 e-ISSN No. 2584-1025

Guardian Cipher Multiple Encryption with Asymmetric Keys

Name: Aditya Sangle, Aditi Bhattacharya, Aditya Pate, Utkarsha Undre, Prof. Pooja Oza

Affiliation: CSE Department, MIT Art Design and Technology University, Pune

Email id: adityasangle1302@gmail.com, bhattacharyaaditi4all@gmail.com, aadityaspate@gmail.com,utkarshaundre3@gmail.com, pooja.oza@mituniversity.edu.in

Abstract—

The Guardian Cipher is a new method of data protection by encryptions with multiple keys. As more and more sensitive data are stored in a digital world, more attention is devoted to prevent data leaking and attacks. This research paper outlines the design and functioning of the Guardian Cipher. The research paper talks about the design and functioning of the Guardian Cipher. This scheme, in which protections are provided bythe use of multiple asymmetric keys is specially designed to increase resistance. For instance, even if hackers capture one layer ofdata, the underlying data will remain protected behind another layer of security. It is hoped that this novel innovations in data protection will increase the security ofsensitive data.

1. Introduction:-

In today's digital landscape, data privacy demands robust encryption methods. Conventional asymmetric encryption, while effective, may struggle against evolving threats. Our solution introduces a cascading asymmetric multiple encryption system,

ensuring robust protection and interoperability. Leveraging computational advancements, each encryption layer is tailored for enhanced security. Balancing security and efficiency, our system offers swift encryption without compromising confidentiality. Seamlessly integrating with existing protocols, widespread adoption is facilitated. In conclusion, our study represents a significant step in digital security. By merging advanced encryptionwith innovative design, we set new standards, effectively safeguarding assets against evolving cyber threexisting protocols, widespread adoption is facilitated. In conclusion, our study represents a significant step in digital security. By merging advanced encryption with innovative design, we set new standards, effectively safeguarding assets against evolving cyber threats.

.

2. Literature Survey:-

1. *"SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms"* by *Muhammad Aamir Panhwar,* Sijjad Ali *Khuhro, Ghazala Panhwar, & Kamran Ali Memon* provides a comprehensive analysis of both symmetric and asymmetric cryptographic algorithms, which serves as a strong

foundation for the current research project's objectives. This analysis provides valuable insights into the cryptographic landscape, serving as a foundation for our current research project. The paper demonstrates the significance of understanding cryptographic algorithms in the context of secure data communication and highlightsthe importance of leveraging this knowledge forthe design and implementation of robust encryption systems.

2. *"Study on Symmetric and Asymmetric Key Encryption Algorithms"* by *S. Suguna, Dr. V. Dhanakoti, R. Manjupriya* reflects the ongoing efforts to strike a balance between performance andsecurityin various use cases. The choice between symmetric and asymmetric encryption depends on the specific requirements of the application, andhybrid approaches are emerging as a promising solution to meet these diverse needs.

3. *"An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms"* by *Shahzadi Farah, M. Younas Javed, Azra Shamim, and Tabassam Nawaz* investigates the performance of asymmetric encryption algorithms. The research reviews and compares various algorithms, such as

RSA, Elgamal, and ECC, assessing their efficiency and effectiveness in terms of encryption and decryption speeds. By evaluating these algorithms, the paper aims to provide insights into their practical applicability in securing digital communications, serving as a valuable resource for both researchers and practitioners seeking to make informed choices in selecting the most suitable asymmetric encryption algorithm for their specific use cases.

4. The research paper *"Analysis of asymmetric cryptography in information security based on computational study to*

ensure confidentiality during information exchange" by *Abdul Ghaffar Khan, Sana Basharat, and Muhammad Usama Riaz* explores the application of asymmetric cryptography in information security, focusing on ensuring confidentiality during data exchange. The authors likely reviewed existing literature on the topic, investigating the role of asymmetric cryptography in safeguarding sensitive information. This study aims to contribute to the understanding of how computational methods can enhance the security of data exchange, addressing the critical need for confidentiality in the ever-evolving field ofinformation security.

5. The research paper *"Asymmetric New Cryptography Algorithm Based on ASCII Code"* by*Yaser M.A. Abualkas and Arshed Raad Raheem* says that Symmetric-key cryptography is based onpersonal secrecy in this paper presented a new Asymmetric cryptography algorithm based on ASSCI code. The proposed algorithm can be usedto encrypt and decrypt text messages based on the ASCII code of characters in most sensitive data and critical position like bankaccount details, messages etc. The main idea of the proposed algorithm is to ensure higher security and to hide data in effective way.

3. Guardian Cipher

3.1 Benefits:-

1. **Enhanced Data Security:** By utilizing severallevels of encryption to safeguard sensitive data from unauthorized accessand cyberattacks, the cascading asymmetric multiple encryption methodmaximizes protection while maintaining the integrity and confidentiality of sensitive data.

2. **Comprehensive Solution:** The encryption scheme provides a comprehensive solution for datasecurity in a variety of applications and environments by addressing important issues including key management, performanceoptimization, and compatibility.

3. **Resilience Against Cyber Threats:** By protecting sensitive data and vital assets for enterprises, the strong defense mechanism offered by the encryption system helps to foster resilience against ever-evolving cyber threats.

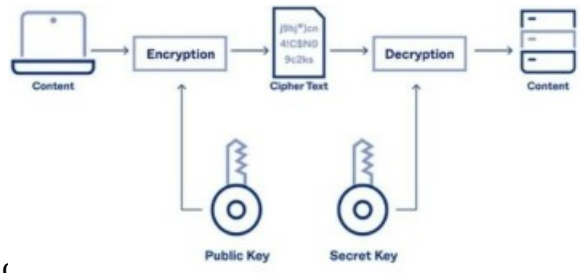
4. **Trust in Digital Transactions:** The project increases user confidence and reduces the risk of data breaches and unauthorized access by fortifyingdata protection mechanisms. This fosters trust in digital transactions and communications.

3.2 Methodology:-

1.2. Methodology

To implement a secure multiple encryption system using asymmetric key algorithms, start by generating multiple pairs of public and private keys for different asymmetric algorithms. Divide the sensitive data into smaller blocks for parallel processing. Encrypt each data block with a different

public key in a cascading manner, with the output ofone encryption becoming the input of the next. Develop a robust key management system to securely store and retrieve private keys while ensuring proper access control. Optimize the encryption and decryption processes to ensure efficiency



and
various platforms and devices. Rigorously test the system's security and performance, documenting the design, implementation, and key management procedures. Deploy the system in a secure environment and continuously monitor and update it, ensuring compliance with relevant data protection regulations. Train users on the system's proper usage and key management practices and periodically conduct security audits and penetration testing to maintain its integrity. This comprehensive methodology ensures the creation of a robust, efficient, and compatible multiple encryption system that effectively addresses key management and performance challenges.

The most basic and important points required are explained hereby like Asymmetric Encryption, RSA Algorithm, Key Management, Cascading Encryption.

1.2.1. Asymmetric Encryption

Asymmetric encryption (*aka* asymmetric cryptography) allows users to encrypt information using shared keys.

Asymmetric encryption provides a highlysecure method for transmitting messages over the internet,
ensuring that only the intended recipient can accessthe content.

Security in an asymmetric encryption environment works with two keys.

- **Public key encryption:** Anyone cansee thisand access it.
- **Private key encryption:**Only the authenticated recipient has access to it.

These two keys are separate but equal, and they're both required to decode a message. Ifyou have onlyone, decryption is impossible.

Symmetric encryption is asymmetric encryption's counterpart. If you use symmetric encryption, one key both encrypts and decrypts data. A hacker with access to that one key can do both functions.

Asymmetric encryption relies on two keys. One encrypts, and the other decodes. The result is a stronger level of security.

3.2.2 Key Management

1.2.2. Key Management

Maintaining the security of encryption systems, especially those that use the RSA method, depends heavily on key management. It includes the creation, storing, distributing, and maintaining of cryptographic keys across their whole lifecycle. Establishing safe pathways for key distribution, storing private keys to avoid

 e-ISSN No. 2584-1025

unwanted access, and securely generating RSA key pairs are all necessaryfor effective key management. In order to mitigate potential vulnerabilities, key rotation procedures arealso used to update keys on a regular basis. To ensure the safe and long-lasting operation of RSA-based encryption systems, access limits and key revocation procedures are set up for compromised keys.

1.2.3. RSAAlgorithm

The RSA (Rivest-Shamir-Adleman) algorithm stands as a cornerstone in the realm of information security, serving dual roles in authentication and confidentiality. Its asymmetric encryption model, based on the mathematical complexity of factoring large numbers, offers a secure method for verifying the identities of communication participants and safeguarding the privacy of data transmitted over open networks. RSA's authentication capabilities rely on the principle of digital signatures, which allow recipients to validate the origin and integrity of messages, while its confidentiality attributes ensure that sensitive information remains encrypted and confidential during transit. This research paper delves into the multifaceted applications of the RSA algorithm, exploring its strengths and potential vulnerabilities in the pursuit of robust authenticationand data confidentiality in the digital age.

1.2.4. Digital Signatures

When it comes to confirming the integrity and authenticity of digital documents or messages, digital signatures are essential. Every item of data is given a unique digital signature created using a private key; the signature is verified using a matching public key. Digital signatures are necessary for safe online transactions and the prevention of fraud and data tampering since they guarantee data validity, non-repudiation, and integrity.

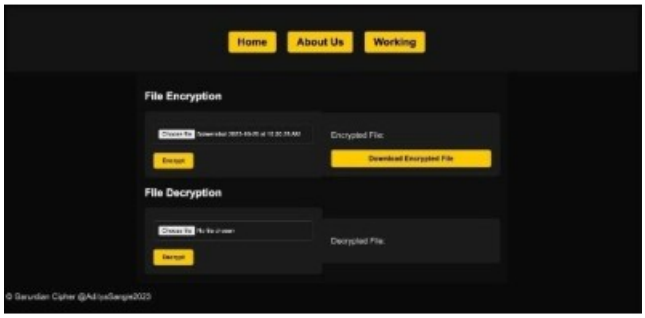
3.5 Implementation Pictures:-

IMG-1- Homepage

IMG-2- Encryption

 e-ISSN No. 2584-1025

IMG-3- Decryption



Future Scope:-

Advanced Key Management: For any encryption system, but particularly for one as complex as Guardian Cipher, strong key management is essential. Effective and safe key management is crucial as the system grows and processes more data. It will be crucial to use strategies like safe key storage methods, key rotation procedures, and hierarchical key management.

Post-Quantum Cryptography (PQC) Readiness: Guardian Cipher's long-term viability depends on its ability to anticipate the threat scenario going forward. Current encryption techniques are vulnerable to compromise as quantum computing advances. Anticipating this change and putting PQC algorithms into practice will show how committed the project is to long- term security.

Performance Optimization: In encryption systems, striking a balance between security and speed is a constant issue. On the other hand, several encryption levels improvesecurity.

User-Friendliness: A major factor in Guardian Cipher's broad acceptance is making sure it continues to be usable by users with different levels of technical expertise. Offering user-friendly interfaces, unambiguous documentation, and smooth interaction with current workflows will improve the user experience and promote adoption among various user demographics and sectors.

Standardization: Complying with accepted encryption standards guarantees Guardian Cipher's security and promotes interoperability. Adopting the project more easily by security-conscious enterprises can be facilitated by adhering to industry-recognized standards and putting it through rigorous third-party audits.

Threat Analysis and Compliance: Guardian Cipher's efficacy and compliance depend on ongoing observation of new cyberthreats and changes in legal requirements.

Acknowledgement

We like to expand our ardent appreciation to everybody who helped us finish this project on cascading asymmetric multiple encryptions successfully.

We owe a huge debt of gratitude to our associates and partners for their commitment, diligence, and collaboration,all of which were essential to the creation and execution of the encryption system. Theproject outcomes were significantly enhanced by their combined effort and knowledge.

In addition, we thank MIT-ADT University

for its resources and support, which made this project go more smoothly.

Not to mention, we would want to thank our family and friends for their steadfast understanding, support, and encouragement during this attempt.

Aditya Sangle

Aditya Pate

Utkarsha Undre

Aditi Bhattacharya

Prof. Pooja Oza

This project could not have happened without the combined efforts and assistance of everyone listed above. We sincerely appreciate everyone's contributions anddedication.

Conclusion:-

In conclusion, our study project presents a comprehensive approach to enhancing sensitive information security in the digital age, primarily focusing on the RSA method and developing a multiple encryption system. We carefully selected encryption algorithms, considered data segmentation, cascade encryption, and key management to bolster security. Our project emphasizes secure cryptographic key handling, effectivedecryption procedures, integrity protection, and metadata management. We optimized encryption processes to maintain operational ef ficiency without compromising security, ensuring compatibility with existing systems for seamless integration. Continuous monitoring, training,

and documentation foster a culture of improvement and threat adaptation. Rigorous security testing guarantees system dependability and resilience against potential threats. Ultimately, our research aims to deliver a robust encryption system that addresses various

aspects of the interconnected digital landscape, bolstering data security effectively.

References:-

1. SACA: A Study of Symmetric and AsymmetricCryptographic Algorithms – Muhammad Aamir Panhwar, Sijjad Ali Khuhro, Ghazala Panhwar, Kamran Ali Memon

2. Study on Symmetric and Asymmetric Key Encryption Algorithms - S. Suguna, Dr. V. Dhanakoti, R. Manjupriya

3. An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms -https:// www.researchgate.net/publication/ 275338264

4. Analysis of asymmetric cryptographyin information security based on computational study to ensure

confidentiality during information exchange. https://www.researchgate.net/publication/328630416

5. Role of Multiple Encryption in Secure Transaction – Himanshu Gupta and Vinod Kumar Sharma .

6. Asymmetric New Cryptography AlgorithmBased on ASCII Code - Yaser M.A. Abualkas and Arshed Raad Raheem

7. Asymmetric Encryption – Okta. https://rb.gy/wok6t

*****