2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986

Baghdad Science Journal

Cybersecurity Enhancement through Hybrid Encryption: Combining RSA and Vigenère Algorithms in the Cypher-X System

Abir AlSideiri*, Saif AlShamsi, Hajar AlBreiki, Manal AlMoqbali, Mithaa AlMaamari, Shaima AlSaadi

Department of Information Technology, Al Buraimi University College, Muscat, Oman.
*Corresponding Author.
ICCDA2023: International Conference on Computing and Data Analytics 2023.

Received 28/12/2023, Revised 19/04/2024, Accepted 21/04/2024, Published 25/05/2024

Abstract

In the contemporary digital landscape, the imperative issue of data security continues to be a prominent concern. Numerous encryption systems have faced challenges stemming from their intricate nature and susceptibility to cyber threats. This study introduces Cypher-X, an advanced encryption and decryption system that adeptly integrates classical algorithms, namely RSA and Vigenère, to fortify data confidentiality. This research endeavors to address prevailing concerns by focusing on three primary objectives: augmenting data security measures, evaluating system efficiency, and identifying vulnerabilities exploited by cyber adversaries. The outcomes of our investigation affirm the robust encryption capabilities of Cypher-X, underscoring its potential for further enhancement through the incorporation of multi-factor authentication and access control mechanisms. In the realm of data security, Cypher-X emerges as a beacon of hope, offering a promising solution to safeguard sensitive information in the digital sphere. It is essential to acknowledge the ongoing necessity for elucidating our research question, methodology, key findings, and practical implications as we navigate the complex landscape of data protection.

Keywords: Cypher, Cypher-X, Encryption, Non-Symmetric algorithms, Symmetric algorithms, Vigenère.

Introduction

Cypher is a term used to describe the process of converting plaintext into cipher text to protect it from unauthorized access. It is a crucial tool in today's world, where information is exchanged online and stored in various digital formats. The need for encryption arises from the growing concern over data breaches and cyber-attacks that can compromise sensitive regarding the reference [1]. The use of encryption technology, such as Cypher, is therefore essential to safeguarding data integrity, confidentiality, and availability.

However, the cybersecurity landscape is constantly evolving, presenting new challenges and vulnerabilities. Hackers are becoming increasingly adept at understanding algorithms, methodologies, and the mathematical principles behind them, enabling them to decrypt messages and steal information more effectively than ever before discerption regarding the reference[2]. This poses a major threat to current encryption systems, especially those that rely on sequential algorithms, as hackers can exploit their predictability and penetrate

2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

multiple layers of defense, such as setting one algorithm followed by another algorithm discerption regarding the reference[3]. This is a big problem because they think that it will be difficult for a hacker to penetrate it, but this is the case. This is not true. If the method did not change and if the algorithms did not integrate differently than before, the hacker will penetrate the first and follow it with the second. It is more like a small doll toy with a smaller doll inside it. Therefore, something different needs to be done in the field of encryption.

Recognizing these challenges, this research seeks to address the shortcomings of current coding methodologies by presenting a new approach. By combining two distinct encryption algorithms and innovating their integration methods, this project aims to revolutionize encryption technology discerption regarding the reference[4-6]. The resulting algorithm not only enhances cryptographic resilience against hacking attempts, but also improves overall efficiency when the algorithms are combined together. The key contributions of this study include:

1. Introducing a novel encryption methodology that mitigates the predictability of traditional algorithms, rendering them more resistant to hacking attempts.
2. Enhancing the efficiency and effectiveness of encryption by optimizing the fusion of disparate algorithms.
3. Providing insights into the methodologies employed by hackers to dismantle encryption systems, thereby facilitating the identification and remediation of potential vulnerabilities.
4. Offering a comprehensive understanding of the broader implications and future directions in encryption technology, paving the way for continued advancements in data security.

The proposed encryption solution, Cypher-X, represents a significant advancement in data security. Leveraging advanced techniques such as the RSA algorithm and the Vigenère cipher, Cypher-X ensures robust protection for sensitive information. By employing a double-layered encryption approach, Cypher-X adds an additional barrier against unauthorized access, instilling confidence in users regarding the security of their data transmissions.

In an era characterized by escalating cyber threats, Cypher-X stands as a beacon of security, offering a secure and user-friendly encryption solution for individuals and organizations alike.

This paper is organized into five sections. First the introduction followed by the literature review. The third section is about the proposed algorithm, and then the results and discussion. Finally, the conclusion and future work.

Literature Review

This section summarizes some literature work about the most widely used algorithms in encryption and decryption:

Encryption converts data in cipher text, Decryption covert the data in plain text. It faces many challenges, most notably Takes more time to encrypt and decrypt data, a discerption regarding the reference[7].

Data is encrypted with private key; cipher text and plain text is also used. It faces many challenges, most notably Here need more time discerption regarding the reference[8].

Security does not degrade as the number of cipher texts an adversary can see increases. It faces many challenges, most notably the level of security is not very high discerption regarding the reference[9].

Protecting data from unauthorized users or different type of attackers. Secondly, the process of encryption is very fast. Third, encryption provides security to data by the shared key. It faces many challenges, most notably Firstly, Better key generation rates. Secondly, the integration of a QKE system into a computer network discerption regarding the reference[10].

AES is fast speed and excellent security. Secondly, transforming message to make them secure and immune to attack. It faces many challenges, most notably .Firstly, stealing your personal data when it is being transferred. Secondly, time consumption discerption regarding the reference[11].

After reading several scientific papers and articles, they indicate the importance of encryption in various

2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

fields. Therefore, a system is created to allow users to code in an easy way[11]. Where, Integration of RSA and Vigenère algorithms: RSA and Vigenère algorithms will be integrated throughout a more secure encryption system. The system will use Vigenère's algorithm to encrypt or decrypt the message with an updated version key made by the algorithm. After, Testing and Debugging: The system will be tested and debugged to ensure that it functions correctly and safely. The project's outputs will include a software application or code that allows users to encrypt and decrypt messages using both the RSA and Vigenère algorithms, along with documentation describing the operation of the system and how it is used discerption regarding the reference[12].

Methods

Cryptography

Cryptography is the practice of securing communication from unauthorized access. A cipher is a technique used to encrypt or decrypt messages, and there are two main types of ciphers as shown in Fig. 1: symmetric and asymmetric (non-symmetric) ciphers. Symmetric ciphers use the same key for both encryption and decryption of a communication discerption regarding the reference[13,14]. The key is kept secret and is participated between the sender and the receiver. Asymmetric or Non-Symmetric ciphers use two different keys-bone for encryption and another for decryption[14]. The encryption key is made public and is used by anyone who wants to shoot a communication to the proprietor of the decryption key.

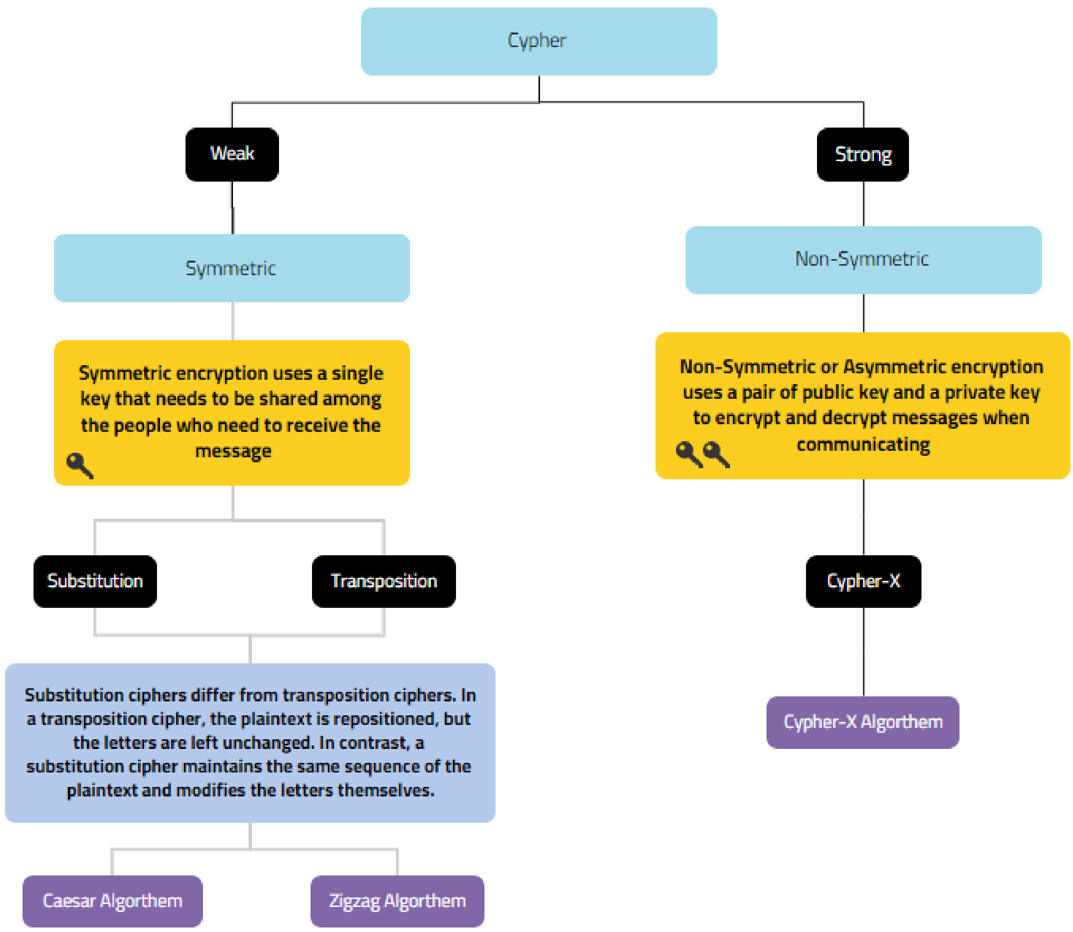

Figure 1. symmetric and asymmetric (non-symmetric) ciphers

2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Proposed Algorithms

The suggested algorithm consists of:

Key Generation: The RSA algorithm is used to induce a public-private crucial brace. The public key is used to cipher the Vigenère key, while the private key is used to decipher it. The Vigenère key is also used to cipher or decipher the communication.

Encryption: To cipher a communication, the Cypher-X system first generates an arbitrary Vigenère key. The Vigenère key is also translated using the public key generated by the RSA algorithm. The translated Vigenère key is also combined with the communication and translated using the Vigenère cipher.

Decryption: To decipher a communication, the Cypher-X system first uses the private key generated by the RSA algorithm to decipher the translated Vigenère key. The decrypted Vigenère key is also used to decipher the communication using the Vigenère cipher.

Security: The Cypher-X system provides a fresh subcaste of protection by using both the RSA algorithm and the Vigenère cipher. This double-layered approach makes it nearly impossible for unauthorized individuals to pierce the information.

User Interface: The Cypher-X system provides a stoner-friendly interface that allows druggies to fluently cipher and decipher dispatches. Druggies can enter the communication and RSA p, q values, and the Vigenère key, also they wish to cipher or decipher, and the system will handle the rest.

Overall, the Cypher-X system provides a largely secure and stoner-friendly encryption and decryption result that can be used to protect sensitive information from unauthorized access discerption regarding the reference[15-17].

Algorithm development process is shown in Fig. 2:

1.Data collection

At this point, precise information is gathered on how to create the Vigenère and RSA encryption algorithms while thwarting any potential outside threats. Additionally, information was gathered regarding the best organizational decisions to make as well as the plan for carrying out this project without making any mistakes in the future.

2.Data analysis

In this step, the raw data collected in the first step was implemented and converted into data that can be seen and implemented in windows to solve the encryption problem of RSA and Vigenère.

3.Algorithm development

At this stage, the algorithms are developed into an innovative, sophisticated, and powerful algorithm, which in turn keeps sensitive information safe from attackers.

4.Algorithm programming

At this stage, a formula or procedure is chosen to be used to solve the problem of theft of private information for companies or other beneficiaries. It depends on performing a series of specific procedures in which you describe these procedures and how to implement them without any problems, and the system will follow the method of this algorithm every time by following a set of procedures consisting of inputs until the correct outputs are obtained (the outputs required in this system) discerption regarding the reference[18] .

5.Algorithm testing

In the last stage, the algorithm is tested and reviewed step by step, to ensure that it is correct and free from errors, provided that the output of the procedures matches the expected outcomes.

5.Algorithm testing

In the last stage, the algorithm is tested and reviewed step by step, to ensure that it is correct and free from errors, provided that the output of the procedures matches the expected outcomes.

2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986

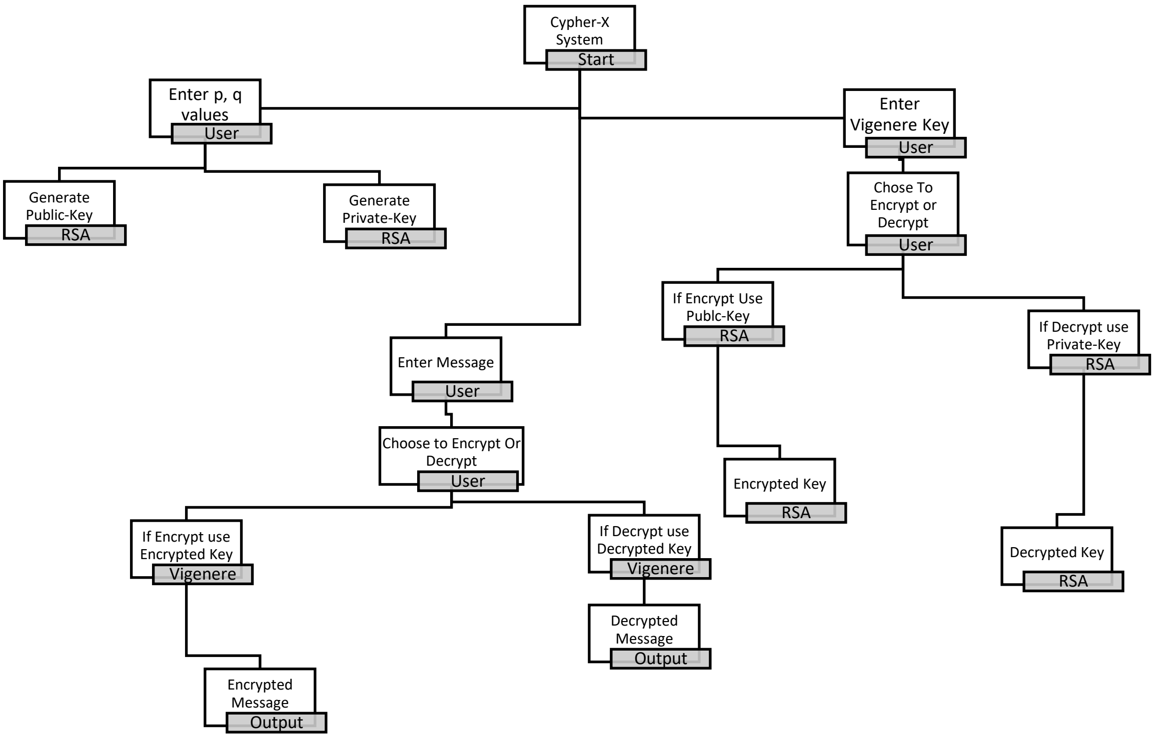

Figure 2. Proposed Algorithm

Results and Discussion

The results presented in Fig. 3 demonstrate the distinct advantages of Cypher-X over conventional ciphers such as the Caesar and Zigzag ciphers. The Caesar cipher, a basic substitution cipher, operates by shifting each letter in the plaintext by a fixed number of positions in the alphabet. However, it is susceptible to decryption through frequency analysis, as the distribution of letters in the ciphertext often mirrors that of the plaintext. Similarly, the Zigzag cipher, functioning as a transposition cipher, rearranges the letters of the plaintext according to a specific pattern. Although the Zigzag cipher offers better security than the Caesar cipher, it is vulnerable to brute force and known plaintext attacks discerption regarding the reference[19,20].

In contrast, Cypher-X utilizes the robust RSA algorithm, providing a significantly higher level of security compared to traditional ciphers. The security of the RSA algorithm lies in the formidable challenge of factoring large numbers, making it extremely difficult for potential attackers to break the encryption. Additionally, Cypher-X incorporates the Vigenère cipher, a polyalphabetic substitution cipher that employs multiple cipher alphabets, significantly increasing the difficulty of decryption compared to simple substitution ciphers like the Caesar cipher.

A key innovation in Cypher-X is the combination of the RSA and Vigenère algorithms, which synergistically enhance security. In this configuration, the RSA algorithm is essential for both encrypting and decrypting the Vigenère key. Subsequently, the Vigenère key is used to encrypt and decrypt the message itself. This dual-layered approach strengthens data protection by combining the fast encryption capability of the RSA algorithm with the robust security features of the Vigenère cipher.

The amalgamation of the RSA and Vigenère algorithms creates a multifaceted security protocol. The RSA algorithm efficiently secures the transmission of the Vigenère key, leveraging its computational efficiency in encryption, while the Vigenère cipher protects the content of the message,

2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

leveraging its encryption strength. Consequently, the combined capabilities of these algorithms enhance the overall security of Cypher-X, ensuring the integrity and confidentiality of sensitive information.

In summary, Cypher-X emerges as a superior solution that surpasses the security capabilities of traditional ciphers like the Caesar and Zigzag ciphers. By harnessing the power of the RSA algorithm and the Vigenère cipher, along with the innovative dual-layered approach, Cypher-X addresses the high-level security requirements of individuals and organizations, effectively securing their most sensitive data and communication channels. This results in a more robust and formidable security architecture, making Cypher-X an invaluable asset in the realm of secure data transmission and communication.

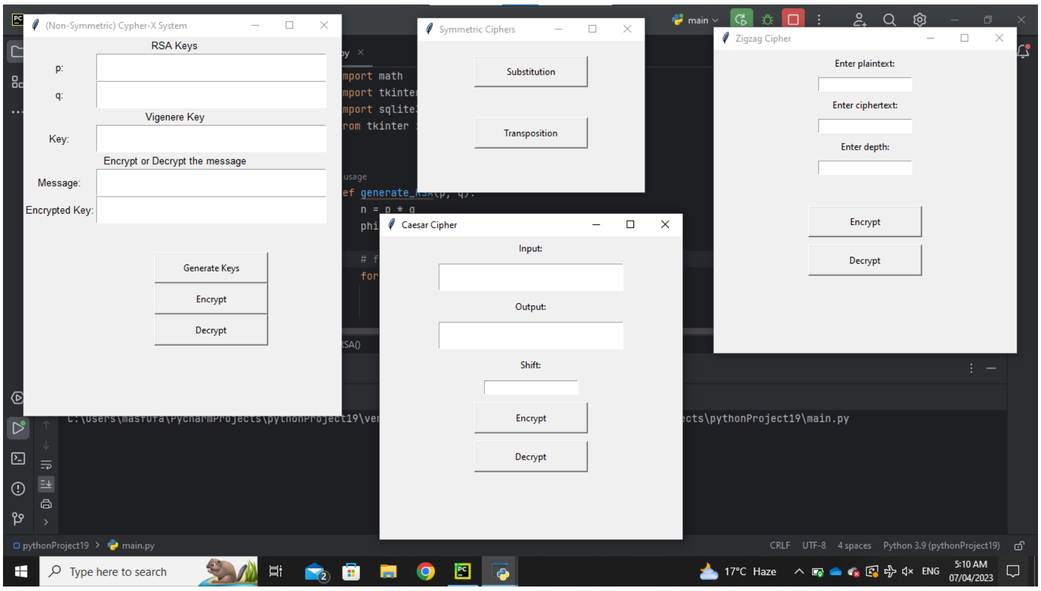

Figure 3. Proposed Algorithm

Table 1 presents a comprehensive evaluation of Cypher-X in contrast to traditional cryptographic methods, specifically the Caesar and Zigzag ciphers. Cypher-X demonstrates its supremacy by offering the highest attainable level of security, underpinned by a combination of the RSA algorithm and the Vigenère cipher within a dual-layered framework, rendering the encryption nearly impervious to decryption attempts. The Caesar cipher, while straightforward to implement, suffers from critical security vulnerabilities. It operates as a basic substitution cipher, where each letter in the plaintext is substituted with a letter located a fixed number of positions down the alphabet. This simplicity, however, makes it susceptible to attacks, particularly through frequency analysis. Consequently, its usage in scenarios where robust data security is essential is discouraged.

In contrast, the Zigzag cipher provides a more secure alternative to the Caesar cipher. Functioning as a transposition cipher, it reorganizes the arrangement of letters in the plaintext according to a predefined pattern. Nonetheless, the Zigzag cipher, though an improvement in terms of security, still exhibits vulnerabilities that could be exploited. Notably, it remains susceptible to threats like brute-force and known-plaintext attacks, limiting its suitability for high-stakes security requirements. Cypher-X, in response to these limitations, emerges as the pinnacle of secure data transmission and communication. It accomplishes this by incorporating the formidable RSA algorithm, renowned for its reliance on the arduous task of factoring large numbers, making it a daunting challenge for potential attackers to decrypt the data. Additionally, Cypher-X leverages the Vigenère cipher, a polyalphabetic substitution cipher, which employs multiple cipher alphabets to heighten the complexity of the encryption process, surpassing the elementary security offered by the Caesar cipher.

The remarkable feature of Cypher-X lies in the synergistic integration of the RSA and Vigenère

2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

algorithms, resulting in an exceptional level of security. This intricate amalgamation warrants scrutiny regarding its execution complexity and performance enhancements when compared to the proposed algorithm. Within this architectural framework, the RSA algorithm plays a dual role, concurrently serving as both the encryptor and decryptor for the Vigenère key. This dual functionality necessitates a closer examination of the system's execution complexity, particularly in terms of computational resource utilization. The Vigenère key, in its pivotal role, contributes to both message encryption and decryption. The impact of this multifaceted involvement on the system's overall execution complexity merits thorough evaluation, as it may influence the efficiency of data protection measures and the system's responsiveness to user needs discerption regarding the reference[19, 20].

The confluence of the RSA and Vigenère algorithms engenders a multi-tiered security protocol. In the context of evaluating performance improvements, it is crucial to assess the computational efficiency of the RSA algorithm, which secures the transmission of the Vigenère key, a critical component in the encryption process. The efficiency of this process directly impacts the system's overall performance and execution time. Concurrently, the Vigenère cipher, known for its encryption strength, guards message confidentiality. Performance enhancements with respect to this aspect would involve evaluating the algorithm's processing speed and resource utilization to gauge its contribution to the system's overall performance improvements discerption regarding the reference[21-23].

In summary, while Cypher-X indisputably surpasses traditional ciphers in terms of security, it is imperative to investigate the execution complexity and performance improvements brought about by its innovative dual-layered encryption approach. The amalgamation of the RSA algorithm and the Vigenère cipher holds the potential to influence the integrity, confidentiality, and availability of sensitive information. This evaluation is particularly relevant in applications where data security is of paramount concern, as it enables a more comprehensive understanding of Cypher-X's operational efficiency and effectiveness in securing data for both individuals and organizations.

Table 1. Comparison Between Different Encryption Method After Testing

Ciphers	Caesar cipher	Zigzag cipher	Cypher-X	AES
Encryption method	Simple substitution cipher	Transposition cipher	Double-layered encryption with RSA and polyalphabetic substitution cipher	AES 256-bit encryption, symmetric block cipher
Level of security	Low	Moderate	High – Very High	Very High
Vulnerabilities	Easily breakable through frequency analysis	Vulnerable to brute-force and known-plaintext attacks	Vulnerable to attacks RSA based on the length of the key	Potential vulnerabilities in implementation
Advantages	Simple to implement and understand	Offers more security than the Caesar cipher	Fusion of RSA and Vigenère algorithms for heightened security - Efficient encryption with RSA - Strong encryption with Vigenère	Utilizes Advanced Encryption Standard (AES) with 256-bit keys - Often regularly updated
Disadvantages	Vulnerable to attacks	Not as secure as modern encryption methods	Requires a key pair, and may require significant computational resources based on the length of the key	May require significant computational resources

Despite the improvements shown by the Cypher-X system, there are still things that make it hard to use and work well. First, the system relies on the RSA code, which can be at risk if the codes made are not random or if the prime numbers used are not big enough. Also, making public and private codes can be hard, especially with prime numbers that have six digits. Also, while the Vigenère code makes things safer, it can still be broken, mainly with short codes or using the same code again. These limits show the need to make the system better and look at other ways to keep info safe from possible attacks.

Conclusion

Cypher-X system uses the RSA algorithm as the encryption and decryption technology in Vigenère keys, providing a reliable method for those who need greater security not only on a personal level but also on a corporate level. However, to further enhance the significance of this study, it is necessary to examine its theoretical and practical implications. This paper plays a vital role in emphasizing the worth of this study. Regarding practical benefits, Cypher-X stands out as a powerful platform for secure data processing providing confidentiality and integrity for sensitive communications and transactions. The flexible nature of its design to various security needs positions it as an important item for organizations that operate in highly regulated environments or handle sensitive information. Nevertheless, it's highly important to admit the study's limitations. The RSA algorithm and Vigenère cipher become the weak points that could be exploited by the adversaries when being relied on. Furthermore, the difficulty in key generation and the chances of a frequency analysis attack require constant vigilance and continuous refinement of the system security features.

Future research avenues should center on addressing these limitations to enhance the system's security and user-friendliness. Enhancements may include incorporating Elliptic Curve Cryptography (ECC) or post-quantum cryptography (PQC) algorithms, which are notably more resilient against quantum computing threats. Moreover, an AI-powered encryption system is planned to develop that leverages novel cipher algorithms, promising heightened security and privacy in applications like communications, financial transactions, and sensitive data storage. Furthermore, future endeavors should investigate strategies to optimize Cypher-X's performance, particularly in large-scale implementations. Options may involve leveraging distributed computing techniques or cloud-based resources to mitigate computational overhead in RSA key pair generation and enhance the efficiency of encryption and decryption operations.

Acknowledgment

We are appreciative of the time, knowledge, and work that our research team and collaborators have put into this project. Their commitment and diligence have been crucial to the accomplishment of this research. We owe a debt of gratitude to the Buraimi University Collage who facilitated the smooth operation of our research activities.

Authors’ Declaration

- Conflicts of Interest: None.
- We hereby confirm that all the figures and tables in the manuscript are ours. Furthermore, any figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- No human studies are present in the manuscript.
- No animal studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in Al Buraimi University, Oman.

Authors’ Contribution Statement

All the authors contributed to the design and implementation of the research, to the analysis of the results and to the writing of the manuscript. A. A. worked in design, data, analysis, revision and proofreading, S A . did the conception and data, analysis, H. Al. contributed in interpretation and data, analysis, M. A. did the acquisition of data and design, M. A. and S. A. contributed in interpretation, drafting the manuscript.

References

1. Abdullah SA, Al Ashoor AA. Ipv6 security issues: A systematic review following prisma guidelines. Baghdad Sci J . 2022 Dec 5; 19(6 (Suppl.)): 1430-. https://doi.org/10.21123/bsj.2022.7312
2. Kumar L, Badal N. A review on hybrid encryption in cloud computing. In2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU) 2019 Apr 18 (pp. 1-6). IEEE. https://doi.org/10.1109/IoT-SIU.2019.8777503
3. AlHamdani W, Sadiq AT, Yasser YA. Honeyword Generation Using a Proposed Discrete Salp Swarm Algorithm. Baghdad Sci J. 2023; 20(2) :567-574. https://doi.org/10.21123/bsj.2022.6930
4. Singh P, Kumar S. Study & analysis of cryptography algorithms: RSA, AES, DES, T-DES, blowfish. Int J Eng Technol. 2017 Dec; 7(1.5): 221. https://doi.org/10.21123/bsj.2022.6930
5. Sood R, Kaur H. A literature review on rsa, des and aes encryption algorithms. Emerging Trends in Engineering and Management (ETEM). 2023 Feb: 57-63. https://doi.org/10.56155/978-81-955020-3-5-07
6. Dişkaya O, Avaroğlu E, Menken H, Emsal A. A New Encryption Algorithm Based on Fibonacci Polynomials and Matrices. Trait Signal. 2022 Oct 1; 39(5): 1453. https://doi.org/10.18280/ts.390501
7. Jintcharadze E, Iavich M. Hybrid implementation of Twofish, AES, ElGamal and RSA cryptosystems. In2020 IEEE East-West Design & Test Symposium (EWDTS) 2020 Sep 4 (pp. 1-5). IEEE. https://doi.org/10.1109/EWDTS50664.2020.9224901
8. Bevers J. The Study of Symmetric and Asymmetric Key Encryptions (Doctoral dissertation, University Honors College, Middle Tennessee State University). https://doi.org/10.18280/ts.390501
9. Verma R, Sharma A. Cryptography: A Comparative Analysis of AES and RSA Algorithms. Mukt Shabd Journal, ISSN. 2020; (2347-3150): 4705-16.
10. Loe A, Medley L, O'Connell C, Quaglia EA. Applications of timed-release encryption with implicit authentication. InInternational Conference on Cryptology in Africa 2023 Jul 13 (pp. 490-515). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-37679-5_21
11. Zhang S, Xie X, Xu Y. A brute-force black-box method to attack machine learning-based systems in cybersecurity. IEEE Access. 2020 Jul 10;8: 128250-63. https://doi.org/10.1109/ACCESS.2020.3008433
12. AlSideiri A, Alsharida RA, Hammood M, Shakir M, Cob ZB, Al Shamsi IR, et al. Users Acceptance Online Attendance Application Using Barcode Scanner: The Case Study in al Buraimi University College (BUC) Students. In2022 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) 2022 Jun 22 (pp. 23-28). IEEE. https://doi.org/10.1109/ICETSIS55481.2022.9888852
13. Khorikov V. Unit Testing Principles, Practices, and Patterns. Simon and Schuster; 2020 Jan 6.
14. Sandhya G, Sharma DK. Software Implementation of Plantlet Stream Cipher Using Verilog Hardware Description Language. InVLSI, Microwave and Wireless Technologies: Select Proceedings of ICVMWT 2021 2022 Sep 4 (pp. 107-118). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-0312-0_12
15. Hamza A, Kumar B. A review paper on DES, AES, RSA encryption standards. In2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) 2020 Dec 4 (pp. 333-338). IEEE. https://doi.org/10.1109/SMART50582.2020.9336800
16. Sarkar A, Chatterjee SR, Chakraborty M. Role of cryptography in network security. The" essence" of network security: an end-to-end panorama. 2021: 103-43. https://doi.org/10.1007/978-981-15-9317-8_5
17. Khan I, Al Sadiri A, Ahmad AR, Jabeur N. Tracking student performance in introductory programming by means of machine learning. In2019 4th mec international conference on big data and smart city (icbdsc) 2019 Jan 15 (pp. 1-6). IEEE. https://doi.org/10.1109/ICBDSC.2019.8645608
18. AlSideiri A, Tawafak RM, AlFarsi G, Khudayer BH, Cob ZC. Development of Online Clearance System Using Web-Based System. In2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT) 2023 Feb 22 (pp. 1-6). IEEE. https://doi.org/10.1109/ICECCT56650.2023.10179667
19. Merkepci M, Abobala M, Allouf A. The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm. Fusion: Practice and Application. 2023; 10(2): 69-74.

2024, 21(5 Special Issue): 1765-1774
https://doi.org/10.21123/bsj.2024.10539
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

20. Erondu UI, Asani EO, Arowolo MO, Tyagi AK, Adebayo N. An encryption and decryption model for data security using vigenere with advanced encryption standard. InUsing Multimedia Systems, Tools, and Technologies for Smart Healthcare Services 2023 (pp. 141-159). IGI Global. https://doi.org/10.4018/978-1-6684-5741-2.ch009
21. Ugbedeojo M, Adebiyi MO, Aroba OJ, Adebiyi AA. RSA and Elliptic Curve Encryption System: A Systematic Literature Review. Int J Inf Secur Priv. 2024 Jan 1; 18(1): 1-27. https://doi.org/10.4018/IJISP.340728
22. Karmakar T, Biswas S, Das I, Nath S. Varibox encryption algorithm: The new generation of hybrid security measure for the era of quantum computation. J Discrete Math Sci Cryptogr. 2022 Feb 25: 1-27. https://doi.org/10.1080/09720529.2021.1968573
23. Challa R, Gunta V. A modified symmetric key fully homomorphic encryption scheme based on Read-Muller Code. Baghdad Sci J. 2021 Jun 20; 18(2 (Suppl.)): 0899. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).0899

تعزيز الأمن السيبراني من خلال التشفير الهجين: الجمع بين خوارزميات RSA وVigenère في نظام Cypher-X

عبير السديري، سيف الشامسي، هاجر البريكي، منال المقبالي، ميثا المعمر، شيماء الساعدي

قسم تقنية المعلومات، كلية البريمي الجامعية، البريمي، مسقط، سلطنة عمان.

الخلاصة

لا يزال أمن البيانات مصدر قلق في عصرنا الرقمي، مع فشل العديد من أنظمة التشفير بسبب تعقيدها وقابليتها للتهديدات السيبرانية. Cypher-X، هو نظام تشفير وفك تشفير متطور، يدمج الخوارزميات الكلاسيكية، RSA وVigenère، لحماية سرية البيانات. ويسعى مشروعنا إلى معالجة هذه المخاوف من خلال التركيز على ثلاثة أهداف رئيسية: تعزيز أمن البيانات، وتقييم كفاءة النظام، وتحديد نقاط الضعف التي يستغلها القراصنة. تؤكد النتائج التي توصلنا إليها قدرات التشفير القوية لـ Cypher-X، مع احتمالات تعزيزها بشكل أكبر من خلال تكامل المصادقة متعددة العوامل وآليات التحكم في الوصول. بينما نتعامل مع المشكلة المتمثلة في أمن البيانات، تبرز Cypher-X كمنارة للأمل، حيث تقدم حلاً واعدًا لحماية المعلومات الحساسة في المشهد الرقمي.

الكلمات المفتاحية: Cypher، Cypher-X، التشفير، الخوارزميات غير المتماثلة، الخوارزميات المتماثلة، Vigenère .