# Pretty Good Privacy on Online Product Shopping

Prof. Kaustubh Shinde[1], Vishwajeet Pawar[2], Kirtesh Patil[3], Utkarsh Raskar[4], Siddharth Patil[5]
*Department of Computer Engineering, Sinhgad Institute of Technology and Science, Narhe, Pune[1,2,3,4,5]*

---------------------------------------------------------------------***---------------------------------------------------------------------

***Abstract -*** This paper surveys the integration of Pretty Good Privacy (PGP) encryption into e-commerce systems, focusing on the use of RSA and AES encryption algorithms. PGP provides a reliable mechanism for securing digital communication and transactions, and its combination of asymmetric (RSA) and symmetric (AES) encryption methods ensures data privacy, integrity, and authenticity. The paper reviews the principles of PGP, examines the encryption techniques involved, and explores their applications in securing online transactions in e-commerce platforms.

***Key Words:*** Pretty Good Privacy (PGP), RSA, AES, Product Authentication, Digital Signatures, Public Key Cryptography, E-commerce Security, Data Integrity, Online Shopping.

## 1. INTRODUCTION

The fast development of online business over the past decade has transformed the global marketplace, making it more accessible and efficient. Internet shopping offers buyers unparalleled convenience, with the ability to browse, compare, and purchase items from anywhere in the world. However, this convenience comes with significant security risks.

As more personal and financial data is exchanged online, the threat of cyberattacks, fraud, and counterfeit products has become an increasing concern. Customers are becoming more cautious about the authenticity of the stores they buy from and the integrity of the products they receive. Similarly, business owners face challenges in ensuring that their identity is not compromised and that the products they offer are not tampered with or counterfeited by malicious actors.

In order to improve security and privacy while shopping for products online, this project proposes the use of Pretty Good Privacy (PGP) as a solution to these issues. PGP is well-known for its ability to facilitate secure communication between parties, utilizing digital signatures and encryption. This solution ensures that both the shopkeeper's identity and product verification are handled with a high level of security by integrating PGP with RSA encryption and AES.

We propose a unique multi-layered encryption technique in response to the shortcomings of single-layered encryption and the evolving security risks in cloud environments. This multi-layered approach creates a robust algorithmic structure: AES (Advanced Encryption Standard): AES effectively encrypts data blocks, transforming them into unbreakable ciphertext, thereby protecting the data from attacks. RSA (Rivest-Shamir-Adleman): By encrypting the AES key itself, RSA provides an additional layer of protection through public-key encryption. Unlike conventional symmetric encryption, RSA uses distinct public and private keys. This ensures that even if the public key is compromised, the private key (used for decryption) remains secure.

## 2. RELATED WORK

Lately, various investigations in view of various cryptographic methods, for example, roll-based encryption, AES calculations, also, RSA calculations — have been distributed. All things considered, no single review endeavors to examine each improvement in RSA, AES, what's more, roll-based encryption in a calculated and exhaustive manner. We have remembered some writing for this area that spotlights on the audit of numerous elective lightweight and awry key cryptography techniques, albeit most of the examinations we cover in this segment are unsystematic audits.

The RSA conspire, a mainstay of topsy-turvy cryptography, goes through steady examination in research. This paper “Exploration patterns survey on RSA plan of lopsided cryptography techniques," [1] dives into its advancing scene. Zeroing in on the past decade, it uncovers public organizations and remote sensor networks as the top spaces using RSA, trailed by picture encryption. Security rules as the essential worry, with specialists creating strategies like various indivisible numbers and extra keys to brace it. While RSA sparkles in defending touchy information, its strong key size represents a test for asset restricted gadgets. Generally, this survey features the ceaseless improvement of RSA, accentuating its vigorous security while recognizing its limits. Further exploration could dig further into explicit strategy adequacy and investigate future headings for this significant cryptographic instrument.

[2] Since electronic correspondence makes it conceivable to communicate data rapidly over significant stretches, it has become fundamental to present day culture. Nonetheless, in light of the fact that it gives unapproved individuals admittance to private data, this accommodation additionally accompanies security risks. The RSA (Rivest-ShamirAdleman) calculation has turned into a famous cryptographic method to diminish these risks. To ensure message privacy, it encodes information prior to sending it and unscrambles it when it is gotten. Indeed, even with the overflow of safety efforts accessible, it is consistently important to work on current strategies. Sending information or interchanges safely is the fundamental objective of cryptography, keeping an aggressor from understanding the substance or in any event, recognizing the presence of a mystery message. In any case, capable individuals can in any

case unravel the message's unique importance utilizing an assortment of encryption strategies.

[3] A well-known cryptographic method that makes computerized marks and safe correspondence conceivable is public key cryptography, or PKC. RSA, one of the most notable PKC strategies, relies upon the computationally troublesome course of factorizing enormous whole numbers. The strategy habitually utilizes a great deal of energy and time. Analysts from everywhere the world are endeavoring to think of ways to accelerate RSA estimations and utilize less power without forfeiting security. The utilization of equal programming shows guarantees in working on the presentation of RSA. This study analyzes a few simultaneous RSA executions on different equipment and programming stages.

[4] We present another verification method for the quantum three-pass convention (QTPP) that utilizes the Slope figure calculation. This strategy involves applying the conventional Slope figure calculation to both encode and unravel plaintext. After then, at that point, the encoded message is communicated to quantum states, which utilize photons as qubits. Prior to being sent, the polarization of each photon is pivoted by a point Tj not entirely settled indiscriminately. For encryption, the source and beneficiary settle on a Slope figure key. The QTPP is utilized for encryption and the clarification of the decoding technique follows. To represent the working of the calculation, a model is given. Finally, an intensive security assessment of this strategy is displayed.

[5] In the system of the Slope Code calculation, this study presents an original technique for making self-invertible grids. Generally, unscrambling has been incomprehensible on the grounds that the converse of the network used to scramble plaintext could not necessarily exist in all cases. Regardless, the encryption network is self-invertible while utilizing the self-invertible framework creation approach. This soothes out the decoding technique and brings down processing intricacy by getting rid of the need to decide the grid's backwards.

[6] In the advanced age, the requirement for secure picture transmission is principal. Nonetheless, the generally utilized Slope figure calculation, while effective, is scrutinized for its security weakness because of the requirement for sharing a confidential key. To address this, a clever method, Elliptic Bend Cryptosystem with Slope Code (ECCHC), is proposed, planning to make the Slope figure safer and productive by changing it into a hilter kilter encryption strategy. This approach utilizes a self-invertible key network, eliminating the requirement for figuring the reverse key lattice during unscrambling. The review assesses the grayscale picture encryption proficiency utilizing measurements like Entropy, PSNR, and UACI, offering a far-reaching evaluation of the proposed method's presentation.

[7] Battling cybercrime is a main pressing issue in the field of network safety. To diminish this peril, various techniques are being researched, for example, the utilization of watermarking, steganography, and cryptography. The mix of steganography with cryptography is another area of information security that spotlights on further developing information honesty. One area of extraordinary consideration is the mix of the Slope figure procedure and Morse code, which is a correspondence code that Scouts have generally utilized. This original methodology means to improve and modernize information trustworthiness support. The production of new calculations designated at upgrading information security, particularly concerning pictures, is the normal consequence of this blend of procedures.

## 3. SYSTEM ARCHITECTURE

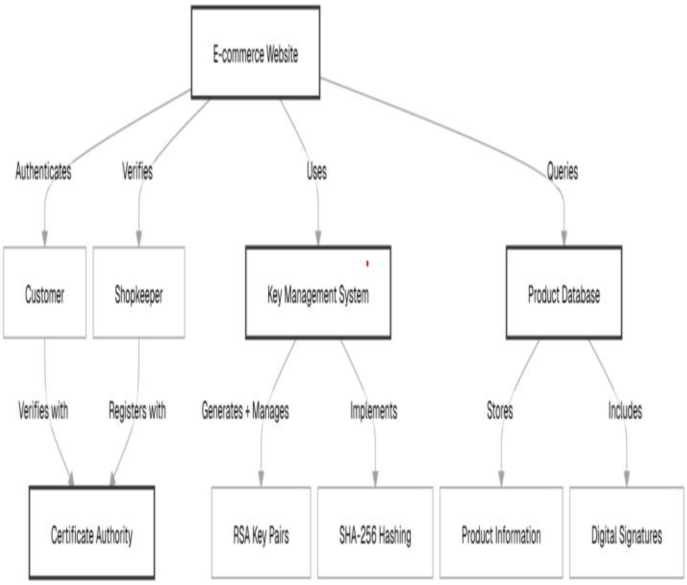

Fig: - System Architecture.

1. Shopkeeper Side:

    - Shopkeeper Registration: Shopkeepers register in the system, generating their RSA key pair.

    - Product Registration: Shopkeepers register their products, creating a unique identifier and product details.

2. System Components:

    - Key Management System: Manages RSA key pairs for shopkeepers and the system.

- Authentication Server: Verifies the identity of shopkeepers and customers.
- Product Database: Stores product information, including hashes and digital signatures.

3. Customer Side: Product Verification: Customers can verify the authenticity of products they intend to purchase.
4. Cryptographic Operations: RSA Encryption /Decryption: Used for secure communication between parties.

## 4. CONCLUSION

This survey paper provides an in-depth review of PGP's use in e-commerce systems, particularly focusing on RSA and AES encryption methods. It highlights how these encryption techniques can ensure secure transactions, protect sensitive data, and offer privacy, authentication, and data integrity in the digital marketplace. Reiterate the importance of using RSA and AES in securing ecommerce transactions through PGP. The ongoing need for innovation in encryption technologies to stay ahead of evolving cyber threats in the e-commerce space.

## 5. REFERENCES

[1] M. S. A. Mohamad, R. Din, and J. I. Ahmad, ‘‘Research trends review on RSA scheme of asymmetric cryptography techniques,’’ Bull. Electr. Eng. Informat., vol. 10, no. 1, pp. 487–492, Feb. 2021, doi: 10.11591/eei.v10i1.2493.

[2] C. Vyas and J. Dangra, ‘‘A review of modern cryptography techniques with special emphasis on RSA,’’ Int. J. Technol. Res. Manage., vol. 4, pp. 2348–9006, Jul. 2017, Accessed: Aug. 12, 2021. [Online]. Available: http://cs.unc.edu/~fabian/course_papers/diffie.hellman.pdf

[3] S. Saxena and B. Kapoor, ‘‘State of the art parallel approaches for RSA public key based cryptosystem,’’ Int. J. Comput. Sci. Appl., vol. 5, no. 1, pp. 81–88, Feb. 2015, doi: 10.5121/ijcsa.2015.5108.

[4] Abdullah, A. A., Khalaf, R., & Riza, M. (2015). A Realizable Quantum Three-Pass Protocol Authentication Based on Hill Cipher Algorithm. Mathematical Problems in Engineering, 2015. https://doi.org/10.1155/2015/481824.

[5] Acharya, B., Rath, G. S., Patra, S. K., & Panigrahy, S. K. (2007). Novel Methods of Generating SelfInvertible Matrix for Hill Cipher Algorithm. International Journal of Security, 1(1), 14–21.

[6] Dawahdeh, Z. E., Yaakob, S. N., & Razif bin Othman, R. (2018). A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher. Journal of King Saud University - Computer and Information Sciences, 30(3), 349–355. https://doi.org/10.1016/j.jksuci.2017.06.004.

[7] Nofriansyah, D., Defit, S., Nurcahyo, G. W., Ganefri, G., Ridwan, R., Ahmar, A. S., & Rahim, R. (2018). A New Image Encryption Technique Combining Hill Cipher Method, Morse Code and Least Significant Bit Algorithm. Journal of Physics: Conference Series, 954(1). https://doi.org/10.1088/1742-6596/954/1/012003.