Data Security System for a Bank Based On Two Different Asymmetric Algorithms Cryptography

Soumya Gangele

Master Student, Cyber Law and Information Security, National Law Institute University, Bhopal

ABSTRACT

Protecting private financial data within the banking infrastructure has become crucial in the digital age. In order to provide a reliable and effective data security system for banks, this research investigates the combination of RSA along with ECC. To improve data transmission security, simplify key management, and guarantee trustworthy authentication, RSA, recognized for its historical relevance in digital authentication and the exchange of keys, and ECC, with its effectiveness and adaptability for constrained by resources systems, are integrated. By strengthening data integrity, data authentication, and confidentiality in financial institutions, this integrated approach strives to safeguard assets like client account information. This strategy solves the difficulties facing modern banking by fusing RSA's resilience and ECC's effectiveness, and it offers the knowledge required to adjust to changing security requirements. This amalgamated strategy is set to become a pillar of modern era's banking security methods as more research is conducted.

KEYWORDS: RSA, ECC, Data transmission, Key management, Confidentiality

1) INTRODUCTION

In today's scenario of digital occupancy, the maintenance of the monetary information in a secured manner has become the need of the hour within the banking infrastructure. A considerable amount of sensitive data including the account details of the user, financial records and individual identity information is being stored and retained by the banks. However, to strengthen their defenses against the vulnerabilities and threats posed by the various cyber hacktivists, banks must implement complex and multi-layered privacy techniques.

One such approach is the integrated implementation of two hugely used asymmetric cryptographic algorithms: RSA and ECC.

This research study dives into the integrated implementation of RSA and ECC to establish a robust and efficient data security system for a bank. By making the best use of the benefits of these two different asymmetric techniques, the banks can fortify themselves against a pyramid of cyber threats. This integration eases safe and secure data communication, streamlined key management, and dependable authentication techniques, which are all crucial aspects of a modern-day bank's security infrastructure.

Due to the reliability and proficient working of the RSA algorithm, it has been utilized in the domain of digital signatures and secure key exchange for a considerable period. Whereas, an efficient and costeffective alternative has been provided by ECC which proves to be of a better usage for mobile banking systems.

The scenarios incorporating the usage of lower bandwidth transmission, ECC have always proved to be an efficient approach. The amalgamation of these two effective approaches may lead to the discovery of a viable solution, to the modern-day problems faced by the contemporary banking institutions, which can help in overcoming these shortcomings and limitations in a better and efficient manner. Various important aspects of the data security system such as the confidentiality, enhanced data authentication and integrity in the monetary institutions, could be improvised with the integrated amalgamation of RSA and ECC. The expertise which is required to establish an effective data security system, which could protect the assets and maintain the user trust in a banking infrastructure, and which could also adapt to the ever-changing requirements of the contemporary banking institutions, is being provided through this integration of the techniques.

1.1) STATEMENT OF PROBLEM

Lack of robust data security infrastructure in banking institutions due to isolated use of asymmetric cryptographic algorithms

1.2) RESEARCH OBJECTIVES

- To study two different asymmetric algorithms
- To examine the functionality and benefits of these techniques
- To analyze the impact of the integrated usage of such algorithms
- To explore the influence of such integrated usage on the security system of a bank

1.3) HYPOTHESIS

The integration of two different asymmetric cryptographic techniques (RSA and ECC) within a banking data security system can result in a robust defense mechanism compared to the isolated use of either technique

1.4) RESEARCH QUESTIONS

- Which asymmetric cryptographic algorithms are best suited for securing data in a banking institution?
- How can the monetary transactions and sensitive data be secured through the operational functionality of the selected suited cryptographic algorithms?
- What benefits does the integrated use of two different asymmetric cryptographic algorithms offer to a banking institution's digital security system?

1.5) RESEARCH METHODOLOGY

The researcher in this study is applying a doctrinal approach of research. The study of the research aims to understand the working and the benefits of the asymmetric algorithms which are robust enough to operate in a banking scenario. The researcher also delves into the integrated usage of these techniques and what impact they have on the security system of the banking infrastructure. OSCOLA's 4th edition method is used in citation in this research.

1.6) SCOPE AND LIMITATIONS

The scope of this research provides future researchers the idea regarding the working and posed benefits of two different asymmetric techniques namely RSA and ECC. The findings of the researcher will also help in realizing the importance of the implementation of an integrated data security system in a banking institute.

Due to the shortage of time, the researcher will only focus upon the purpose and the advantages of the integrated data security system.

As this is a doctrinal type of a research, the researcher hasn't performed any sort of experiment in quantitative form.

2) RSA AND ECC

2.1) RSA

This encryption method which makes use of the public key, is used to transfer data in a secured manner over internet. As this is a reliable way of secured transmission of confidential information, it is being used in a wide domain.

A code is added to the common message to assure security. Because of the algorithm's foundation in the factorization of huge numbers, it is difficult for third-party organizations to intercept messages.

2.2) WORKING

A private key that is exclusively known to the recipient is employed for decoding in the RSA Authentication Algorithm. Two significant prime numbers are used to create the public key, which is then disclosed. It is virtually impossible to ascertain these prime factors, thus rendering it impractical to decode with no the private key. So, the private[1] key can only be created by the individual who produced the public key.

- To encrypt data, two enormous numbers that are prime, A and B, must be chosen. N = A*B is the product of both numbers.
- Pick a key that is publicly accessible, E, that doesn't have the factors (A-1) as well as (B-1) as factors. The plaintext will be converted into ciphertext using this public key. General key is made public and that anyone can access it.
- Select the private key, D, for decryption following selecting the public key. This private key needs to be (A-1)*(B-1) mod (D*E) equal to 1 compliant. The private key must be kept confidential and must not be disclosed to anyone. The ciphertext is converted back to plaintext using the private key.
- Use the equation: The word cipher = Plaintext module N to encode a message, where unencrypted is the message that you want to convey. The recipient can then use the private key they obtained to decrypt the resultant ciphertext back to simple text using the equation Unencrypted = Ciphertext module N.

2.3) BENEFITS

- The algorithm is an ideal choice for the successful transmission of sensitive information
- Reliable and secure option.

[1] 'What is RSA: How does an RSA Work?' https://www.encryptionconsulting.com/education-center/what-is-rsa/ Accessed on 15 September 2023

- Due to the complex mathematics involved in the design, RSA[2] algorithm is a challenging route to break through.
- Can be implemented efficiently and quickly as the distribution of public key is an uncomplicated process, to consumers.
- RSA ensures the security of data transmission over the internet
- Highly effective method for the secure communication.

2.4) ECC

The encryption and decryption process are limited by a predetermined number of iterations that can be completed.

This limit is determined by the value of the private key, also known as "n." The larger the key used, the higher the maximum value that the equation can reach.

Therefore, the size[3] of the key plays a crucial role in determining the efficiency and effectiveness of the encryption and decryption process.

$$\mathbf{y^2=x^3 + ax + b}$$

2.5) WORKING

When both points P and Q are added together, an additional point called R exists in the universe of elliptic curves. The example below illustrates this procedure, which is called "point addition."

The capacity to "point double"[4] in cryptography is another useful capability. Using a set point P on an elliptical curve, this involves locating a point 2P that fulfills the formula P + P = 2P. This procedure is depicted in the provided diagram.

Up until we get to the "infinity point," denoted by the symbol O, we can keep doubling the points. According to this scenario, the gap between P and 2P gets closer and closer to zero.

Other than for point O, we can multiply and add points on a curve with an elliptic shape without getting an identical instant twice. As a result, it is possible to multiply and divide any spot P on the trajectory endlessly to produce any additional point, including O.

2.6) BENEFITS

- ECC uses less keys[5] in order to accomplish a comparable level of security.
- This is especially crucial in locations with little storage space.
- Mobile applications, low-power gadgets with limited computing power, and cryptocurrency systems like the likes of Ethereum and Bitcoin are just a few of the platforms where ECC is growing in popularity.
- ECC offers equivalent security while consuming reduced processing and battery resources.

[2] 'RSA Encryption: Definition, Architecture, Benefits and Use' (2023) https://www.okta.com/identity-101/rsa-encryption/ Accessed on 15 September 2023

[3] 'Elliptical Curve Cryptography' https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography Accessed on 15 September 2023

[4] https://www.techtarget.com/searchsecurity/definition/elliptical-curve-cryptography Accessed on 15 September 2023

[5] 'Elliptic Curve Cryptography Definition', https://avinetworks.com/glossary/elliptic-curve-cryptography/#:~:text=Elliptic%20Curve%20Cryptography%20(ECC)%20is,and%20encryption%20of%20web%20traffic. Accessed on 15 September 2023

- ECC is a flexible tool
- Applied to a wide range of tasks, such as key exchange and digital signatures.

3) INTEGRATED WORKING

3.1) KEY GENERATION

3.1.1) RSA

A key that is accessible to everyone (n, e) and a key that is confidential (n, d) are produced while creating RSA keys. P and Q, two enormous prime numbers, are selected to accomplish this. Then, combining p and q jointly yields the value of n. The formula (p-1)(q-1) is then used to determine the totient of n. The next step is to choose an exponent for encryption, e. This quantity must be coprime to n, higher than 1, smaller than n, and greater than 1. Calculating the module-based associative reverse of e modulo (n) yields the decryption exponent, d. This implies that, in terms of mathematics, d is equivalent to e(-1) mod n.

3.1.2) ECC

To utilize ECC, one must first select a private key - a random number, and calculate the corresponding public key point on the chosen elliptic curve. This requires deciding on an elliptic curve and its base point (G), an example being y2 = x3 + ax + b. Next, generate a private key (d) as a random integer, ensuring that it satisfies the property of being less than the base point order (G). Finally, utilize Q = d * G to determine the corresponding public key (Q).

3.2) DATA ENCRYPTION

For encrypting data, it is recommended to use both RSA and ECC encryption techniques. To begin, start with ECC encryption by following these steps:

- Extract a numerical value from the plaintext data that represents an intersection on the elliptical curve.
- For determining an indefinite position (C1) on the curve, use the formula C1 = k * G
- Random value (k).
- Calculate C2 = plaintext + k * Q to calculate the ciphertext point (C2).
- Transmit the encrypted information as (C1, C2).
- Use the public key associated with RSA to encrypt C1, C2 using RSA encryption.
- Transmit (C1_rsa, C2_rsa)

3.3) DATA TRANMISSION

Utilize a comparable protocol to enable secure data transmission across a network. By doing this, the data is encrypted twice, adding an additional degree of defense against security risks and breaches. One can feel confident knowing that their confidential data is being delivered privately and with all due caution by using such precautions.

3.4) DATA STORAGE

Use the financial institution's networks or data storage facilities, which are outfitted with cutting-edge security features like twice-encrypted protection. Your precious data is in good hands and shielded from any conceivable dangers or breaches thanks to such strong security features.

3.5) DATA RETRIEVAL

Only individuals with the appropriate authorization must be given access to sensitive information. The two-dimensional data that has been encrypted must be downloaded from its safe storage place in order to get this information. This guarantees that the information is always kept private and secure.

3.6) DATA DECRYPTION

To employ RSA decryption, first decrypt (C1_rsa, C2_rsa) using the private key of the RSA encryption algorithm (n_rsa, d_rsa). You can achieve this by:

- First calculating C1, which is simply C1_rsa mod n_rsa, followed by calculating C2, which is C2_rsa mod n_rsa.
- Once you have done this, you can move on to using ECC decryption.
- When using this method, it is important to know how to calculate the plaintext point.
- To do this, you can use the equation Plaintext = C2 d* C1.

3.7) DATA PROCESSING

After the data has been successfully decrypted, it is crucial to move forward with the banking operations. This could entail more processing, such as data validation and verification in compliance with accepted protocol. The security and accuracy of the information provided throughout the banking procedure must be ensured by taking all essential precautions.

3.8) AUTHENTICATION AND DIGITAL SIGNATURE

It is advised to use the bank's RSA private key to enable secure digital document signing. The formula below should be used for figuring out the authentication for the information, such as transactions:

Datad_rsa mod n_rsa, for the signature.

Receivers can verify the preciseness of this information through utilizing the lending institution's RSA public key to compare the signature to the original data once the signature has been generated. This procedure aids in preserving the integrity and authenticity of digital documents.

4) PURPOSE OF DUAL INTEGRATION

In addition to the realization that each of ECC and RSA has advantages and disadvantages of their own, neither one of them can be regarded as the best option for an information security system, particularly whenever it comes to handling the security framework of prestigious commercial banking establishments. Therefore, a combined strategy helps to improve operational functionality while also making up for each other's weaknesses.

4.1) SECURITY PURPOSES

ECC

It is renowned for maintaining shorter key lengths while yet being able to offer the same level of security. ECC is helpful in situations with limited resources, when working with smart card systems or mobile devices, because lower key lengths require fewer computational resources for both encrypting and decode data.

This may be particularly crucial in the banking sector, where real-time transactions must take place smoothly and without delay.

Financial organizations may guarantee that their IT infrastructures are optimized for optimal efficiency while still upholding the highest level of security by implementing ECC.

RSA

It is a popular encryption technique that is regarded as being very dependable and secure. This is because it has a long history of being a solid security choice, supported by years of in-depth investigation and study. Regarded as nearly impregnable when used with appropriately long key lengths, making it a favored option in high-security contexts like banking. Whenever it comes to protecting private financial data, where trustworthiness and security are of paramount importance, its dependability is particularly important.

4.2) PERFORMANCE ENHANCEMENT

ECC

ECC has a sizable computational and bandwidth advantage over RSA. ECC uses far more compact keys than RSA while still managing to achieve a comparable level of security. Due to its ability to enable more rapid and successful encryption and decryption procedures, ECC is the more efficient alternative. This factor is extremely important in the banking sector, where many transactions must be handled quickly. Banks can manage a large volume of transactions swiftly and efficiently while upholding the greatest level of security by utilizing the advantages of ECC.

RSA

RSA decryption and encryption operations can be demanding, especially when dealing with longer key lengths. These procedures need more time to process, which could be problematic in the banking industry where being able to react swiftly and effectively is highly valued. When using RSA encryption, it's critical to be cautious about these potential bottlenecks and to think about ways to lessen their negative effects on system performance.

4.3) KEY LENGTH CONSIDERATION

ECC

ECC uses keys of lower lengths, which streamlines and improves the key management procedure. This is especially helpful for the banking sector, where keeping track of several encryption keys can be very difficult from an operational standpoint. Banks can enhance their security protocols and streamline their key management procedures by deploying ECC. In general, any firm wishing to improve its data protection capabilities would be wise to implement ECC.

RSA

RSA encryption method requires longer keys than ECC does in terms of security. The reason for this is that RSA keys need more bits in order to provide the precise same same degree of confidentiality as ECC keys. However, managing lengthier keys can be more difficult and may result in a rise in computing workload. Therefore, it is essential to carefully consider the advantages and disadvantages of each encryption technique based on the specific preferences and requirements of the user.

4.4) FUTURE PROOFING

ECC

Cryptography of ECC offers an elevated degree of protection with shorter keys. It is therefore the best option in circumstances where security for the foreseeable future and the capacity to respond to evolving threats are essential. ECC offers a trustworthy system for data encryption as well as decryption and has its foundation on the mathematical idea of elliptic curves. ECC improves security by employing shorter keys and makes use of memory and processing resources more effectively. It is a great choice for businesses and people who value security and system future-proofing.

RSA

If the right key lengths are used, it is presently accepted whether RSA encryption technology can still be deemed secure. Nevertheless, there are worries that the safeguards of RSA can conceivably deteriorate as computing resources continue to develop. In the future, it might be essential to switch to longer RSA key lengths, which could present administration of keys difficulties.

4) BENEFITS OF THE INTEGRATED APPROACH

5.1) ENHANCED SECURITY

- The system's security is greatly increased by using the cryptographic methods ECC and RSA.
- ECC is quickly gaining reputation for its power in authentication and signatures that are digital, particularly when working with constrained resources, whereas RSA has been a well-liked option with a track record in security.
- Combining these two methods adds a further layer of defense against different types of cyberattacks, improving the system's overall security.

5.2) COMPATIBILITY

- RSA is extensively employed in many organizations.
- ECC-based systems can survive peacefully when both ECC and RSA are used in combination.
- Smooth and safe surroundings for information movement as well as safeguarding is produced.

5.3) PERFORMANCE OPTIMIZATION

- ECC is computationally more effective than RSA.
- Utilize ECC for key exchange and RSA for digital signatures to achieve an appropriate compromise between speed and security.
- To gain advantages of both methods without sacrificing speed or security.

5.4) KEY MANAGEMENT

- RSA is used for secure key distribution and management
- ECC is employed for encrypting and decrypting data.
- The key management procedure can be streamlined
- Made more secure by giving aforementioned various responsibilities.
- The possibility of security breaches while enabling more effective protection and retrieval of critical data is reduced.

5.5) RESISTANCE TO FUTURE THREATS

- The mix of ECC and RSA ensures the greatest level of defense against hazards elated to breach of confidential data.
- This strategy increases the system's resistance to prospective assaults
- Reduces the likelihood that the entire system will be impacted irrespective of whether one algorithm is hacked.
- Bank is better able to protect the private information of its clients
- Uphold stakeholder confidence.

5.6) REGULATORY COMPLIANCE

- Required for banks to use digital signatures
- To adhere to regulatory regulations and industry conventions.
- Dual integration guarantees adherence to the established specifications
- Creation of a robust and trustworthy security protocol.
- Preserve an effective degree of confidentiality
- Compliance with the demands of the sector by using aforementioned methods.

5) CONCLUSION ND SUGGESTION

The purpose of this study is to investigate the beneficial interaction between RSA and ECC and to provide light on the potential benefits of combining both asymmetric cryptographic algorithms for data security in the banking sector. By understanding the subtleties of RSA along with ECC and how they can be implemented, banks may be better prepared to protect their irreplaceable assets and uphold the faith of their customers in an environment that is becoming increasingly digital. A comprehensive information protection solution for banks that integrates RSA and ECC holds significant promise for enhancing defenses against evolving cyberthreats, in conclusion. By integrating the benefits of the two computational methods, banks are better able to protect their valuable assets, maintain customer confidence, and adapt to changing requirements for digital banking security. This integrated approach is likely to become the cornerstone of modern banking security strategies as further research is conducted.

In order to move forward with the coordinated application of RSA and ECC, it is crucial that we carry out tests based on empirical data, optimize the effectiveness of the system, enhance the general public's consciousness, and promote academic research. These actions result in a more secure and reliable environment for the protection of banking information.

6) BIBLIOGRAPHY

1. Md. Ashiqul Islam and others, “Data Security System for A Bank Based on Two Different Asymmetric Algorithms Cryptography” (2021) <https://www.researchgate.net/publication/343373834_Data_Security_System_for_A_Bank_Based_on_Two_Different_Asymmetric_Algorithms_Cryptography> Accessed 15 September 2023
2. Devendrasinh Vashi “An Efficient Hybrid Approach of Attribute Based Encryption For Privacy Preserving Through Horizontally Partitioned Data” (2020)

<https://www.sciencedirect.com/science/article/pii/S1877050920307626> Accessed 15 September 2023

3. Rose Adee and others "A Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography" (2021) <https://www.mdpi.com/1424-8220/22/3/1109> Accessed 15 September 2023
4. Tabassum, T and others "Data Security System for a Bank Based on Two Different Asymmetric Algorithm Cryptography" (2021) <https://www.scirp.org/(S(vtj3fa45qm1ean45vvffcz55))/reference/referencespapers.aspx?referenceid=3561952> Accessed 15 September 2023
5. Priya Matta and others "A comparative survey on data encryption Techniques: Big data perspective" (2021) <**https://www.sciencedirect.com/science/article/abs/pii/S2214785321012153**> Accessed 15 September 2023
6. Nicolas Poggi **"**Types of Encryption: Symmetric or Asymmetric? RSA or AES?" (2021) **<https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes>** Accessed 15vSeptember
7. Eveque Mutabaruka **"**Enhancing Data Security By Using Hybrid Encryption Technique"(2021) <https://www.academia.edu/35842343/Enhancing_Data_Security_By_Using_Hybrid_Encryption_Technique_AES_and_RSA_> Accessed 15September 2023