Journal of Informatics, Computer Science, Data Science And Arificial Intelligence
Volume 2 No. 2 Juni 2025, ISSN : 3031-9145

RSA ENCRYPTION FOR DATA SECURITY IN QR CODE BASED DIGITAL PAYMENT SYSTEM

Muhammad Khalid Hakim Manulang [1], Mhd Zulfansyuri Siambaton [2], Heri Santoso [3]
[1] Universitas Islam Sumatera Utara, khalidmanullang@gmail.com.
[2]Universitas Islam Sumatera Utara, zulfansyuri@ft.uisu.ac.id. [3]Universitas Islam Negeri Sumatera Utara, herisantoso@uinsu.ac.id.

ARTICLE INFO

ARTICLE HISTORY:
Received : 22 Juni 2025
Revised : 22 Juni 2025
Accepted : 22 Juni 2025

Keywords: Digital Payment, QR Code, RSA, Key Generator.

ABSTRACT

This research, titled "RSA Encryption for Securing Data in QR Code-Based Digital Payment Systems," aims to enhance transaction data security in the increasingly popular digital payment environment. In today's digital era, the use of cashless payment methods through applications such as OVO, DANA, and GoPay simplifies transactions but also introduces risks related to data security. Therefore, a solution is needed to ensure the confidentiality and integrity of data. In this study, the RSA (Rivest-Shamir-Adleman) algorithm is employed to encrypt transaction data before it is embedded in a QR Code format. This process involves the generation of public and private keys, data encryption, and the creation of a unique QR Code for each transaction. The results indicate that using RSA with a 2048-bit key length provides a high level of security, effectively protecting data from unauthorized access and ensuring data integrity throughout the transmission process.Based on the analysis, the integration of RSA encryption and QR Code technology proves to be effective in mitigating data theft risks. This research is expected to serve as a reference for the further development of more secure digital payment applications, while also offering insights into the real-world application of cryptography.

INTRODUCTION

In the current era of rapid digital transformation, cashless payment systems have become an essential component of modern society. The widespread adoption of digital payment platforms such as OVO, DANA, and GoPay—leveraging Indonesia's QRIS (Quick Response Code Indonesian Standard)—has significantly improved the convenience, speed, and efficiency of financial transactions. Among the core technologies enabling these systems is the Quick Response (QR) Code, which serves as a digital medium for storing transaction-related information that can be instantly scanned by smart devices to initiate payments.

Despite the benefits, the implementation of QR Code-based systems introduces notable security vulnerabilities, including data breaches, unauthorized manipulation of transaction details, and various forms of cyberattacks. These risks underline the necessity of integrating robust data protection mechanisms to ensure the confidentiality, integrity, and authenticity of transaction data.

RSA (Rivest–Shamir–Adleman) is a well-established public-key cryptographic algorithm known for its high level of security, which is based on the computational difficulty of factoring large prime numbers. Due to its proven effectiveness, RSA is widely used in secure communications and digital identity verification across various domains. In the context of digital payment systems, RSA encryption can be utilized to secure transaction data encoded in QR Codes, ensuring that only authorized parties can access the original information (Surya et al., 2024).

Motivated by these challenges, this study proposes the implementation of RSA encryption as a security enhancement for QR Code-based digital payment systems. The objective is to demonstrate how RSA can be effectively applied to encrypt transaction data, thereby mitigating potential threats and enhancing the overall security of cashless payment solutions.

The RSA scheme is one of the most widely used public key encryption systems. It exploits the mathematical properties of modular exponentiation and relies on the computational difficulty of factoring large integers(Zhang et al., 2020).

One of the core features of RSA is the modulus $N = p \times q$, where p and q are large prime numbers such that $q < p$. Let $\varphi\ (N) = (p-1)(q-1)$ denote Euler's totient function. The values e and d are then selected to serve as the public and private keys, respectively (Nitaj et al., 2022).

A QR Code is a two-dimensional image used to represent data, primarily textual information. It is an evolution of the traditional one-dimensional barcode into a two-dimensional format. Unlike barcodes, which encode data in only one direction, QR

Codes store information in both vertical and horizontal directions. As a result, QR Codes are capable of containing significantly more information than conventional barcodes (Anjani et al., 2021).

The Quick Response Code (QR Code) is an evolutionary advancement of the traditional one-dimensional barcode into a two-dimensional format. The underlying motivation for the development of QR Codes was the limited data capacity of barcodes, which could store only up to 20 alphanumeric characters (Munawar, 2019).

A digital payment system is a method of conducting financial transactions through electronic devices such as smartphones, computers, or payment cards (debit, credit, or prepaid). This system leverages financial technology (FinTech) to enable faster, more convenient, and more secure transactions compared to conventional cash-based payments. The digitalization of payment systems has become a significant global trend, driven by the increasing adoption of the internet and information technology devices. The shift from cash-based transactions to digital payments has strengthened financial inclusion and modernized the way individuals and businesses conduct their daily transactions (Eren, 2024).

Rapid technological advancements have had a significant impact on the evolution of payment systems within the business sector, particularly in maintaining the continuity of business relationships between parties. As a fundamental pillar of financial stability, payment systems have undergone a transformation—from traditional cash-based methods to digital payment systems or electronic money (e-money). This technological innovation has shifted the role of physical currency toward more efficient and cost-effective cashless payment systems. Today, cashless transactions are carried out without the use of physical money, instead utilizing interbank or intrabank transfers via internal banking networks. In addition, non-cash payments can also be made using transaction cards such as ATM cards, debit cards, and credit cards (Tarantang et al., 2019).

Python is a versatile interpreted programming language designed with an emphasis on code readability. It is widely regarded as a language that combines power and capability with highly readable syntax. Python is also equipped with an extensive and comprehensive standard library, making it well-suited for a wide range of programming tasks (Sinaga, 2017).

Python was first created by Guido van Rossum in the Netherlands in 1990. Its name was inspired by van Rossum’s favorite television show, Monty Python’s Flying Circus. Initially developed as a hobby project, Python has since evolved into a widely adopted programming language in both industry and education due to its simplicity, concise syntax, intuitive structure, and extensive library support (Sinaga, 2017).

RESEARCH METHODS

The design of this research can be seen in the following diagram :

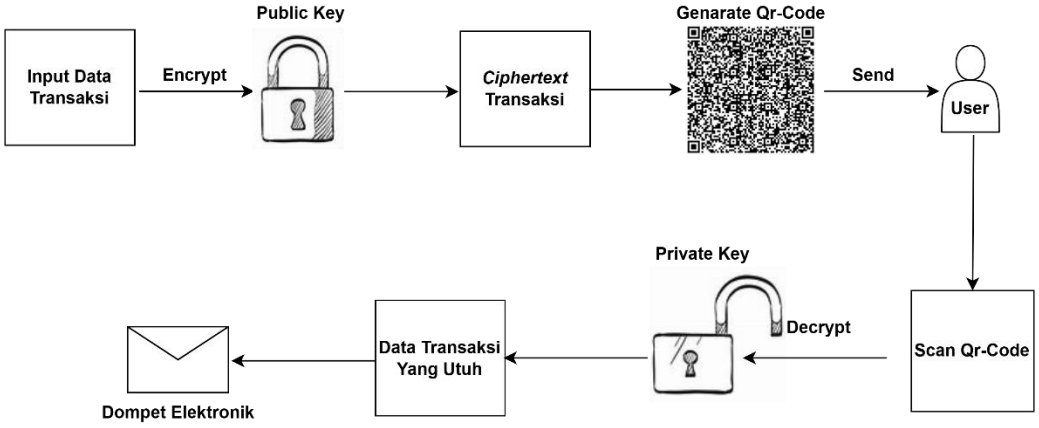

Figure 1. Overview of the Research Design

Figure 1 illustrates the general research diagram of "RSA Encryption for Securing Data in QR Code-Based Digital Payment Systems." When a user initiates a transaction, they are required to input transaction data, such as the recipient's phone number for the payment, the amount of money to be transferred, and the sender's name. After the data entry process is completed, the next step is to encrypt the transaction data using the RSA public key. At this stage, the original transaction data (plaintext) is converted into encrypted data (ciphertext), making it unreadable to unauthorized parties.

The next step is to generate a QR code, which is uniquely associated with a single transaction. This QR code is then sent to the recipient. The recipient scans the QR code, and the scanned encrypted data is decrypted using the recipient's RSA private key. Once the decryption is successful, the complete transaction details are revealed, and the recipient receives the transferred amount as specified.

The flowchart of the encryption process within the system is presented in Figure 2 below.

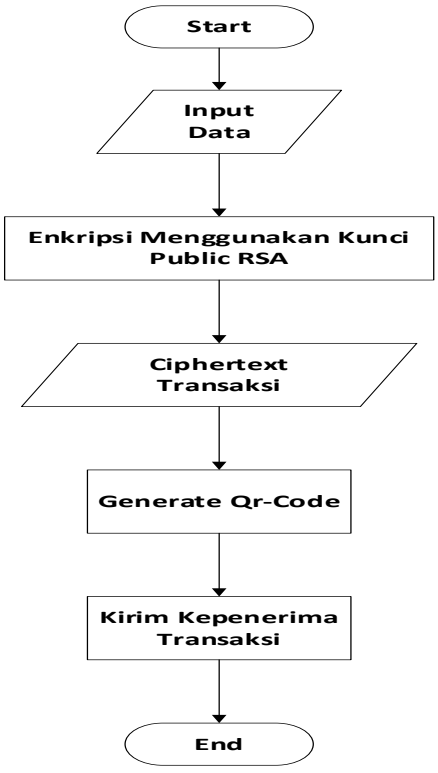

Figure 2. The flowchart of the encryption process

Figure 2 shows the system encryption flowchart, where the process begins with a "Start" step, followed by inputting the transaction data. The transaction data is then encrypted using the RSA public key, resulting in the ciphertext of the transaction. The next step is to generate a QR code, which is then sent to the transaction recipient.

The flowchart of the decryption process within the system is presented in Figure 3 below :

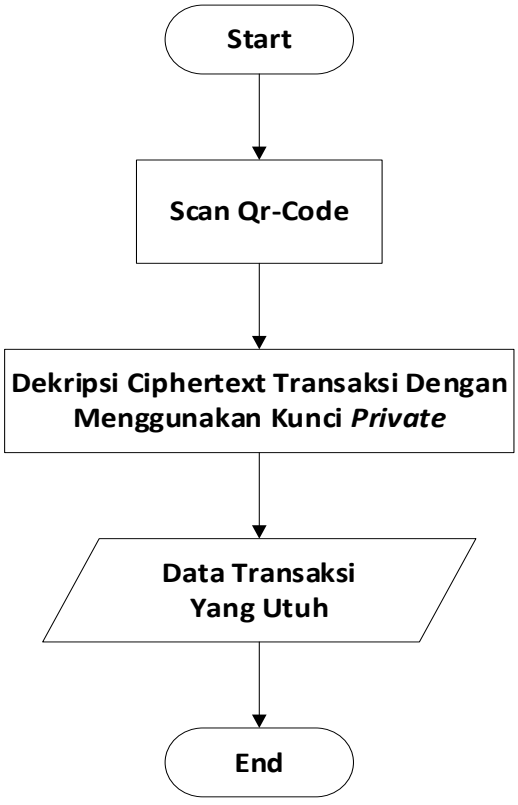

Figure 3. The flowchart of the dcryption process

Figure 3 illustrates the decryption flowchart, where the process begins with a "Start" step, followed by scanning the QR code. The scanned ciphertext is then decrypted using the recipient's private key. Once the decryption process is completed, the result is the original, complete transaction data.

RESULTS AND DISCUSSION

In this study, the RSA algorithm was successfully implemented for securing data in a QR code-based digital payment system. The implementation consists of three main stages: the encryption process, QR code generation, and the decryption process.

1. Encryption Process

Transaction data, such as the recipient's account number, payment amount, and user identity information, is encrypted using the RSA public key. The encrypted result, in the form of ciphertext, is then stored as a QR code. This process ensures that the original data cannot be accessed without the corresponding private key.

2. QR Code Generation

After the data is encrypted, the system generates a unique QR code for each

transaction. This QR code serves as a medium for storing the ciphertext and can be scanned by the transaction recipient.

3. Decryption Process

The transaction recipient scans the received QR code. The data within the QR code is decrypted using the RSA private key to restore the original data. The decryption result includes complete transaction information, such as the account number, payment amount, and recipient's name.

The implementation of the RSA algorithm with a 2048-bit key length provides a high level of security, in accordance with modern security standards. The QR code is also used as a practical storage medium, facilitating the secure transmission of transaction data.

CONCLUSION

1. In this study, the RSA algorithm was successfully applied to encrypt transaction data, such as the recipient's account number, payment amount, and user identity information. The encrypted data was stored in ciphertext format within a QR code, ensuring that only parties with the corresponding private key could access the original data.
2. With a 2048-bit key length, the RSA algorithm provides a high level of security against brute-force attacks, while also ensuring data integrity during transmission. The QR code is utilized as a practical storage medium, enabling secure and efficient delivery of transaction data.
3. The encryption process using the RSA public key and the decryption process using the RSA private key were successfully implemented in an integrated manner, resulting in a secure and reliable digital payment system.
4. This study demonstrates that the integration of the RSA algorithm and QR code can serve as an effective solution to mitigate the risk of data theft in digital payment systems, particularly in safeguarding the privacy and security of cashless transactions.

REFERENCES

Anjani, D., Novianti, D., & Wear, A. S. (2021). *Pelatihan Pemanfatan Quick Responde Code Technology dalam Pengembangan Media Pembelajaran*. *1*(2), 123–131.

Eren, B. A. (2024). QR code m-payment from a customer experience perspective. *Journal of Financial Services Marketing*, *29*(1), 106–121. https://doi.org/10.1057/s41264-022-00186-5

Munawar, Z. (2019). *TEMATIK - Jurnal Teknologi Informasi Dan Komunikasi Vol. 6, No. 2 Desember 2019*. *6*(2).

Nitaj, A., Ariffin, M. R. B. K., Adenan, N. N. H., Lau, T. S. C., & Chen, J. (2022). Security Issues of Novel RSA Variant. *IEEE Access*, *10*, 53788–53796. https://doi.org/10.1109/ACCESS.2022.3175519

Sinaga, M. C. (2017). Kriptografi dan Python. *Academia*, 157. https://www.academia.edu/34788898/Kriptografi_dan_Python_pdf

Surya, R. W., Rudhistiar, D., Ariwibisono, F. X., & Informatika, T. (2024). *PEMANFAATAN QR CODE TERENKRIPSI MENGGUNAKAN*. *8*(6), 12424–12431.

Tarantang, J., Awwaliyah, A., Astuti, M., & Munawaroh, M. (2019). *PERKEMBANGAN SISTEM PEMBAYARAN DIGITAL PADA ERA REVOLUSI INDUSTRI 4.0 DI INDONESIA*. *4*, 60–75.

Zhang, H., Yu, J., Tian, C., Tong, L., Lin, J., Ge, L., & Wang, H. (2020). Efficient and Secure Outsourcing Scheme for RSA Decryption in Internet of Things. *IEEE Internet of Things Journal*, *7*(8), 6868–6881. https://doi.org/10.1109/JIOT.2020.2970499