



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

A Comprehensive Comparative Analysis of RSA-Based Cryptographic Security and Modern Authentication Techniques For Secure Question Paper Management

Mohiyuddin Khan¹, Ankur Khare^{2*} and Ashoka S.B³

¹Research Scholar, Department of Computer Science and Information Technology Rabindranath Tagore University, Raipur - 464993, Madhya Pradesh, India

²Assistant Professor, Department of Computer Science & Information Technology, Rabindranath Tagore University, Raipur - 464993, Madhya Pradesh, India

³Professor, Department of Computer Science, Maharani Cluster University, Bengaluru - 560001, Karnataka, India

*Corresponding Author: Email ID: khareankur94@gmail.com

Abstract

The RSA algorithm is a widely used public-key cryptographic technique designed to ensure secure data transmission and authentication. Among the main strategies for ensuring information security is the application of cryptographic techniques. It must guarantee the confidentiality of the information in addition to offering digital signatures, authentication, secret sub-storage system security, and other features. Consequently, the encryption and decryption solution can guarantee the information's confidentiality, integrity, and certainty, preventing tampering, forgery, and counterfeiting. By guaranteeing that the content is private and unchangeable throughout transmission, the RSA algorithm is essential to improving the security of digital exam papers. Each question or the entire question paper is encrypted in this method, rendering it unintelligible to unauthorized users. Sensitive exam material is safeguarded against leaks and unauthorized access by limiting decryption and printing of the questions to approved individuals with access to the private key. This technique offered a dependable means of safeguarding and printing the question paper while preserving integrity and confidentiality by combining RSA with controlled decryption and secure storage.

Keywords: Cryptographic, Encryption, Decryption, RSA algorithm, Question paper, Digital.

1. INTRODUCTION

In the digital era, data security has grown to be a serious issue for individuals, businesses, and organizations worldwide. Large volumes of sensitive data are stored and transferred electronically on a daily basis, including financial records, personal information, private business reports, academic question papers, and government files. It is now more important than ever to protect this data because of the increase in cyberthreats like ransomware, phishing, hacking, and unauthorized data breaches. [12] [16]. In order to guarantee the security, confidentiality, and integrity of such data, file encryption and decryption are essential. The encryption is the process of converting readable data, known as plaintext, into an encoded format called ciphertext. This transformation is achieved using the complex cryptographic algorithm and an encryption key [17]. The primary purpose of encryption is to prevent unauthorized access, ensuring that the ciphertext can only be reversed back to the original data by authorized users who possess the appropriate decryption key in its original readable format.

Decryption is the reverse of encryption, where the encrypted data is converted back to the original using a predefined key and algorithm [15] [14]. Together, these processes form the backbone of secured data transmission and storage. [7]

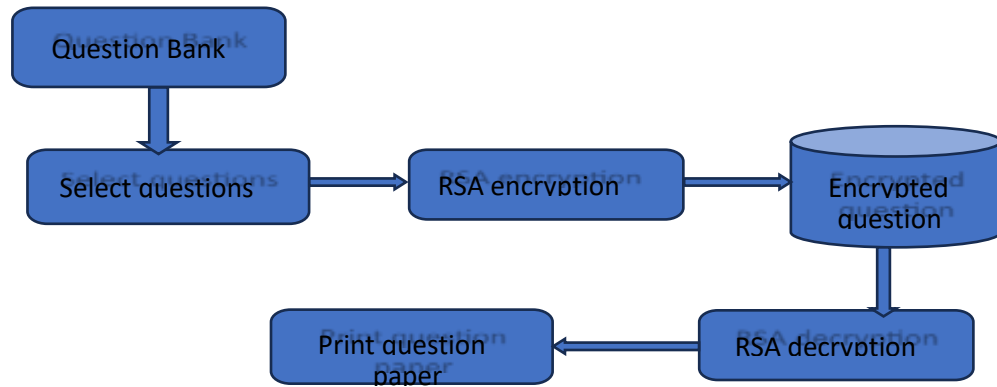


Fig 1. Architecture of Question Paper Protection using RSA

Moreover, the applications of RSA encryption in this context demonstrate the versatility and adaptability of cryptographic techniques to address specific security challenges across different sectors. The encryption and decryption process built into RSA offers a comprehensive solution for preserving information integrity and preventing unauthorized tampering, forgery, or counterfeiting as educational institutions increasingly use digital platforms for assessment and evaluation. The RSA algorithm provides a sophisticated method of improving security in the context of digital question papers. Figure 2 depicts the paper security flowchart. This technique effectively lowers the possibility of information leaks or unapproved entry by encrypting entire question papers, making the content unreadable to unauthorized users. The private key is utilized to decrypt the exam papers, guaranteeing that the receiver alone is able to view and print them. By reducing the possibility of question paper leaks or unauthorized access, this approach not only speeds up the examination procedure but also improves the overall credibility and fairness of assessments. It also offers the highest level of security and confidentiality.

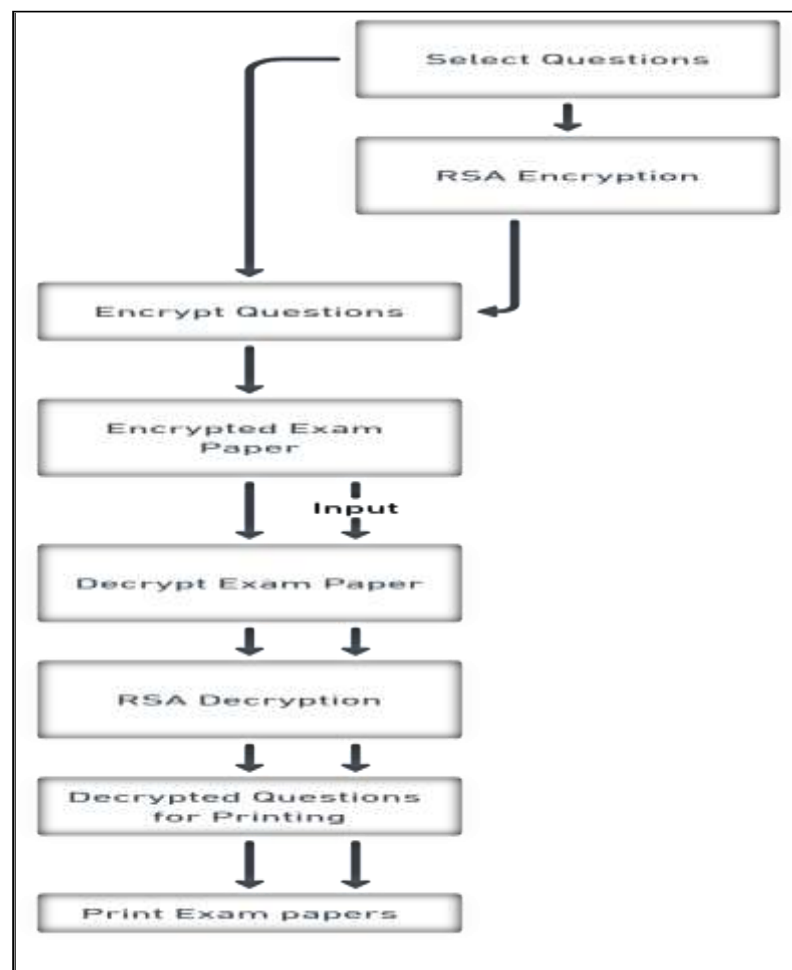


Fig2. Encryption and Decryption Flow for Exam Paper Security

The use of RSA encryption for a digital question paper also aligns with broader trends in cybersecurity and data protection. Furthermore, the implementation of RSA encryption in an educational context serves as a model for other sectors dealing with sensitive digital content. The principles of methodologies employed in securing digital question papers can be adapted and applied to various scenarios where information integrity and secrecy are paramount. This cross-sector applicability underscores the fundamental importance of robust cryptographic technique in a digital age.

II. LITERATURE SURVEY

The authors Murphy, S., et al., Describes the public key cryptographic and its role in establishing secure communications with an untrusted party. It effectively differentiates between the public key and symmetric cryptosystems and explains how protocols such as Diffie-Hellman and QKD are used to set up a symmetric key. The introduction of core public key primitive's public-key encryption and digital signatures is appropriate and well supported with an example like RSA. It also briefly touches upon the importance of security proofs for such primitives and emphasizes the need for entity authentication through the use of certificates. [2]

Al-Ghonmein et al. analyze the issues surrounding online examination systems in the post-COVID educational environment. It highlights the necessity of incorporating stronger protection mechanisms to promote broader adoption and clearly identifies the primary security challenges, such as fraud, hacking, cheating, and leaks. Additionally, the results clearly show how inadequate the current protections are and support the need for improvement. The suggested framework is suitably presented as a way to improve the confidentiality, integrity, and dependability of an online test. It includes encryption and biometric authentication. [3].

Li, W., Susilo et al. explain the advantages and difficulties of cloud computing with a special emphasis on data security and integrity. It successfully highlights the possibility of unintentional data loss and the difficulties users encounter when attempting to confirm whether their encrypted data and its replicas are securely stored across cloud servers. PVPKEET, the suggested solution, is clearly described as a method that permits public verification of encrypted data copies without the need for decryption, preserving confidentiality while guaranteeing integrity. This schema's practical applicability is increased by its capacity to withstand chosen-plaintext attacks and produce verifiable proof. [4]

Halder, B et al., explains the significance of authorization and authentication methods for safe online transactions in a variety of industries, including banking security and hospitality. It accurately identifies the shortcomings of conventional single-user authorization and emphasizes the necessity of more secure multi-user authorization methods in a multi-party setting. In order to improve the authorization process security and dependability, a resolution based on the arithmetic greatest common divisor is presented. further strengthened data protection by introducing a modified N-Prime RSA algorithm for encryption and decryption. The suggested methods' practical applications in the hospitality sector contribute to illuminating their applicability in the real world. [5]

Salah, Omar et al, explains the security of data storage because networks and Internet of Things devices produce a lot of data. It effectively highlights the drawbacks of both asymmetric and symmetric cryptography when applied separately emphasizing that private key methods are not as suitable for an authorization. Public key techniques however are slower but more secure. The hybrid MRSADH technique which combines Diffie-Hellman and RSA with an XOR operation to achieve both high security and faster execution is a well-presented solution. Additionally, describe how the method uses both symmetric and asymmetric encryption to lower computational complexity and boost efficiency. [6]

Goon, S., and Dihidar effectively highlight the challenges faced during the COVID-19 pandemic regarding the secure distribution of university question papers. It made it very clear that while online distribution is a useful substitute for in-person delivery, there are significant security risks connected to it, including the possibility of interception and manipulation by hackers. The study suggests using K-out-of-N visual cryptography in conjunction with AES password protection to reduce these risks. Two layers of security are added by first encrypting the original question papers using AES and then creating visual cryptographic shares. In order to improve confidentiality and prevent unauthorized access, the examination center requires multiple stakeholders to combine the shares and enter the password. This ensures that no single individual can access the content. [7]

Singhal, Vikas, et al. explain the necessity of data security in light of the Internet's explosive growth in information transfer. It correctly presents steganography and cryptography as the two main methods of data protection and describes their functions. It is possible to characterize the suggested model as a dual-

layer security strategy that improves confidentiality and resilience against attacks by combining AES for encryption and LSB for data hiding. by highlighting the thorough examination of various encryption methods and describing the benefits of combining both algorithms. [8]

In this paper, the authors Abid, R., Iwendi, C., et al. explain why cryptographic methods are essential for protecting data during transmission and storage and emphasize the significance of secure information exchange in today's digital networks. It identifies the limitations of traditional homomorphic encryption methods, specifically their slow transmission and decryption speed, and introduces the HE-CRT-RSA algorithm as an optimized solution that combines homomorphic encryption with the RSA and the Chinese Remainder Theorem. By employing multiple keys, the suggested method improves security and shows improved performance with a 3–4 percent decrease in decryption time when compared to the traditional RSA. [9]

Imam, R., et al., explains in detail why RSA is frequently utilized in a variety of fields, including cloud security and image protection, and emphasizes that in spite of its widespread use, there hasn't been a thorough analysis of RSA-based strategies. and emphasizes the growing need to safeguard the massive amounts of digital data from ever-more-advanced attacks as well as the significance of RSA in the larger framework of public-key cryptography. [10]

Ganavi, M., et al., highlights the growing need for strong security measures to safeguard multimedia data in the current digital environment. Confidentiality, authenticity, integrity, and non-reproduction are accurately identified as essential security requirements. It also highlights the growing danger of malicious attacks like phishing. In order to enhance data security, the paragraph presents steganography and cryptography as complementary methods. It clarifies that RSA requires optimization because despite being secure, it can be computationally demanding. The suggested method, which encrypts secret text using a modified RSA algorithm and embeds it in an image using a random pixel replacement technique, is thoroughly explained, demonstrating how effective it is at preventing unwanted access. [11]

III. ENCRYPTION AND DECRYPTION METHODS IN CRYPTOGRAPHY

Three primary processes make up the exam preparation workflow. First, the system automatically creates a set of questions that are unique and fair to each paper by eliminating repetition and duplication. Second, the generated question paper is encrypted to convert it into an unreadable format, which protects it from unauthorized access or leakage before printing. Third, after decryption and printing, the sealed question paper boxes are transported to the examination centers using a secure delivery mechanism to maintain confidentiality and integrity throughout the distribution process [1]. This paper employs RSA public-key cryptography, which is used to secure the selected questions through an encryption and decryption process to provide confidentiality and protection against unauthorized access or leakage before printing.

A. Cryptography

The study of cryptography deals with protecting data and communicating against unauthorized access or transforming data into an unintelligible format during transmission with the right key. Providing security, integrity, authenticity, and non-repudiation for both digital and physical communication is an essential objective. Since financial transactions, intellectual property, and information are being transmitted over unprotected networks like the Internet, cryptography is used extensively in a modern society as a defense against malevolence and cyberthreats.

The two basic techniques of encryption and decryption are the foundation of cryptography.

- The process of encryption uses cryptographic keys and the mathematical method to transform readable plaintext into unintelligible text.
- Decryption is the opposite procedure, which uses the matching decryption key to convert the returning ciphertext to the original plaintext.

Key concept in cryptography

The key generation encryption and decryption process—it is critical to comprehend the basic components:

- Plaintext: The original readable data or message.
- Ciphertext: The encryption forms the plaintext, which appears meaningless without the proper decryption key.
- Key: A parameter that determines the output of a cryptographic algorithm.
- Encryption algorithm: A mathematical operation that converts plaintext into ciphertext.
- Decryption algorithm: A mathematical function that reverses the encryption, retrieving plaintext from the ciphertext.

B. Encryption Process

Encryption is our secure question paper system that uses RSA to transform the original readable content into an unreadable format, thereby protecting it from unauthorized access during storage. Initially, the

question paper, which is in plain text, is converted into a numerical format suitable for mathematical operations. This numerical representation is then encrypted using the public key, which is part of the asymmetric cryptography key pair. Use the mathematical operation: it produces a ciphertext, which appears as a seemingly random string of characters and cannot be read or understood without the corresponding private key. Because the public key is openly shared, anyone can encrypt the question paper, but no one can decrypt it without the private key, which is securely held by the authorized printing system. This ensures that while the question paper is stored before printing, it remains confidential and tamper-proof. Only at the printing stage is the ciphertext decrypted to return to its original readable form using the private key, allowing the question paper to be printed securely. This method protects the integrity and secrecy of the exam content throughout the process.

RSA Encryption Algorithm

The algorithm for the RSA encryption process used in our secure question paper system:

- **Input:**
 - Plaintext message M (the question paper content).
 - Public key (n, e) , where n is the modulus and e is the public exponent.
- **Convert Message:** Convert the plaintext message M into an integer representation m such that $0 \leq m < n$.
- **Encrypt Message:** Compute the ciphertext c using the formula:
$$c = m^e \bmod n$$
- **Output:** The ciphertext c , representing the encrypted question paper.
- **Store:** store the encrypted ciphertext c securely until it reaches the authorized printing system for decryption.

C. Decryption Process

The decryption process in your secure question paper system using RSA is a reverse of encryption and is designed to convert the unreadable returning ciphertext to its original, legible state. During the decryption, the mathematical operation effectively reverses the encryption step, revealing the original numerical representation of the question paper. This number is then converted back into the readable text format of the question paper. The content remains secure and confidential until the point of printing. This process guarantees that the question paper data is protected from interception or tampering while encrypted, and it's only made intelligible at the intended secure endpoint, preserving the secrecy and integrity necessary to uphold exam security.

RSA Decryption Algorithm

The algorithm for the RSA decryption process used in our secure question paper system:

- **Input:**
 - Ciphertext c (the encrypted question paper).
 - Private key (n, d) , where n is the modulus and d is the private exponent.
- **Decrypt Ciphertext:** Compute the original message m using the formula:
$$m = c^d \bmod n$$
- **Convert to Plaintext:** Convert the integer m back into the readable plaintext message M (the original question paper content).
- **Output:** The decrypted plaintext message M .
- **Print:** Use the decrypted question paper for secure printing.

IV. Comparative Study

A. Comparative study of Question Paper Generation Approaches

The complementary aspects of the modern examination system are automated question paper generation, secure encryption of question papers, and an IoT-based secure delivery mechanism. Taken together, they reflect a shift from conventional manual processes to intelligent, technology-enabled frameworks that prioritize efficiency, security, and trust. The creation phase of the examination process substitutes an automated data-driven approach for the conventional manual question paper preparation, which is frequently laborious and subject to human bias. While the generation process becomes quicker and more scalable, the randomization technique and duplication checks support equity across several paper versions. Additionally, the method allows for quantitative performance monitoring (time randomness quality and repetition rates), something that is not achievable with a traditional method.

A brief comparison of the suggested approach and the conventional approach to question paper preparation is presented in the table below.

Aspect	Traditional Method	Proposed Method
Selection of Questions	Questions are manually selected, often subjectively by instructors or exam committees. May lead to repetition or bias.	Randomized selection of unique questions ensuring variety and avoiding duplicates.
Organization of questions	Typically organized manually into sections or parts based on the topic or difficulty.	Automatically split into parts with an equal number of questions.
Checking for duplicates	Relies on manual proofreading or peer review to avoid similar/repeated questions.	Uses Sequence Matcher to algorithmically detect highly similar questions across all parts.
Generating versions/series	Different versions may be made by manual rearrangement of questions or printing multiple papers.	Generates series by rotating question parts programmatically, creating distinct questions easily.
Time and effort	labour-intensive, time-consuming, and subject to bias and human error.	Effective automated organization and selection with controlled verification and randomness.
Scalability	Large question banks or several exam sets are challenging to scale effectively.	Large cushion banks and the creation of numerous paper versions make it easily scalable.

B. Comparative study between Traditional Paper Security vs. Cryptographic Method (RSA Encryption and Decryption):

RSA encryption is used to safeguard the question paper's integrity and secrecy after it has been created and stored. This approach, which prioritizes efficiency, focuses on data security. The conventional approach primarily relies on manual supervision and physical security, which is prone to human error, potential leaks, and inefficiencies. Cryptographic techniques are used in our papers' suggested RSA encryption/decryption system to guarantee digital confidentiality, integrity, and controlled access. It lowers the possibility of unwanted access by using public keys to encrypt questions and private keys to decrypt them.

The table below shows a simple summary of a comparison between traditional paper security and the cryptography-based RSA method.

Aspect	Traditional Method	Proposed RSA-based Method
Security approach	Frequently uses physical security measures such as sealed envelopes, manual oversight, and trusted personal digital documents, which may have inadequate or no encryption.	Uses strong RSA asymmetric encryption to secure question papers digitally. Only by printing paper can the encrypted questions be decrypted.

Data confidentiality	Vulnerable to leaks if digital copies are intercepted without encryption or if physical security is compromised.	Since encrypted data cannot be read without a private key, confidentiality is guaranteed, preventing unwanted access or transmission interception.
Efficiency and overhead	High labor and time overhead for safe handling and distribution despite low technology.	requires a lot of processing power for key generation, encryption, and decryption; however, it is very safe and scalable.
Risk of unauthorized user	There is a high risk that private information will be disclosed during transmission or physical handling.	Low risk due to encrypted data inaccessible to unauthorized users without the private key
User accessibility	Requires physical presence and manual handling of exam papers	Enable secure remote distribution with encrypted digital materials authorized users can decrypt at printing.

C. Comparative study between biometric authentication and GPS tracking:

The distribution and physical transport phase of the examination system proposes an IOT-based framework integrating GPS location tracking, biometric authentication, and a tamper detection mechanism. This enhances accountability and transparency throughout the delivery process by enabling real-time monitoring and prompt notification of route deviations, unauthorized access attempts, and tampering incidents.

1. The comparative study of GPS tracking between the traditional method during securing question paper transmission.

Due to their inability to track paper bundles or vehicles in real time and their heavy reliance on human oversight during transportation, traditional methods are vulnerable to theft, misrouting, and delayed loss detection. Our recommended method utilizes GPS tracking technology that is integrated into transport vehicles and question paper boxes to continuously track movement and location. When used in conjunction with alert systems and geofencing, it improves security by facilitating prompt anomaly detection and response. Our IoT framework's integration of biometrics and tamper sensors, along with this real-time visibility, offers a complete, reliable solution to more successfully and openly secure question paper transportation. Control and confidence over the security and integrity of exam materials during distribution are greatly increased by this transition from manual supervision to automated real-time GPS tracking. The table below shows a simple summary of the comparison between GPS tracking of the proposed method and the traditional method.

Aspect	Traditional Method	Proposed Method
Tracking capability	A straightforward comparison of the GPS tracking of the suggested method and the conventional method is displayed in the table below.	Question paper boxes and vehicles are continuously tracked via GPS in real time, giving remote access to their current location and movement history.
Security against theft/loss	Dependent on human vigilance; vulnerable to theft, misrouting, or loss due to lack of real-time monitoring.	Immediate detection of route deviation or unauthorized movement triggers an alert for intervention, reducing the risk of theft or loss.
Alert system	frequently reactive depending on postevent discovery.	The proactive alerting system uses geofencing to instantly alert authorities to tampering, route deviation, or unauthorized access attempts.

Transparency and accountability	Manual records are prone to mistakes or manipulation, and there are few transparent records.	In-depth location data and access to event logs facilitate auditing and guarantee accountability while in transit.
Integration with other security measures	primarily sealed boxes without technology integration or independent physical security guards.	combined with tamper detection sensors and biometric access control to create a complete IoT-based security framework.
Data accessibility	Only available through a manual report or at a checkpoint.	Take away the ability for stakeholders to monitor status and get real-time updates through a web or mobile interface.
Response time	Slow response is possible due to delayed awareness of transparent issues.	Faster, real-time responses are enabled due to immediate detection of anomalies.
Scalability	Difficult to scale efficiently with more transport routes or paper batches	Highly scalable to multiple routes and batches with centralized cloudbased data handling
Technological requirements	Low technology; mainly depends on manual supervision and physical security	Requires GPS modules, network connectivity, and cloud infrastructure, which adds complexity but greatly improves security and control.

2. The comparative study of biometric authentication between traditional and proposed IoTbased methods

In order to secure exam materials either physically or digitally, traditional methods mainly rely on what users know or carry (passwords, pins, and IDs), which are vulnerable to theft, loss, and impersonation. For authorization and access control in exam paper handling, particularly during transportation and question box access, our suggested biometric approach incorporates distinct physiological characteristics (such as fingerprints). In addition to improving user convenience and traceability, this significantly increases security by guaranteeing that only verified sensitive information is accessible to authorized persons. Research indicates that biometrics provide significantly higher accuracy and security per cost when compared to traditional knowledge-based methods, making them a better option for securing crucial examination processes. However, biometric implementations necessitate appropriate protection against spoofing and privacy issues. For high-stakes integrity-sensitive settings like exam quotient paper security, biometric security is therefore a potent addition to and improvement over traditional authentication. The table that follows provides a brief overview of the differences between the suggested and conventional methods of biometric authentication.

Aspect	Traditional Method	Proposed Method
Authentication basis	Relies on knowledge-based (passwords, PINs) or possessionbased (ID cards, tokens) authentication.	makes use of biometric features like question paper boxes and fingerprint recognition.
Security strength	Passwords and tokens are susceptible to theft, loss, guessing, and sharing. vulnerable to fraud and breaches.	Biometric authentication uses distinct physical characteristics to increase security and lower the risk of impersonation.
Conveniences	Users are required to carry tokens or remember passwords, which may result in lost or forgotten credentials.	Biometric systems improve user convenience by providing seamless, fast access without the need for passwords.

Implementation cost	Generally inexpensive up front, but there is a chance that breaches and password resets will increase operating costs.	Moderate cost for biometric hardware but offer a better security-per-cost value and less operational overhead.
Risk of unauthorized access	Higher risk due to sharing or theft of credentials.	Lower risk since biometrics are intrinsic and difficult to spoof.
Applicability to exam security	Physical or manual checks can be bypassed or faked; security lapses	Enables biometric-locked physical access (e.g., fingerprint scanner on paper boxes), ensuring only
	are common during paper transport or access.	authorized personnel open boxes at specified times/locations.

V. Conclusion

In conclusion, the integration of RSA encryption within digital question paper generation and distribution offers a highly secure and reliable framework that safeguards examination materials from unauthorized access and tampering. By combining randomization techniques with asymmetric cryptography, the proposed method ensures both unpredictability and data confidentiality across the entire workflow from question selection to distribution and final access. Only authorized personnel possessing the private key can decrypt and print the papers, thereby preserving the integrity and confidentiality of the examination process. This not only strengthens the security of the digital assessment system but also enhances trust and transparency by preventing leaks or fraud during the transportation and storage. As educational institutions continue to adopt digital platforms, the incorporation of robust cryptographic techniques like RSA will continue to be crucial for maintaining the credibility, fairness, and resilience of modern examination systems.

References

- [1]. Khan, N. M. (2025). Next-Gen Exam Paper Protection: IoT Smart Lock with GPS, Biometrics & Anti-Tampering. *Journal of Information Systems Engineering & Management*, 10(42s), 1138–1147. <https://doi.org/10.52783/jisem.v10i42s.8267>.
- [2]. Murphy, S., & Player, R. (2025). Public-key cryptography (pp. 61–76). Oxford University Press Oxford. <https://doi.org/10.1093/actrade/9780192882233.003.0006>.
- [3]. Al-Ghonmein, Ali M., et al. "Enhancing online exam security: encryption and authentication in Jordanian and international universities." *International Journal of Electrical & Computer Engineering* (2088-8708) 15.1 (2025).
- [4]. Li, W., Susilo, W., Xia, C., Huang, L., Guo, F., & Wang, T. (2024). Secure Data Integrity Check Based on Verified Public Key Encryption with Equality Test for Multi-Cloud Storage. *IEEE Transactions on Dependable and Secure Computing*, 21(6), 5359–5373. <https://doi.org/10.1109/tdsc.2024.3375369>.
- [5]. Halder, B., Sinha, R., & Paul, P. (2024). Enhancing the security in group message communication using Multi-Party key distribution technique. *Journal of Mobile Multimedia*, 961–996. <https://doi.org/10.13052/jmm1550-4646.2051>.
- [6]. Salah, Omar, Ahmed El-Sawy, and Mohamed Taha. "A Hybrid Algorithm For Enhancement of the Data Security during Network Transmission Based on RSA and DH." *International Journal of Intelligent Engineering & Systems* 16.3 (2023).
- [7]. Banga, P., Nirottam, N., Singh, S. K., Shubham, N., & Singh, P. (2023). A SECURE FILE ENCRYPTION AND DECRYPTION SYSTEM USING AES FOR TEXT AND IMAGES. *International Journal of Research -GRANTHAALAYAH*, 11(12).
- [8]. Goon, S., Dihidar, S., & Pal, D. (2022). A Novel Approach to Ensure the Security of Question Papers Using Visual Cryptography (pp. 647–653). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-4193-1_63.
- [9]. Singhal, Vikas, Devendra Singh, and S. K. Gupta. "Crypto STEGO techniques to secure data storage using DES, DCT, Blowfish and LSB encryption algorithms." *Journal of Algebraic Statistics* 13.3 (2022): 1162–1171.

- [10]. Abid, R., Iwendi, C., Javed, A. R., Rizwan, M., Jalil, Z., Anajemba, J. H., & Biamba, C. (2021). An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Personal and Ubiquitous Computing*, 27(3), 1405–1418. <https://doi.org/10.1007/s00779-021-01607-3>.
- [11]. Imam, R., Areeb, Q. M., Alturki, A., & Anwer, F. (2021b). Systematic and Critical review of RSA based public key cryptographic schemes: past and present status. *IEEE Access*, 9, 155949–155976. <https://doi.org/10.1109/access.2021.3129224>.
- [12]. Whitfield, D., & Sushil, S. (2020). *Cryptography and Information Security: Introduction to Modern Cryptography*. Springer International Publishing.
- [13]. Shivamurthaiah Mallaiah, Sitesh Kumar Sinha, July 2020. *Image Processing Based Trigger and Dissemination of Exam Paper*. Publisher: LAMBERT Academic Publishing, Latvia, European Union. ISBN: 978-620-2-67773-8.
- [14]. Ganavi, M., & Prabhudeva, S. (2018). A Secure Data Transmission using Modified RSA and Random Pixel Replacement Steganography. 1–7. <https://doi.org/10.1109/icctct.2018.8550848>.
- [15]. Biryukov, A., & Shamir, A. (2003). Cryptanalysis of the Advanced Encryption Standard. *Proceedings of the International Workshop on Selected Areas in Cryptography*, 1-14.
- [16]. NIST. (2001). *Advanced Encryption Standard (AES)*. Federal Information Processing Standards Publication 197. National Institute of Standards and Technology.
- [17]. Perrig, A., Canetti, R., Tygar, J. D., & Song, D. (2000). The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes*, 3(2), 2-6.