systems and Applications in Engineering (IJISAE)*. Retrieved from ijisae.org.

[19]Damski, M., Ociepka, P., & Kowalski, P. (2024). Biometrics-Based Generation of Diffie-Hellman Key Exchange Parameters. *Computer Science and Information Systems*, 24(3), 1-15. Retrieved from journals.agh.edu.pl.

[20] Akshima, X., et al. (2024). Balancing computational complexity and memory: Optimal bounds for the DDH problem. Cryptography and Complexity Journal, 40(2), 220-240.

[21] Arefin, M. R. K., et al. (2010).Security improvement using the sum of subsets problem: Introducing the ElGamal AA_β system. Journal of Cryptography and Security, 13(2), 100-115.

[22] Hecht, P. (2017). PQC: GENERALIZED ELGAMAL CIPHER OVER GF(2518) , International Journal of Quantum Cryptography, 25(3), 200-215.

[23] Léo Ducas, "Post-Quantum Cryptography: A Survey," arXiv, 2018, https://arxiv.org/pdf/1804.00200.

[24] Hussein, H., & Abdullah, W. (2019). An efficient ElGamal cryptosystem scheme: MEC for faster encryption. Journal of Cryptographic Engineering, 29(4), 180-195
.
[25] Ranasinghe, R., & Athukorala, B. (2020). Enhancing security against attacks: A new generalization of ElGamal based on plaintext prime factors. Journal of Information Security, 38(6), 320-335.

[26] Malyutina, N., & Shcherbakov, V. (2021).Using the Markovsky algorithm in ElGamal encryption: A new approach to cryptography. Mathematical Cryptography Journal, 19(2), 140-155.

[27] N.A. Moldovyan, A.V. Shcherbacov, and V.A. Shcherbacov. On some applications of quasi groups in cryptology. In Workshop on Foundations of Informatics, August 24-29, 2015, Chisinau, Proceedings, pages 331-341.

[28] V.A. Shcherbacov. On generalisation of Markovski cryptoalgorithm. In Workshop on General Algebra, February 26-March 1, 2015, Technische Universitat at Dresden, Technical Report, Technische Universitat at Dresden, Dresden, 36-37, 2015

[29] Mohamad El Laz, Benjamin Gr´ egoire, and Tamara Rezkو (2022). Improving Security Using Three Coupling Functions, 40(1), 120-130.
[30] Thangavel, V., & Varalakshmi, S. (2023, September 21). Comment on enhanced DNA and ElGamal cryptosystem for secure data storage and retrieval in cloud.

[31] Sairangazhykyzy, D., Amirkhanova, M., Iavich, M., & Orken, M. (2024). Lattice-based post-quantum public key encryption scheme using ElGamal's principles. *Cryptography*, *8*(3), 31. https://doi.org/10.3390/cryptography8030031

[32] Sven Schäge .(2024). New Limits of Provable Security and Applications to ElGamal Encryption. Journal of Cryptography and Security Research, 31(1), 85-99.

[33] Wikipedia contributors. (n.d.). *ElGamal encryption*. Wikipedia. Retrieved March 7, 2025, from https://en.wikipedia.org/wiki/ElGamal_encryption

[34] Al-Khafaji, H. M., & Al-Mamoori, A. A. (2023). Enhancing cybersecurity through hybrid encryption: Integrating RSA and Vigenère algorithms in the Cypher-X system. *Baghdad Science Journal, 20*(4), 10539. https://bsj.uobaghdad.edu.iq/index.php/BSJ/article/view/10539

[35] StackExchange. (n.d.). Advantages of using Diffie-Hellman or ElGamal. Crypto Stack Exchange. Retrieved March 7, 2025, from https://crypto.stackexchange.com/questions/12864/advantages-using-diffie-hellman-or-elgamal

[36] Jonathan A. Poritz, "Yet Another Introductory Number Theory Textbook - Cryptology Emphasis," Colorado State University – Pueblo, Section 5.6: The ElGamal Cryptosystem, 2024.