DOI: 10.22146/jnteti.vol13i4.12867

# Comparison of Mobile Transaction Security using NFC and QR Codes

**Lucia Nugraheni Harnaningrum[1], Kristoforus Nanda Mahardhian[1]**

[1] Informatics Study Program, Faculty of Information Technology, Indonesia Digital Technology University, Bantul, D.I. Yogyakarta 55198, Indonesia

[Received: 12 May 2024, Revised: 18 July 2024, 2024, Accepted: 9 October 2024]
Corresponding Author: Lucia Nugraheni Harnaningrum (email: ningrum@utdi.ac.id)

**ABSTRACT** — Mobile device transactions have become commonplace today. Quick-response (QR) codes and near-field communication (NFC) are popular cashless and contactless payment methods. These two payment methods have their characteristics. NFC payments use secure elements that encrypt credential data to ensure safe transactions. In contrast, QR code payments transmit data in its original form without encryption. In other words, existing data are sent between devices in the form of original data. Given the extensive adoption of these methods, it is imperative to secure transaction data to prevent theft and misuse. It is necessary to know and compare the security level of each transaction and provide the best recommendations. This study undertook a comparative analysis of the security and performance of NFC and QR code-based mobile payment models. The study found that NFC transactions required 1,074 ms for encryption, while QR code transactions took 5.9359 ms. The entropy value, indicating data randomness, was 3.96 for NFC and 3.23 for QR codes. The p-value, representing statistical significance, was 0.45 for NFC and 0.069 for QR codes. Both payment methods demonstrated acceptable levels of safety, with processing times and data randomness within satisfactory ranges. However, the analysis concludes that NFC transactions offer superior performance in terms of processing time and data security compared to QR code transactions.

**KEYWORDS** — NFC, QR, Secure Element, Encryption, Data Randomness.

## I. INTRODUCTION

Transactions via mobile devices have become commonplace among the public today. Mobile devices, with all their facilities, have become a basic need for today's society. According to a survey by Statistica, mobile payments in Indonesia, notably those made using quick-response (QR) codes, account for 50% of all existing mobile payments. In the United States, QR code payments are a popular payment method based on statistical data. Payments with near-field communication (NFC) mobile devices have gained significant popularity when the COVID-19 pandemic hits the world. Statistical data indicates that NFC secure element shipments were 620 million units worldwide in 2018.

QR codes have been widely used in various activity areas, including patient monitoring [1], marketing with mobile devices [2], inventory management systems [3], mobile payment systems [4], and transportation [5]. Transactions using QR codes are also more widely used because all smartphones are currently equipped with cameras to scan QR codes.

Despite their similarity in cashless and contactless payment, QR code and NFC have their characteristics. Payments with NFC use a secure element. This secure element ensures that payments occur safely, and that credential data are encrypted. On the other hand, payments with QR codes do not use encryption. Existing data are sent between devices in the form of original data. Current transactions accommodate payments using many methods. The data above indicates that QR codes and NFC are widely utilized payment methods. However, users must be careful of thieves who exploit transaction data to harm customers and sellers. For this reason, securing data during transactions is imperative.

This research reviewed transactions using NFC and QR codes, especially from a security perspective. The security reviewed was data confidentiality and transaction speed. By comparing the two methods, it is hoped that the advantages and disadvantages and the best method are obtained, minimizing the possibility that data can be stolen and used by others. Research on transactions using NFC has been carried out previously. In this research, mobile transactions using QR codes were tested. The results were compared with previous studies.

Secure mobile payment transactions are imperative. With so many transactions, security also needs to be improved. The security level of each transaction must be known and compared to provide the best recommendations. This research compared mobile payment transaction models using NFC and QR codes.

## II. NFC AND QR CODE APPLICATION PROTOCOL

Research has been conducted on mobile transactions using NFC and QR codes. A study on payment protocols for mobile NFC cited addressed vulnerabilities such as random-access memory (RAM) scraping, denial of service (DOS), distributed denial of service (DDOS), and phlashing attacks. Moreover, they mitigated well-known mobile application weaknesses like Heartbleed and ROBOT [6]. Another research developed a security protocol for automatic teller machine (ATM) transactions utilizing NFC on mobile devices [7]. This study enhanced the dynamic array PIN protocol (DAP), which is susceptible to certain video eavesdropping or camera recording attacks. The improvements focused on the PIN authentication process at ATMs to bolster NFC transaction security. The effectiveness of the proposed security solution was demonstrated by showing that attackers could not discern the correct PIN through an intersection multiple records attack.

Another application of NFC technology is its use in a flexible epidermal sensor that utilizes an NFC protocol specifically designed and tested for monitoring cortisol levels in sweat [8]. This prototype benefited from high frequency (HF)

communication, ensuring it was robust against variability and maintains consistent user communication. It achieved a detection range of about 3.5 to 4 cm for each user and application point on the body. Preliminary testing of the sensor has confirmed the reliability of the data collected, which is on par with that of far more costly devices.

NFC technology has also been utilized in a battery management system (BMS) [9]. This study used NFC technology to present a novel system for secure data transfers between the BMS and mobile readers. The design worked well for active and passive BMS setups, whether using a standard controller or a modulated battery pack. The system incorporated secure NFC data exchange format (SNDEF) security record and a lightweight symmetric encryption approach to ensure authentication, data confidentiality, and integrity during the mobile reading. Challenges addressed included battery longevity, storage, reuse, and wiring issues. The research suggested enhancing traditional BMS designs by integrating NFC to enable wireless reading of battery pack statuses. Moreover, it added a lightweight security layer to the NFC protocol to ensure that battery packs were managed solely by authorized devices and that data were secure from external interception and modification.

NFC technology has also been employed alongside QR codes. QR codes create customer tokens or PINs for transactions [4]. Customers generate these while waiting in line at a merchant for payment. When payment initiation occurs, the merchant displays a QR code. The customers scan this code, and a one-way private key is generated with merchant data, which is then transmitted to the merchant using NFC communication. Subsequent transactions proceed as agreed. These data are then passed on to third parties, which should suffice for completing the transaction without additional verification. The payment model determines whether the mobile operator bills the customer, the customer's bank handles the funds transfer, or the service provider facilitates the transfer of funds from the customer to the merchant's bank.

Additional security measures can be implemented while scanning a customer's QR code, such as entering a PIN. However, this step is often unnecessary because the phone is typically locked. The scanning process authenticates the customer's identity and restricts the transaction amount. Moreover, the absence of a handshake to confirm transactions between third parties and customers is expected to expedite processing times compared to credit card payments. This research aimed to address both processing speed and security concerns. The approaches suggested in this paper are adaptable across the four mobile payment models discussed—the lack of a handshake for payment confirmation results in faster processing than traditional credit card transactions. However, the security proposed is designed to be as robust as credit card payments.

NFC and QR codes are increasingly utilized in public transportation payment systems [5]. With the development of the Internet, along with NFC and QR code technologies, a novel payment system for public transit has been launched. This system is integrated with banking and ticketing systems to facilitate quicker and more efficient travel. The research enhances this system by incorporating NFC and QR code technologies with integrated circuit (IC) cards to address existing limitations. It creates a platform that supports payment interconnection across all three technologies. The system's functionality is verified through simulations of registration, login/logout processes, and payment transactions to ensure security and functionality. The findings indicate that the system can cater to the diverse needs of users and accept various payment methods simultaneously, thus offering passengers a more comprehensive and satisfying experience.

TABLE I
COMPARISON OF CODING WITH NFC AND QR CODE

| NFC | QR Codes |
|---|---|
| NFC incorporates encryption by default, which significantly enhances security for payment transactions. Additionally, it operates over short ranges, which limits the ability of hackers to intercept data during NFC-enabled transfers. | QR codes can be encrypted, but it is impossible to know whether they are, so it is up to the user to judge whether a particular code is secure. |
| NFC tags must have a chip encoded within them to enable device reading. | QR codes are free to create via websites or applications. |

The use of QR codes as a payment system was examined in [10]. This study detailed the design and implementation of a secure payment system utilizing QR codes, which have become increasingly popular due to their ability to streamline the payment process and enhance user convenience. Despite their advantages, QR code-based online payment systems are susceptible to security threats. As such, the transaction process must be robust enough to safeguard the integrity and confidentiality of each payment. Additionally, online payment systems must verify the sender and recipient's authenticity in each transaction. This paper introduces a security solution for the proposed QR-based system using visual cryptography. The system includes a mobile application and a payment gateway server that employs visual cryptography to provide a straightforward and secure user interface for conducting payment transactions.

## III. TRANSACTION WITH NFC AND QR CODE

### A. COMPARISON OF TRANSACTIONS WITH NFC AND QR CODES

Table I compares NFC and QR code coding. NFC has a relatively good security system and long-established transaction protocol systems compared to the NFC device. NFC also has a protocol standard based on the International Organization for Standardization (ISO). This situation makes NFC quite recognized and trusted. Meanwhile, coding with QR codes is still in development, and many security gaps could threaten their transactions.

### B. POTENTIAL QR CODE SECURITY THREATS

Numerous instances have occurred where QR codes have been exploited and misused. Hackers and malicious entities often use QR codes as a method for launching attacks. The prevalent form of exploitation involves embedding a harmful URL into the QR code. The most common security threats associated with QR codes include malware attacks, phishing attempts, QR-code related bugs, and financial theft. QR code users need to ensure that the QR code generator is safe. QR code generators are safe if the platform used to generate them provides the right features and has a good reputation. The best action is to ensure security and privacy by remaining vigilant. QR code scanning is carried out using a camera, and the scanned QR code must be within the reader's camera field of view.

### C. DATA ENCRYPTION AND ENCAPSULATION MODEL

Data transmitted from the smartphone to the point of sale (POS) were first encrypted and encapsulated. Once the data reached the POS, they were decoded to retrieve the original data. This proposed model used smartphone users' data, even card data. These data were stored, encrypted, sent, and received in encrypted form. Data were decrypted only when a transaction was carried out. They are removed after the transaction is completed because decryption data is only stored in a variable.

Encryption was carried out using the advanced encryption standard (AES) and Rivest-Shamir-Adleman (RSA) cryptographic algorithms, which were tested using the transaction protocol. AES was used because the symmetric cryptographic algorithm is light. Meanwhile, RSA was used in the transaction process because the asymmetric cryptographic algorithm is more suitable for short-distance data exchange [11]. The selected algorithms are straightforward, lightweight, and feature adjustable parameters. They were chosen for their simplicity and minimal resource demands. Additionally, security can be enhanced by altering the parameters for each new transaction.

### D. DESIGN ANALYSIS OF MODEL TEST RESULTS

The transaction model built using QR codes was based on security and speed. Security was tested by analyzing data randomness. Speed was tested since faster processes reduce attack opportunities. This model was tested on Android smartphones with different brands, memory sizes, and versions. The test results were analyzed using the method is described in the subsequent section. This model referred to a transaction model using NFC that had been tested, and results had been obtained [12]. Then, the results obtained in this research were compared with the test results in [12].

The following is a security analysis that incorporates data randomness testing. The security level of the encrypted data can be analyzed for randomness. Random data makes it difficult for attackers to interpret the data even if they successfully capture them. Attackers can only obtain the original data if they know the encryption method and parameters, including the encryption key. The data were tested for randomness using the monobit test to obtain this analysis' p-value and entropy. Data randomness analysis was done using the frequency (monobit) test method [13]. Security test parameters are shown in Table II.

Shannon's entropy test parameters explain [11], [14] that the entropy value approaches $2^n$, where $n$ is the number of probability bits. This parameter determines whether the encrypted data is in the unpredictable category. Regarding the processing time parameter [14], the fastest time for factorization was 17.5 ms with $n$ = 500. The parameter ensures that the processing time is faster than attacker's time to interpret the data. Regarding resistance to factorization attacks and statistical calculations [15], [13], the process of factorization and statistical calculations still took a long time. This parameter determines the value of randomness that can defend against attacks. The parties involved mutual authentication parameter must be guaranteed to be trustworthy [16]–[20], because the parameter is used to ensure data transmission originates from and is addressed to the correct or appropriate party. Security and authentication levels parameter, secure data makes users trust [16], [17]. This parameter ensures that data sent between parties has a good security layer.

TABLE II
SECURITY TEST PARAMETERS

| Test Parameters | Supporting Papers | Explanation | Objective |
|---|---|---|---|
| P-value | [11] [13] | If the p-value < 0.01, it is not random, and vice versa | To find out whether the encrypted data is in the unpredictable category |
| Shannon's entropy | [11] [14] | The entropy value approaches $2^n$, where $n$ is the number of probability bits | To find out whether the encrypted data is in the unpredictable category |
| Processing time | [14] | The fastest time for factorization is currently 17.5 ms with $n$ = 500 | To ensure that the processing time is below the time it will take an attacker to interpret the data if the attacker successfully retrieves it. |
| Resistance to factorization attacks and statistical calculations | [15] [13] | The process of factorization and statistical calculations still takes a long time | To find out the value of randomness that can defend against attacks |
| Mutual authentication | [16] [17] [18] [19] [20] | The parties involved are guaranteed to be trustworthy | Ensure data transmission originates from and is addressed to the correct or appropriate party. |
| Security and authentication levels | [16] [17] | Secure data makes users trust | Ensure that data sent between parties has a good security layer. |

Speed was compared to an attacker's time to search for the encryption key. If data processing time were shorter than the encryption key search time, the data were considered secure. Attacks carried out by attackers can occur by looking at the time required to obtain information about the key or plaintext. If the processing time is fast, attacks can be avoided.

## IV. RESULTS AND DISCUSSION

### A. TRANSACTION MODEL ARCHITECTURE

The mobile transaction security model was applied to transactions with NFC, and the same model was applied to QR codes. QR codes were used because all smartphones have cameras that allow them to scan them. This advantage, combined with NFC transaction benefits, uses encryption and requires no internet communication, ensuring secure transactions.

The mobile payment system using a QR code underwent testing during the transaction phase. Payment cards, securely stored on smartphones, were ready for transactions. The

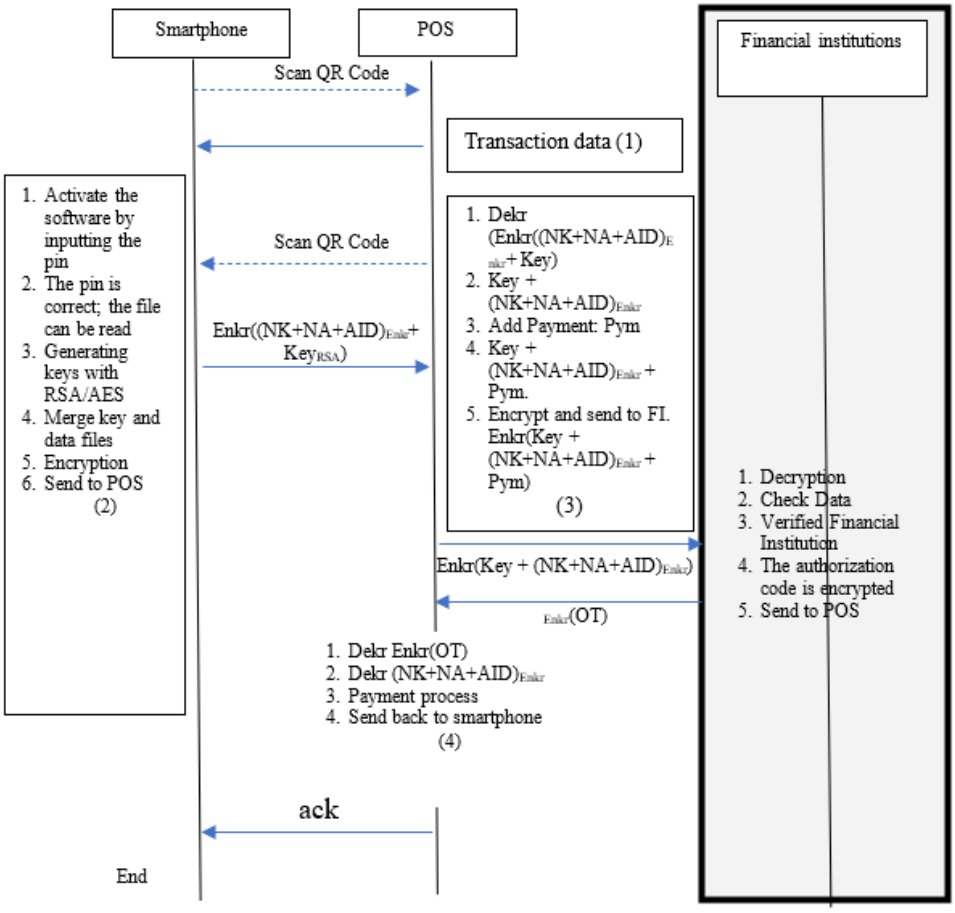


**Figure 1.** Transaction model without internet connection between smartphone and POS (modified from [12]).

transaction model ensured safe and accurate exchanges between the smartphone and the POS. The architecture of the transaction model is depicted in Figure 1.

This transaction model incorporated a security system within the smartphone. The security system, an application designed to protect data and communication between smartphones and POS, was constructed using components installed on the smartphone. Components on both devices were examined and then modified for integration with the security system application.

This transaction model utilized data stored on a smartphone and ensured its security, specifically when using QR code communication. Two measures were implemented to prevent attacks: protecting data from unauthorized access and ensuring correct data request routing. The transaction security system involved three key entities: smartphones, POS, and financial institutions. This study focused on securing transactions between smartphones and POS.

In the first step, the POS converted the purchase amount data into a QR code form and displayed them on the POS screen. When the POS displayed QR code data, the smartphone scanned the QR code using an application related to the transaction. In the second step, the smartphone processed the card data, encrypted them, and converted the encrypted data to QR code form. In the third step, POS scanned the smartphone QR code. Next, the POS authenticated and forwarded the card data to the financial institution's server. POS received notification of approval from the financial institution. The POS received the data sent from the smartphone, then decrypted them, and payment data were added, as shown in (1).

$$D_{trans} = D_{user} + D_{pay} \quad (1)$$

where $D_{trans}$ is the data used for transactions, $D_{user}$ is user data, and $D_{pay}$ is payment data. The POS encrypted the data and sent them to the financial institution, as shown in (2).

$$E_{trans} = (RV, D_{trans}) \quad (2)$$

where $E_{trans}$ is encrypted transaction data, $E(RV, D_{trans})$ is random number data generated during the transaction

At financial institutions, the data were decrypted and checked against customer records. If the financial institution confirmed the match, an encrypted authorization code was generated. If not verified, a message indicating the lack of verification was sent. The financial institution then communicated the relevant data or notification to the POS.

In the fourth step, the POS processed the payment and notified the smartphone if the transaction was successful. Authentication data and data from the smartphone and user were decrypted. Subsequently, the payment transaction was executed. This process concluded with a notification sent to the smartphone, with the POS initiating and the smartphone serving as the target.

Data transmitted from the smartphone to the POS were initially encrypted and encapsulated. Upon reaching the POS, these data were decoded to retrieve the original content. Encryption utilized the RSA cryptographic algorithm. The selected algorithm was uncomplicated and lightweight, featuring modifiable parameters, making it ideal for devices like smartphones with limited memory capacity.

Meanwhile, parameter options can be modified to increase security by changing the parameter values for each new

transaction. The model was also tested using the AES encryption algorithm. AES was chosen because transactions are close, and the encryption key can be shared between two adjacent devices. The mobile application also supports the AES algorithm because it is lightweight.

Up to this point, the transaction model has been finalized. This model was designed for routine transactions. To prevent attacks, data were encrypted when stored and transmitted between devices.

### B. SYSTEM DEVELOPMENT FOR TRANSACTION MODELS

The development of the transaction model was applied to two devices: the smartphone the user used, which already had secure card data; and the POS, which accepted payments from the transaction process. The initial step in the transaction process was for the POS to determine the nominal amount to be transacted. This amount was converted into a QR code at the POS so that it was ready to be scanned by a smartphone user.

POS was ready to send transaction data; the user was on the transaction page after entering the PIN. If the PIN was authenticated, the user was on the transaction page. When entering the transaction page, the camera was activated to read the QR code.

Transactions were carried out by users scanning the QR code and then translating the data contents. The user's smartphone prepared the card data, encrypted them, and converted them into a QR code. The POS received card data, added with payment data, and sent to the financial institution server. If the data were verified, the transaction process continued, with the financial institution sending a success notification to the POS. The POS received and processed the transaction, which was complete.

### C. RUNTIME TESTING

The proposed transaction model was tested on smartphones with Android operating systems versions 8 and 10. The parameters tested were execution time and data randomness analysis using the monobit test.

Figure 2 shows that encryption time varies with key length, memory, and smartphone versions without any clear pattern. The time to scan the QR code with AES and RSA is shown in Figure 3. The RSA-4096 encryption key length required the longest encryption time, while the AES key length was 128. The time needed for encryption and creating a QR code with RSA-4096 was relatively long compared to key lengths and other encryption methods.

### D. MONOBIT AND ENTROPY TEST

The data used for testing were created under the following conditions: ID data (card ID, device ID, and user ID) was made, with the difference between the first and second data being only one character. The selection was made so that the analysis could be carried out by only considering changes close to one bit.

Table III shows the p-value, and Table IV shows the entropy value, showing that the data encryption results are declared random [11]. The entropy value was below 3, except for RSA-4096, so the data were not close to a random value for entropy analysis. In comparison to [19], which has a similar transaction model, the time required for the transaction model in this research was 5.9359 ms, which is faster than the transaction model in [19] which required 50 ms.

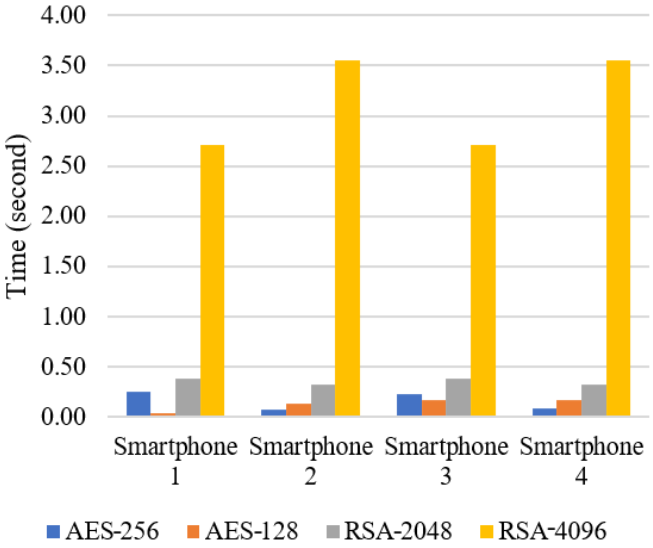


**Figure 2.** Encryption time in generate QR code.

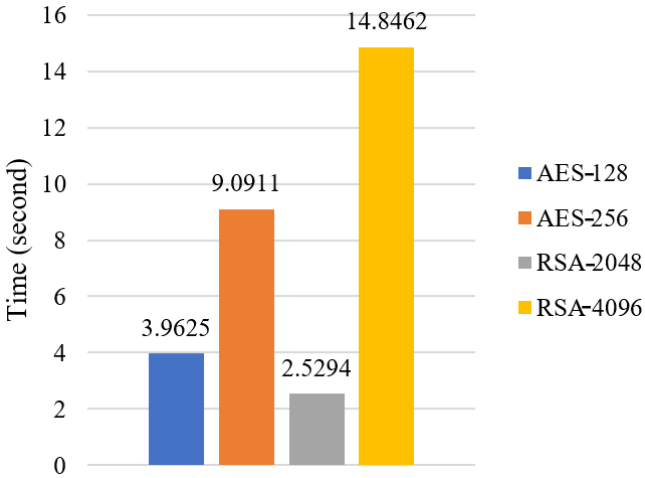


**Figure 3.** Time to scan the QR code.

TABLE III
P-VALUE FOR VARIOUS SMARTPHONE CONDITIONS

| Encryption | HP 1 | HP 2 | HP 3 | HP 4 | Conclusion |
|---|---|---|---|---|---|
| AES-128 | 0.0449 | 0.1228 | 0.0212 | 0.0884 | Random |
| AES-256 | 0.0398 | 0.0697 | 0.1129 | 0.0310 | Random |
| RSA-2048 | 0.0641 | 0.0683 | 0.0768 | 0.0768 | Random |
| RSA-4096 | 0.0641 | 0.0641 | 0.0777 | 0.0777 | Random |

TABLE IV
ENTROPY VALUES FOR VARIOUS SMARTPHONE CONDITIONS

| Encryption | HP 1 | HP 2 | HP 3 | HP 4 | Conclusion |
|---|---|---|---|---|---|
| AES-128 | 3.2617 | 3.2487 | 3.2971 | 3.2971 | Random |
| AES-256 | 3.2388 | 3.2838 | 3.2469 | 3.2686 | Random |
| RSA-2048 | 3.2468 | 3.2710 | 3.2468 | 3.2710 | Random |
| RSA-4096 | 3.2468 | 2.9894 | 3.2468 | 2.9894 | Random |

### E. ANALYSIS OF RESISTANCE TO FACTORIZATION ATTACKS

The resistance to factorization can be analyzed by calculating the possible processes that occur to obtain the RSA algorithm key. The total transaction processing time in this study was 1.074 ms. The time to factor is 4 hours for Fermat's factorization and 1.98 hours for Pollards' rho.

When data were sent to the financial institution's server, an AES or RSA key was generated on the smartphone. This encrypted key then looked for the entropy value and p-value. The entropy and p-value also indicate that the encrypted data are declared random. The data are declared random when the p-value is 0.01 [11], [13]. Data that have been declared random can be said to be safe because, to interpret random data, someone needs an encryption key. The key can be obtained if someone can guess the key. Factorization was used to do this.

The resistance to factorization can be analyzed by analyzing the resistance of the AES algorithm to brute-force attacks [21]. The AES algorithm with a 128-bit key has a possible combination of 3,403 × 1,038, and a key of 192 has a potential combination of 6,278 × 1,057. A key of 254 has a possible combination of 1,158 × 1,077. Current supercomputers have a capacity of 33.86 floating point operations per second (PFLOPS) [21], 415.5 PFLOPS [22], and 488 PFLOPS [23]. The fastest supercomputer today is 415.5 PFLOPS, equivalent to 415.5 × 1,015 FLOPS. Consequently, the AES-256, solved at supercomputer speed, required 7.525 x 1052, with a calculation of 1 year = 31,536,000 s. One year can produce a key combination of 31,536,000 × 488 × 1,015 = 15,389,568 × 1,018, and the time required is 1,158 × 1,077 / 1.539 × 1,024 = 7.525 × 1,052. The AES algorithm is declared safe against attacks that attempt to decipher encrypted data by searching for keys, even though it is carried out by the fastest supercomputers today.

### F. COMPARISON OF TRANSACTIONS WITH NFC AND QR CODES

The trial results of transactions using a QR code were compared with transactions using NFC. Previous research has carried out transaction trials with NFC, with results as shown in Figure 4, Figure 5, Table V, and Table VI.

The required time was significantly under 1 s, with an average of 1.074 ms according to testing (Figure 4 and Figure 5). The time to generate encryption and a QR code was 5.9359 ms. While there was a noticeable difference in the duration of NFC and QR code transactions, both were well within acceptable safety limits. This duration is considerably short compared to an attacker's time to access and decode encrypted data, which exceeds 1 s. This interval is much less than an attacker's minimum time to complete the factorization process using various methods. Fermat's algorithm took 7.2 ms; times for other algorithms exceeded this result.

The entropy value and p-value for transactions using NFC and QR codes in Table V and Table VI also show that the encrypted data are declared random. From these values, the entropy and p-value of transactions with NFC were higher than those with QR codes.

The time required for encryption on transactions with NFC was 1,074 ms, while the QR code was 5.9359 ms. The entropy value on transactions with NFC was 3.96, while on QR code, it was 3.23. The p-value on transactions with NFC was 0.45, while on QR code was 0.069. The difference in speed was because reading the QR code required pattern recognition, while on NFC, it directly read the data sent.

The comparison of NFC and QR codes showed that NFC transactions are better than QR code transactions. However, both were still within safe limits regarding time and data randomness. From the results and analysis of trial results, transaction protocols with NFC and QR codes can be used to prevent attacks that will take data and exploit them.

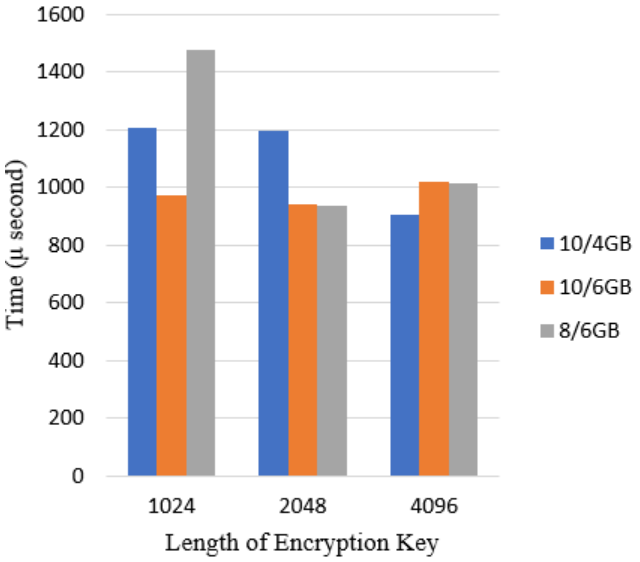


**Figure 4.** Encryption time of data on smartphones with NFC.

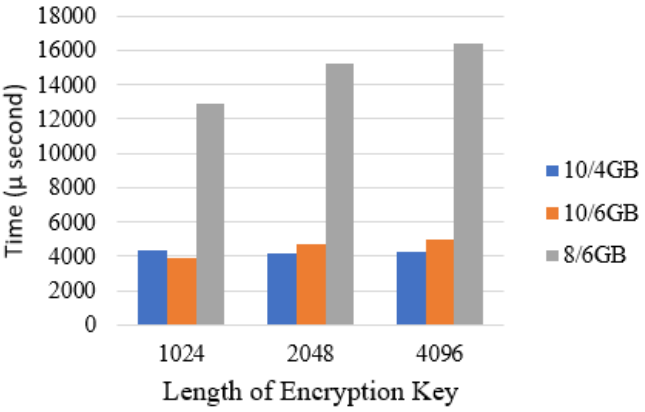


**Figure 5.** Time to send customer data to POS via NFC-host card emulation (HCE).

TABLE V
P-VALUE FOR VARIOUS SMARTPHONE CONDITIONS WITH NFC

| N | P-Value | | | Conclusion |
|---|---|---|---|---|
| | *10/4GB* | *10/6GB* | *8/6GB* | |
| 1024 | 0.456868 | 0.429522 | 0.454812 | Random |
| 2048 | 0.456868 | 0.426614 | 0.454812 | Random |
| 4096 | 0.472147 | 0.447746 | 0.454812 | Random |

TABLE VI
ENTROPY VALUES FOR VARIOUS SMARTPHONE CONDITIONS WITH NFC

| N | Entropy | | | Conclusion |
|---|---|---|---|---|
| | *10/4GB* | *10/6GB* | *8/6GB* | |
| 1024 | 3.955636 | 3.95998 | 3.955243 | Random |
| 2048 | 3.955636 | 3.960128 | 3.955243 | Random |
| 4096 | 3.956296 | 3.960702 | 3.955243 | Random |

## V. CONCLUSION

Mobile transaction protocols can be carried out using NFC or QR codes. This research compared the performance of the two, namely processing time and data randomness. The encryption duration for NFC transactions was 1,074 ms, whereas for QR code transactions it was 5.9359 ms. The entropy value on transactions with NFC was 3.96, while the QR code was 3.23. The p-value on transactions with NFC was 0.45, while the QR code was 0.069. The results indicated that both transactions maintain processing times within safe limits, and

the randomness of the data is declared random. Nevertheless, while comparing the values, mobile transactions with NFC showed advantages regarding time and randomness. This research can be advanced by conducting trials on actual transactions using existing protocols. It can also be developed by comparing it with other mobile transactions.

## CONFLICTS OF INTEREST

The authors declare that this research was conducted and written no conflicts of interest.

## AUTHORS' CONTRIBUTIONS

Conceptualization, Lucia Nugraheni Harnaningrum; methodology, Lucia Nugraheni Harnaningrum; software, Kristoforus Nanda Mahardhian; validation, Lucia Nugraheni Harnaningrum; formal analysis, Lucia Nugraheni Harnaningrum; investigation, Lucia Nugraheni Harnaningrum; resources, Kristoforus Nanda Mahardhian; data curation, Kristoforus Nanda Mahardhian; writing—original draft preparation, Kristoforus Nanda Mahardhian; writing—reviewing and editing, Lucia Nugraheni Harnaningrum; visualization, Kristoforus Nanda Mahardhian; supervision, Lucia Nugraheni Harnaningrum; project administration, Kristoforus Nanda Mahardhian.

## REFERENCES

[1] M. Raikar, P.N. Naik, C. Bhavikatti, and S. Shetty, "QR code based patient monitoring system," *Int. Res. J. Eng. Technol.*, vol. 7, no. 5, pp. 7635–7638, May 2020.

[2] T. Cata, P.S. Patel, and T. Sakaguchi, "QR code: A new opportunity for effective mobile marketing," *J. Mob. Technol. Knowl. Soc.*, vol. 2013, pp. 1–7, Aug. 2013, doi: 10.5171/2013.748267.

[3] S. Kamble, "A QR code technology for centralized inventory management system," *Int. Res. J. Eng. Technol.*, vol.8, no. 4, pp. 1537–1540, Apr. 2021.

[4] S. Nseir, N. Hirzallah, and M. Aqel, "A secure mobile payment system using QR code," in *2013 5th Int. Conf. Comput. Sci. Inf. Technol.*, 2013, pp. 111–114, doi: 10.1109/CSIT.2013.6588767.

[5] C. Shuran and Y. Xiaoling, "A new public transport payment method based on NFC and QR code," in *2020 IEEE 5th Int. Conf. Intell. Transp. Eng. (ICITE)*, 2020, pp. 240–244, doi: 10.1109/ICITE50838.2020.9231356.

[6] S.S. Ahamad, "A novel NFC-based secure protocol for merchant transactions," *IEEE Access*, vol. 10, pp. 1905–1920, Dec. 2022, doi: 10.1109/ACCESS.2021.3139065.

[7] S. Chabbi and N.E. Madhoun, "A new security solution enhancing the dynamic array PIN protocol," in *2022 Int. Wirel. Commun. Mob. Comput. (IWCMC)*, 2022, pp. 991–996, doi: 10.1109/IWCMC55113.2022.9825252.

[8] A.B. Barba *et al.*, "Design and manufacture of flexible epidermal NFC device for electrochemical sensing of sweat," in *2022 IEEE Int. Conf. Flex. Printable Sens. Syst. (FLEPS)*, 2022, pp. 1–4, doi: 10.1109/FLEPS53764.2022.9781563.

[9] F. Basic, C.R. Laube, C. Steger, and R. Kofler, "A novel secure NFC-based approach for BMS monitoring and diagnostic readout," in *2022 IEEE Int. Conf. RFID (RFID)*, 2022, pp. 23–28, doi: 10.1109/RFID54732.2022.9795979.

[10] L. Ahmad, R. Al-Sabha, and A. Al-Haj, "Design and implementation of a secure QR payment system based on visual cryptography," in *2021 7th Int. Conf. Inf. Manag. (ICIM)*, 2021, pp. 40–44, doi: 10.1109/ICIM52229.2021.9417129.

[11] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Harlow, United Kingdom: Pearson, 2013.

[12] L.N. Harnaningrum, A. Ashari, and A.E. Putra, "Mobile payment transaction model with robust security in the NFC-HCE ecosystem with secure elements on smartphones," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 8, pp. 160–168, Aug. 2022, doi: 10.14569/IJACSA.2022.0130819.

[13] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Natl. Inst. Stand. Technol. Spec. Publ., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-22rev1a, 2010.

[14] K. Oad, "Reduce the complexity of big number factoring for RSA breaking," M.S. Thesis, Southeast Missouri State University, Cape Girardeau, MO, USA, 2021.

[15] H.M. Bahig *et al.*, "Performance analysis of Fermat factorization algorithms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 12, pp. 340–352, Dec. 2020, doi: 10.14569/IJACSA.2020.0111242.

[16] K. Fan, P. Song, and Y. Yang, "ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," *Mob. Inf. Syst.*, vol. 2017, pp. 1-7, Apr. 2017, doi: 10.1155/2017/2349149.

[17] N.E. Madhoun, E. Bertin, and G. Pujolle, "For small merchants: A secure smartphone-based architecture to process and accept NFC payments," in *2018 17th IEEE Int. Conf. Trust Secur. Priv. Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (Trust./BigDataSE)*, 2018, pp. 403–411, doi: 10.1109/TrustCom/BigDataSE.2018.00067.

[18] A. Al-Haj and M.A. Al-Tameemi, "Providing security for NFC-based payment systems using a management authentication server," in *2018 4th Int. Conf. Inf. Manag. (ICIM)*, 2018, pp. 184–187, doi: 10.1109/INFOMAN.2018.8392832.

[19] N.E. Madhoun, E. Bertin, and G. Pujolle, "An overview of the EMV protocol and its security vulnerabilities," in *2018 Fourth Int. Conf. Mob. Secure Serv. (MobiSecv)*, 2018, pp. 1–5, doi: 10.1109/MOBISECSERV.2018.8311444.

[20] S.S. Ahamad and A.-S.K. Pathan, "Trusted service manager (TSM) based privacy-preserving and secure mobile commerce framework with formal verification," *Complex Adapt. Syst. Model.*, vol. 7, no. 1, pp. 1–18, Dec. 2019, doi 10.1186/s40294-019-0064-z.

[21] A. Al-Mamun, S.S.M. Rahman, T.A. Shaon, and M.A. Hossain, "Security analysis of AES and enhancing its security by modifying s-box with an additional byte," *Int. J. Comput. Netw. Commun.*, vol. 9, no. 2, pp. 69–88, Mar. 2017, doi: 10.5121/ijcnc.2017.9206.

[22] R. Skibba, "Japan's Fugaku supercomputer crushes competition, but likely not for long," *Engineering*, vol. 7, no. 1, pp. 6–7, Jan. 2021, doi: 10.1016/j.eng.2020.12.003.

[23] Y. Kodama, T. Odajima, E. Arima, and M. Sato, "Evaluation of power management control on the supercomputer Fugaku," in *2020 IEEE Int. Conf. Clust. Comput. (CLUST.)*, 2020, pp. 484–493, doi: 10.1109/CLUSTER49012.2020.00069.