SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I5P113

Volume 10 Issue 5, 139-148, May 2023

Original Article

QRIS and GOST: A Symbiotic Approach for Secure QR Code Transactions

Y. Wahyu Agung Prasetyo[1], Robbi Rahim[2], Melda Agnes Manuhutu[3], S Sujito[4]

[1]*Universitas Pertiwi, Jakarta, Indonesia.*
[2]*Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia.*
[3]*Universitas Victory Sorong, Sorong, Indonesia.*
[4]*Universitas Islam Negeri Raden Mas Sahid Surakarta, Surakarta, Indonesia.*

[2]*Coressponding Author : usurobbi85@zoho.com*

Received: 16 March 2023 Revised: 18 April 2023 Accepted: 15 May 2023 Published: 31 May 2023

Abstract *- This study investigates using the GOST encryption algorithm to enhance security within the QRCode Indonesia Standard (QRIS). Given the ubiquity of QR Codes in digital transactions, particularly for Micro, Small, and Medium Enterprises (MSMEs), robust security measures are paramount. We evaluated the GOST algorithm's ability to secure data within the QR Code, converting the code into an encrypted data carrier decipherable only via a specially-equipped QR Code reader. Our findings reveal that the GOST algorithm presents a potent defence mechanism against potential malicious attacks, offering a promising path for QR Code security enhancement. However, the comprehensive application of this measure within QRIS poses challenges, including the need for specialized reader applications and a broader understanding of encryption procedures. Future research opportunities lie in optimizing encryption processes, exploring alternative encryption algorithms, and developing user-friendly, secure QR Code reader applications, which could ultimately support a more secure standard for QR Code usage.*

Keywords *- Cryptography, GOST, Security, QR code, QRIS.*

1. Introduction

The rapid digitization of financial transactions has paved the way for innovative payment systems[1]. QR Codes have gained significant traction worldwide due to their convenience and speed. To streamline digital payments, Indonesia has introduced the QRCode Indonesia Standard (QRIS), a national standard for QR Code payments[2].

Financial technology, called FinTech, has revolutionized how individuals and businesses interact with financial services[3]. This digital transformation has simplified processes and improved accessibility, particularly for Micro, Small, and Medium Enterprises (MSMEs)[4–6]. Given their crucial role in the global economy, MSMEs promote innovation, economic growth, and employment opportunities. They constitute the majority of businesses worldwide and are significant contributors to job creation and economic development[7–9].

However, despite their economic importance, MSMEs often face numerous challenges, including limited access to capital, lack of financial literacy[10], and lack of credit history. This is where FinTech has played a transformative role. By leveraging technologies like blockchain[11], artificial intelligence[12], and data analytics, FinTech has opened up new avenues for MSMEs to access financial services. From digital payments and lending platforms to insurtech and robo-advisors, FinTech solutions have democratized access to financial services, enabling MSMEs to overcome traditional barriers and fueling economic growth [3, 13–15].

Therefore, as we delve into the intricacies of data security in QRIS[2] – an essential aspect of FinTech – we should consider its broader implications on MSMEs and the economy. The focus on data security, particularly in QR code transactions, is critical in ensuring the trust and reliability of FinTech solutions[16], empowering MSMEs to leverage these digital tools effectively and contribute significantly to the economy.

While QR Codes are a game-changer in the digital payment landscape, their widespread use has opened up new avenues for cyber threats[17, 18]. QR Codes can easily be read by anyone using a QR Code scanner, potentially revealing sensitive information or even exposing users to malicious content[19, 20], such as auto-injecting viruses. This presents significant security concerns, particularly for QRIS, given its central role in digital payments in Indonesia.

To mitigate these risks, there is a pressing need to secure the data embedded within QR Codes. One promising solution lies in encryption algorithms[21–23],

which can encode the data in QR Codes so that it can only be deciphered using a specific key. One such algorithm is the GOST (Gosudarstvennyi Standard)[24–26], a Russian encryption standard renowned for its security features.

This study will explore the symbiotic relationship between QRIS and the GOST algorithm, analyzing how the latter can enhance the security of QR Code transactions in Indonesia. By examining the potential of the GOST algorithm to secure QRIS data, we aim to shed light on methods that can help safeguard digital transactions, ultimately contributing to the integrity of the QR Code payment ecosystem in Indonesia.

2. Literature Review

2.1. QR Code and QRIS

QR (Quick Response) Code is a type of 2D barcode that was first created by Denso Wave, a subsidiary of Toyota, in 1994 to track vehicles during manufacturing. It has since expanded its use beyond manufacturing to various sectors, including retail, marketing, and digital payments, owing to its capacity to store a substantial amount of data, which can be quickly scanned and interpreted by a QR code reader, typically a smartphone[27].

QR Codes have become popular in the financial industry as a convenient and cost-effective way to complete digital transactions. They can be read by machines and generated easily, making them suitable for many payment scenarios. Their low cost and ease of implementation have made them famous, especially in emerging nations where the official banking system may be constrained[28, 29].

The QRCode Indonesia Standard (QRIS) standardizes QR codes used in digital payment transactions in Indonesia. The Indonesian Central Bank launched QRIS in 2019. It standardizes QR Code-based payment systems to ensure compatibility amongst payment service providers. Retailers must only show one QR Code (QRIS) for all payment transactions, regardless of the client's payment service provider[30].

QRIS offers convenience and ease of use, but security concerns remain. QR Codes can be viewed by anybody with a scanner, making them vulnerable to criminality, including phishing schemes and data breaches. In a standardized system like QRIS, QR Code transactions must be secured with strict security protocols.

2.2. QR Code Security

As the use of QR Codes in digital transactions increases, so does the need to address the associated security issues. QR Codes, by their very nature, can be easily scanned and interpreted by anyone with a QR Code scanner, which could potentially expose sensitive information to unauthorized individuals[31]

Additionally, the information embedded within QR Codes is not inherently secure. Depending on how they are generated, QR Codes could contain harmful URLs or be used as a medium for spreading malware or other forms of cyber threats[32]. An unsuspecting user might scan a malicious QR Code, leading to unauthorized access to sensitive data, financial loss, or even the spread of malware to the user's device[33]

Furthermore, QR Codes can be tampered with or replaced entirely without the user's knowledge, leading to what is known as QR Code swapping attacks. In this attack, a malicious actor substitutes a legitimate QR Code with a counterfeit one that links to a malicious website, thus deceiving users into providing sensitive information, such as login credentials or payment information[34].

Given these security concerns, exploring and implementing measures that can enhance the security of QR Codes is crucial. One potential solution lies in encryption algorithms, which can encode the data in QR Codes to make it unreadable without a specific key. This approach can help prevent unauthorized access to the information embedded within QR Codes, thus enhancing their security.

The security of QR Codes is critical in the context of standardized QR Code systems like QRIS in Indonesia. Given its widespread use and the sensitive nature of the information involved in digital transactions, ensuring the security of QRIS is paramount.

2.3. Attacks and Weaknesses on QR Codes

Despite the numerous benefits that QR Codes bring to digital transactions, they are not exempt from several types of attacks and inherent weaknesses. These vulnerabilities can lead to significant security risks if not adequately addressed.

2.3.1. QR Code Swapping Attacks

As previously mentioned, one common form of attack is QR Code swapping. This type of attack involves a malicious actor replacing a legitimate QR Code with a counterfeit one, which could lead to harmful websites or prompt the download of malicious software onto the user's device. A comprehensive review by Garg[34] highlighted that these attacks are hazardous due to the ease with which QR Codes can be replaced and the general lack of user awareness about this potential threat.

2.3.2. Phishing Attacks

Phishing attacks are another concern with QR Codes. These attacks typically involve deceptive tactics to trick users into revealing sensitive information. In the context of QR Codes, a malicious actor may generate a QR Code that leads to a fraudulent website designed to mimic a legitimate site, such as a bank or online store. Once the user enters their login credentials or payment information, the attacker can capture this information and use it for illicit purposes[35]

2.3.3. Content Concealment

A significant limitation of QR Codes is the inability of users to authenticate the contents of a QR Code before scanning it. The technology exhibits a constraint in and of itself. As noted by Lin[36], QR Codes can be considered blind links since users are unaware of the destination URL or content until they scan the code. Consequently, the data remains inaccessible to users until they scan the code. The absence of transparency increases the likelihood of inadvertent exposure to hazardous content to consumers.

2.3.4. Denial of Service Attacks

Furthermore, QR Codes can perform Denial of Service (DoS) attacks. In this scenario, an attacker generates a QR Code that, when scanned, overloads the user's device with excessive data or requests, causing the device to slow down or even crash[37]

To mitigate these threats and vulnerabilities, it is crucial to consider security measures[38], such as implementing encryption algorithms, user education, and developing more secure QR Code standards, like QRIS in Indonesia.

2.4. Encryption and the GOST Algorithm

Encryption is crucial in enhancing data security, particularly in the digital space. It involves the process of transforming readable data (plaintext) into an unreadable format (ciphertext), thereby making it inaccessible to unauthorized individuals[39, 40].

A key is required to decipher the data, typically known only to the sender and recipient. This process is reversible, meaning that the ciphertext can be converted back into plaintext using the key, a process known as decryption.

Among the many different encryption algorithms, the GOST (Gosudarstvennyi Standard) algorithm has garnered much interest due to its robust security features. The GOST algorithm is a block cipher that uses symmetric key cryptography. Its inception may be traced back to the times of the Soviet Union. For several decades, the utilization of this encryption has been observed within the Russian government[41]. The algorithm in question provides considerable security due to its utilization of 64-bit blocks and a 256-bit key length, as detailed in the reference[25].

The GOST encryption algorithm is widely recognized for its strength and resilience against conventional cryptographic attacks such as differential and linear cryptanalysis, as documented in reference[42].

This can be attributed to the origin of its development by the Russian government. Notwithstanding its durability, the algorithm's speed and efficiency are significantly contingent on its implementation, rendering it potentially less expeditious than other widely utilized encryption techniques like AES (Advanced Encryption Standard)[43].

In the context of QR Codes, encryption algorithms like GOST can secure the data embedded within the codes, enhancing their security. Encrypting the data before it is encoded into the QR Code prevents unauthorized individuals or systems from accessing the sensitive information contained within the codes. However, the specific application of the GOST algorithm to enhance the security of QR Code transactions, particularly in the context of QRIS, is an area that warrants further exploration.

2.5. GOST Algorithm

The GOST encryption algorithm is a symmetric key block cipher, which uses the same key for both the encryption and decryption processes[24]. The algorithm operates on 64-bit data blocks with a key length of 256 bits, providing a high-security level. Here is a brief outline of the GOST encryption process:

- Key Setup: The 256-bit encryption key is divided into eight 32-bit subkeys.
- Data Division: The plaintext data to be encrypted is divided into 64-bit blocks. If the last data block is less than 64 bits, it is padded to meet the 64-bit requirement.
- Initial Substitution: Each 64-bit block is divided into two 32-bit halves. The left half is passed through a substitution box (S-box), a lookup table designed to obscure the relationship between the key and the ciphertext.
- Key Mixing: The output of the S-box is added to one of the 32-bit subkeys (modulo 2^32), which further scrambles the data.
- Permutation: The result of the key mixing is then subjected to a permutation, which reorders the bits to create the final 32-bit output of the round.
- Iteration: Steps 3-5 are repeated eight times for each 64-bit block, each round using a different subkey. After eight rounds, the two halves of the block are swapped.
- Final Swap: After 32 rounds (four iterations of the eight-round process), the two halves of the block are swapped one last time to create the final 64-bit ciphertext block.

The decryption process is essentially the reverse of the encryption process, using the same subkeys in reverse order. While the GOST algorithm is known for its robust security features, it should be noted that its security largely depends on the security of the key and the choice of the S-boxes. If the key is compromised or weak S-boxes are used, the security of the encrypted data could be compromised[25]. Here is a summary of the GOST algorithm's key features:

Table 1. Advantages and disadvantages GOST algorithm

Advantages	Disadvantages
High Security: The GOST algorithm operates on 64-bit blocks and uses a key length of 256 bits, providing a high level of security	**Complexity**: Encrypting and decrypting data with the GOST algorithm can be complex and computationally intensive, especially compared to other encryption standards.
Resilience Against Attacks: The GOST algorithm is resistant to common cryptographic attacks such as differential and linear cryptanalysis	**Speed and Efficiency**: The speed and efficiency of the GOST algorithm depend heavily on the implementation, making it potentially slower than other widely used encryption standards such as AE
Symmetric Encryption: As a symmetric encryption algorithm, GOST uses the same key for both encryption and decryption, simplifying key management	**Key Management**: While symmetric encryption simplifies vital management, it also requires secure essential exchange methods to prevent the key from being intercepted.
Flexibility: The GOST algorithm allows for using different S-boxes, providing flexibility in its implementation.	**S-Box Selection**: The security of the GOST algorithm can be compromised if weak S-boxes are used, highlighting the importance of careful S-box selection.
Longevity: Having been used by the Russian government for several decades, the GOST algorithm has proven its longevity in data encryption.	**Limited Research**: Compared to more globally recognized encryption standards such as AES, relatively limited research is available on the GOST algorithm, particularly in the context of QR Code security.

Few researchers have contributed significantly to the understanding of the GOST algorithm.

a. Vincent Rijmen and Elisabeth Oswald[44]: Rijmen and Oswald likely analyzed the performance and security of the GOST cipher, possibly in comparison to other encryption standards.
b. Nicolas T. Courtois[45]: These researchers likely conducted a cryptanalysis of the GOST block cipher, exploring its vulnerability to related-key attacks.
c. Bingke Ma[46]: Known for his work on block ciphers and cryptographic protocols, Ma have analyzed the implementation of GOST in different cryptographic protocols and its potential security flaws.
d. Ardabek Khompysh[47]: These researchers are known for their work in the design of S-boxes, a crucial component of many block ciphers, including GOST, where his work involved analyzing and improving the design of S-boxes used in GOST.

3. Methods

In the methodology section of our study, we will discuss two primary components: QRIS (QRCode Indonesia Standard) and the GOST Algorithm. QRIS is a standard set by Bank Indonesia that ensures interoperability and standardization in using QR Codes for payment transactions. All payment service providers in Indonesia are required to adopt QRIS for their QR Code-based payment services. The QRIS generates a QR Code containing the information necessary for a transaction. This information includes the identity of the merchant, the transaction amount, and other necessary data. The customer can scan the QR Code and authorize the payment using a mobile application.

The GOST Algorithm is a symmetric key block cipher developed in the Soviet Union that operates on 64-bit data blocks with a key length of 256 bits. It was published in 1989 and has been used widely in Russia since. A symmetric key algorithm uses the same key for encryption and decryption processes.

In the context of this study, the GOST Algorithm will be used to secure the data contained within the QR Code. This data will be encrypted using the algorithm before being embedded in the QR Code. To read the data, the customer's application must first decrypt it using the same key. The feasibility and security of using the GOST Algorithm In summary, this methodology will involve a combination of practical implementation and theoretical analysis to assess in the context of QRIS.

4. Result and Discussion

Many merchants currently use QR Code to conduct cashless transactions to facilitate payment procedures, to support these transactions, there is a need for the security of data stored in the QR Code and read with unique applications that have been combined with specific algorithms. In this case, the GOST Algorithm. There are several steps in securing QR Code data:

a. Making and determining S-Boxes
b. Key Formation
c. Data Encryption Process
d. Data Decryption Process

The results of tests carried out in several stages to test the data that is secured:

Formation of S-Box: The process of forming an SBox is essential to produce a vital key. In this test, the S-Box table can be seen in the picture with an output S-box value of 7.

Table 2. S-Box value

Tabel S -BOX	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S -BOX (0)	4	10	9	2	13	8	0	14	6	11	12	12	7	15	5	3
S -BOX (1)	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
S -BOX (2)	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
S -BOX (3)	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
S -BOX (4)	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
S -BOX (5)	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
S -BOX (6)	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
S -BOX (7)	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

Key Generation:

Key = ‘mdpi is the best publishers mdpi’
Change the key to binary form.
'm' = 109 = 01101101 = 6D
'd' = 100 = 01100100 = 64
'p' = 112 = 01110000 = 70
'i' = 105 = 01101001 = 69
' ' = 32 = 00100000 = 20
'i' = 105 = 01101001 = 69
's' = 115 = 01110011 = 73
' ' = 32 = 00100000 = 20
't' = 116 = 01110100 = 74
'h' = 104 = 01101000 = 68
'e' = 101 = 01100101 = 65
' ' = 32 = 00100000 = 20
'b' = 98 = 01100010 = 62
'e' = 101 = 01100101 = 65
's' = 115 = 01110011 = 73
't' = 116 = 01110100 = 74
' ' = 32 = 00100000 = 20
'p' = 112 = 01110000 = 70
'u' = 117 = 01110101 = 75
'b' = 98 = 01100010 = 62
'l' = 108 = 01101100 = 6C
'i' = 105 = 01101001 = 69
's' = 115 = 01110011 = 73
'h' = 104 = 01101000 = 68
'e' = 101 = 01100101 = 65
'r' = 114 = 01110010 = 72
's' = 115 = 01110011 = 73
' ' = 32 = 00100000 = 20
'm' = 109 = 01101101 = 6D
'd' = 100 = 01100100 = 64
'p' = 112 = 01110000 = 70
'i' = 105 = 01101001 = 69

Key conversion results into binary form = (k(1), k(2), k(3), ... , k(256))=
01101101011001000111000001101001001000000011010010111001100100000011101000110100001100101001000000011000100110010101110011011101000001000000111000000111010101100010011011000110100101110011001000111001100100000011011010110010000111001000001101001 =
6D6470692069732074686520626573742070756261697368657273206D647069

Group the results obtained in K 0 - 7
K – 0 = 10010110000011100010011010110110 = 960E26B6
K – 1 = 00000100110011101001011000000100 = 04CE9604
K – 2 = 00000100101001100001011000101110 = 04A6162E
K – 3 = 00101110110011101010011001000110 = 2ECEA646
K – 4 = 01000110101011100000111000000100 = 46AE0E04
K – 5 = 00010110110011101001011000110110 = 16CE9636
K – 6 = 00000100110011100100111010100110 = 04CE4EA6
K – 7 = 10010110000011100010011010110110 = 960E26B6

Key K (0) - K (7) will be used for the encryption-decryption process.

Encryption Process:

ENCRYPTION ROUND 0
(1) PLAIN TEXT = 'microsof'
Hex Conversion = 6D6963726F736F66
L(0) = 66F6CEF6
R(0) = 4EC696B6
(2) R(0) + K(0) mod 2^32
R(0) = 1321637558
K(0) = 2517509814
-------------------------------- +
Result = 3839147372 mod 2^32
= 3839147372
= E4D4BD6C

(3) Split into eight groups and enter into SBox.

(4) The results are combined again, and do Rotate Left Shift 11 times.

RotateLeftShift(1)=AC01D8AC
RotateLeftShift (2)=5803B159
RotateLeftShift (3)=B00762B2
RotateLeftShift (4)=600EC565
RotateLeftShift (5)=C01D8ACA
RotateLeftShift (6)=803B1595

RotateLeftShift (7)=00762B2B
RotateLeftShift (8)=00EC5656
RotateLeftShift (9)=01D8ACAC
RotateLeftShift (10)=03B15958
RotateLeftShift (11)=0762B2B0

(5) R(1) = R(0) XOR L(0)
R(0) = 0762B2B0
L(0) = 66F6CEF6
---------- XOR
R(1) = 61947C46

(6) L(1) = R(0) before process
L(1) = 4EC696B6

ENCRYPTION Round 1
(1) L(1) = 4EC696B6
R(1) = 61947C46

(2) R(1) + K(1) mod 2^32
R(1) = 1637121094
K(1) = 80647684
---------- +
Result = 1717768778 mod 2^32

= 1717768778
= 6663124A

(3) Split into eight groups and enter into SBox.

6 = 6 -> SBOX(0) -> 0 = 0
6 = 6 -> SBOX(1) -> 15 = F
6 = 6 -> SBOX(2) -> 4 = 4
3 = 3 -> SBOX(3) -> 1 = 1
1 = 1 -> SBOX(4) -> 12 = C
2 = 2 -> SBOX(5) -> 10 = A
4 = 4 -> SBOX(6) -> 3 = 3
A = 10 -> SBOX(7) -> 3 = 3

(4) The results are combined again, and do Rotate Left Shift 11 times.
RotateLeftShift (1)=1E839466
RotateLeftShift (2)=3D0728CC
RotateLeftShift (3)=7A0E5198
RotateLeftShift (4)=F41CA330
RotateLeftShift (5)=E8394661
RotateLeftShift (6)=D0728CC3
RotateLeftShift (7)=A0E51987
RotateLeftShift (8)=41CA330F
RotateLeftShift (9)=8394661E
RotateLeftShift (10)=0728CC3D
RotateLeftShift (11)=0E51987A
(5) R(2) = R(1) XOR L(1)
R(1) = 0E51987A
L(1) = 4EC696B6
---------- XOR
R(2) = 40970ECC
(6) L(2) = R(1) before process
L(2) = 61947C46

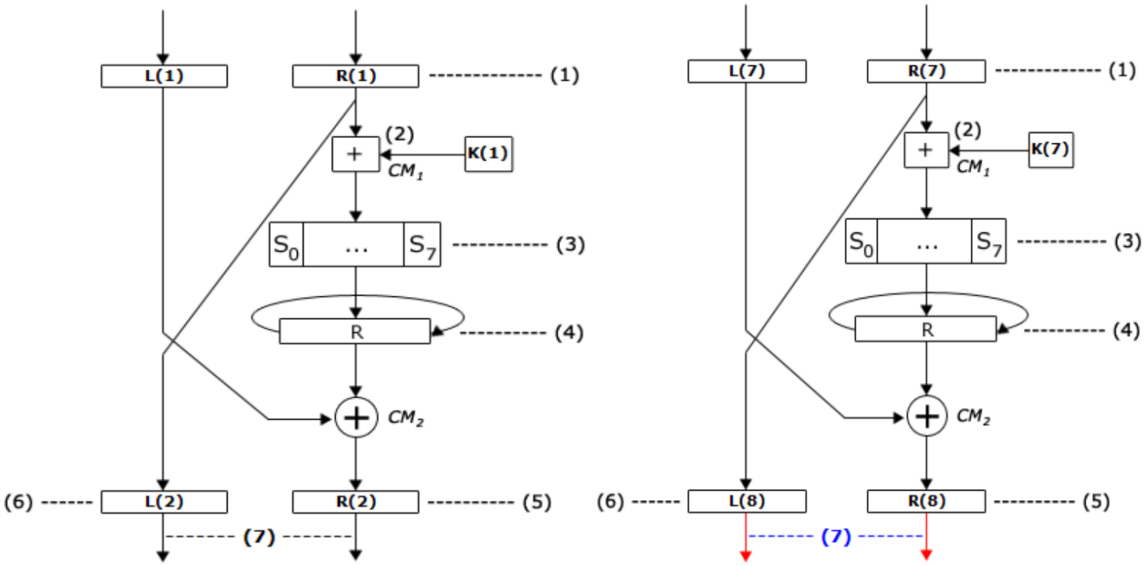

Fig. 1 Encryption process diagram

The encryption process will be carried out 32 times, with the final result in the form of ciphertext as follows:

Hex Result= C619BDF2C9A85D0F
CIPHER TEXT = Æ½òÉ¨]
Decryption Process
Decryption Round 0

(1) CIPHER TEXT = 'Æ½òÉ¨]'
Hex = C619BDF2C9A85D0F
L0 = F0BA1593
R0 = 4FBD9863

(2) R0 + K0 mod 2^32
R0 = 1337825379
K0 = 2517509814
---------- +
Result = 3855335193 mod 2^32
= 3855335193
= E5CBBF19

(3) Split into eight groups and enter into SBox.

(4) The results are combined again, and do Rotate Left Shift 11 times.
RotateLeftShift(1)=BAD9DD64
RotateLeftShift(2)=75B3BAC9
RotateLeftShift(3)=EB677592
RotateLeftShift(4)=D6CEEB25

RotateLeftShift(5)=AD9DD64B
RotateLeftShift(6)=5B3BAC97
RotateLeftShift(7)=B677592E
RotateLeftShift(8)=6CEEB25D
RotateLeftShift(9)=D9DD64BA
RotateLeftShift(10)=B3BAC975
RotateLeftShift(11)=677592EB
(5) R(1) = R(0) XOR L(0)
R(0) = 677592EB
L(0) = F0BA1593
---------- XOR
R(1) = 97CF8778
(6) L(1) = R(0) before process.
L(1) = 4FBD9863

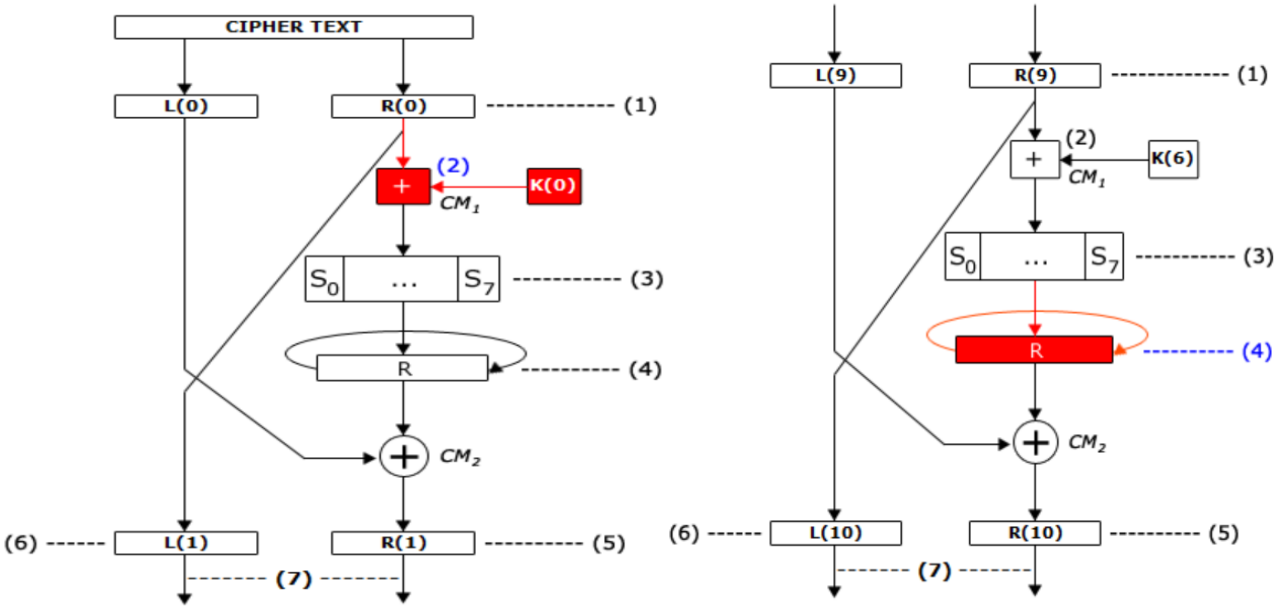

Fig. 2 Decryption process diagram

This decryption has 32 round, too when all process is done, it will show the result below:
Hex Result= 6D6963726F736F66
PLAIN TEXT = microsof

5. Conclusion

The security of QR Codes, particularly in the context of QRIS, the QR Code standard in Indonesia, is a significant concern given the ubiquity and importance of these codes in our rapidly digitizing world. As our study has shown, using the GOST algorithm for encrypting the data embedded in QR Codes presents a robust solution to enhance security measures.

Our exploration into the GOST algorithm demonstrated its feasibility for securing data within the QR Code. Its symmetric key cipher provides a sturdy defence, ensuring that encrypted data can only be deciphered with the correct key. In this model, the QR Code becomes a carrier of encrypted data, requiring a specially-equipped QR Code reader application for decryption and access to the information within. This added layer of security significantly diminishes the risk of malicious attacks, thereby protecting both the users and merchants relying on QR Code transactions.

While our study signals promise in this field, it also underscores that comprehensive implementation of such a security measure within QRIS will require more time and resources. The need for specialized QR Code reader applications, an understanding of the encryption and decryption process, and a wide-scale adaptation to these enhanced security procedures pose challenges. However, they are essential steps in developing a safer and more secure standard for QR Code usage.

Looking ahead, there is vast potential for further research in this area. Future studies could optimize the encryption and decryption processes to make them faster and more efficient. This could be particularly relevant considering the need for quick transactions in many QR Code usage scenarios.

Moreover, the research could explore alternative encryption algorithms used in conjunction with or as alternatives to the GOST algorithm. We could develop even more robust and efficient security solutions by investigating different options. Additionally, studies could delve deeper into user behaviour and QR Code security perceptions. Understanding users' awareness, trust, and willingness to use encrypted QR Codes could offer valuable insights for developing and implementing security measures.

Finally, research on developing user-friendly, secure QR Code reader applications could contribute significantly. A simple, intuitive, yet secure application could bridge the gap between advanced security procedures and widespread user adoption. All these potential research directions underscore the importance and relevance of our study and signal the exciting avenues for future exploration in the realm of QR Code security.

References

[1] Maziyar Ghasemi et al., "The Impact of Information Technology (IT) on Modern Accounting Systems," *Procedia - Social and Behavioral Sciences*, vol. 28, pp. 112–116, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[2] I Kadek Dwi Perdana, and Ni Kadek Sinarwati, "Penerapan Transaksi Payment Gateway Berbasis QRIS Pada UMKM (Study Empiris Pada Pedagang di Pantai Penimbangan)," *Bisma: Jurnal Manajemen*, vol. 8, no. 2, pp. 331–337, 2022. [Google Scholar] [Publisher Link]

[3] Diah Rahayu Ningsih, "Peran Financial Technology (Fintech) Dalam Membantu Perkembangan Wirausaha Umkm," *Prosiding Seminar Nasional Pendidikan Program Pascasarjana Universitas Pgri Palembang*, pp. 70–277, 2020. [Google Scholar] [Publisher Link]

[4] M. Indre Wanof , and Abdul Gani, "MSME Marketing Trends in the 4.0 Era: Evidence from Indonesia," *Apollo: Journal of Tourism and Business*, vol. 1, no. 2, pp. 36–41, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[5] Abu Muna Almaududi Ausat, Tareq Al Bana, Gadzali, Silvy Sondari Gadzali, "Basic Capital of Creative Economy: The Role of Intellectual, Social, Cultural, and Institutional Capital," *Apollo: Journal of Tourism and Business*, vol. 1, no. 2, pp. 42–54, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Uce Karna Suganda, Nanang Rohman, "Analysis of the Factors that Influence the Competitive Advantage of SMEs in the City of Bandung," *Quantitative Economics and Management Studies*, vol. 4, no. 1, pp. 75–83, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] RahayuPuji Suci et al., "Performance Maximization Strategy of Micro, Small & Medium Enterprises Through the Implementation of Quality of Work Life and Job Involvement," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 11, no. 8, pp. 2933–2942, 2019. [Publisher Link]

[8] Joshua Seth Bruhn et al, *MSME FINANCE GAP: Assessment of the Shortfalls and Opportunities in Financing Micro, Small and Medium Enterprises in Emerging Markets*, International Finance Corporation, 2017. [Google Scholar] [Publisher Link]

[9] Rahmaini Rahmaini et al., "Comparison Analysis of Seismic Base Shear 23 Regencies in Aceh Province Based on SNI 03-1726-2012 and SNI 03-1726-2019," *International Journal of Engineering, Science and Information Technology*, vol. 2, no. 3, pp. 83–89, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[10] Agus Dedi Subagja, "Analysis of Factors Leading to E-commerce Adoption," *Apollo: Journal of Tourism and Business*, vol. 1, no. 1, pp. 1–5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Embracing the E-Commerce Revolution in Asia and the Pacific, Asian Development Bank, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] Emmanuel Mogaji, and Nguyen Phong Nguyen, "Managers' Understanding of Artificial Intelligence about Marketing Financial Services: Insights from a Cross-Country Study," *International Journal of Bank Marketing*, vol. 40, no. 6, pp. 1272-1298, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Nemoto, Naoko, and Yoshino, Naoyuki, "Fintech for Asian SMEs," *Asian Development Bank Institute*, 2019. [Google Scholar] [Publisher Link]

[14] Otoritas Jasa Keuanga, "*MSMEs through FinTech Financial Inclusion for Supporting*," Otoritas Jasa Keusngan, 2020. [Publisher Link]

[15] Chidiebere U. Enukoha et al., "ICT Revolutions in the Banking Sector of Nigeria: Determinants of E-Payment Channels By Customers," *Quantitative Economics and Management Studies*, vol. 3, no. 5, pp. 680–690, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] Fasih Ur Rehman et al., "Data Defense: Examining Fintech's Security and Privacy Strategies," *Engineering Proceedings -2nd International Conference on Emerging Trends in Electronic and Telecommunication Engineering*, vol. 32, no. 1, pp. 3, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Surya Tjahyadi, "Development Of QR Code-Based Data Sharing Web Application using System Development Life Cycle Method," *Journal of Information System and Technology*, vol. 2, no. 2, pp. 64–73, 2021. [Google Scholar] [Publisher Link]

[18] Shruti Ahuja, "QR Codes and Security Concerns," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 3, pp. 3878-3879, 2014. [Google Scholar] [Publisher Link]

[19] Abbas M. Al-Ghaili et al., "QR Code-Based Authentication Method for IOT Applications using Three Security Layers," *Telecommunication Computing Electronics and Control (TELKOMNIKA)*, vol. 18, no. 4, pp. 2004-2011, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Krassie Petrova et al., "QR Codes Advantages and Dangers," *Proceedings of the 13th International Joint Conference on E-Business and Telecommunications*, pp. 112–115, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[21] M. Indrasena Reddy, A.P. Siva Kumar, and K. Subba Reddy, "A Secured Cryptographic System Based on DNA and a Hybrid Key Generation Approach, *Biosystems*, vol. 197, pp. 104207, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] Wenbo Mao, Modern Cryptography: Theory and Practice, 2023. [Online]. Available: https://www.amazon.in/Modern-Cryptography-paperback-Hewlett-Packard-Professional/dp/013288741X
[23] Ahmad Syahir, and Chuah Chai Wen, "Secure Login Mechanism for Online Banking," *International Journal on Informatics Visualization*, vol. 2, no. 3–2, pp.179-183, 2018. [CrossRef] [Publisher Link]
[24] Heri Nurdiyanto et al., "Enhanced Pixel Value Differencing Steganography with Government Standard Algorithm," *3rd International Conference on Science in Information Technology (ICSITech)*, pp. 366–371, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[25] Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS), 2006. [Online]. Available : https://datatracker.ietf.org/doc/html/rfc4490
[26] Muhammad Iqbal, Yudi Sahputra, and Andysah Putera Utama Siahaan, "The Understanding of GOST Cryptography Technique," *International Journal of Engineering Trends and Technology*, vol. 39, no. 3, pp.168–172, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[27] Ela Sibel Bayrak Meydanoglu, "QR Code: An Interactive Mobile Advertising Tool," *International Journal of Business and Social Research*, vol. 3, no. 9, pp. 26–32, 2013. [Google Scholar] [Publisher Link]
[28] Naura Nafisa et al., "Quick Response Code Indonesian Standard (QRIS) Payment in Indonesian MSMEs: A Bibliometric Study," *Journal of Pharmaceutical Negative Results*, vol. 13, no. 10, pp. 1223–1233, 2022. [Google Scholar] [Publisher Link]
[29] Ming Tu et al., "The Adoption of QR Code Mobile Payment Technology During COVID-19: A Social Learning Perspective," *Frontiers in Psychology*, vol. 12, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[30] Luh Putu Mahyuni, and I Wayan Arta Setiawan, "How does QRIS Attract Msmes ? A Model to Understand the Intentions of SMES using QRIS," *FORUM EKONOMI: Jurnal Ekonomi, Manajemen dan Akuntansi*, vol. 23, no. 4, pp. 735-747, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[31] Jeevan M. Meruga et al., "Multi-Layered Covert QR Codes for Increased Capacity and Security," *International Journal of Computers and Applications*, vol. 37, no. 1, pp. 17–27, 2015. [CrossRef] [Google Scholar] [Publisher Link]
[32] Heider A. M. Wahsheh, and Flaminia L. Luccio, "Security and Privacy of QR Code Applications: A Comprehensive Study, General Guidelines and Solutions," *Information*, vol. 11, no. 4, p. 217, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[33] Ryan Randy Suryono, Indra Budi, and Betty Purwandari, "Challenges and Trends of Financial Technology (Fintech): A Systematic Literature Review," *Information*, vol. 11, no. 12, p. 590, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[34] Pulkit Garg et al., "Security and Privacy Issues Related to Quick Response Codes," *Advances in Digital Forensics XVII*, pp. 255–267, 2021. [CrossRef] [Google Scholar] [Publisher Link]
[35] M. Taraka Rama Mokshagna Teja, and K. Praveen, "Prevention of Phishing Attacks using QR Code Safe Authentication," *Inventive Computation and Information Technologies*, vol. 336, pp. 361–372, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[36] Pei-Yu Lin et al., "A Confidential QR Code Approach with Higher Information Privacy," *Entropy*, vol. 24, no. 2, pp. 284, 2022. [CrossRef] [Google Scholar] [Publisher Link]
[37] Tasnuva Mahjabin et al., "A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques," *International Journal of Distributed Sensor Networks*, vol. 13, no. 12, 2017. [CrossRef] [Google Scholar] [Publisher Link]
[38] Pooja Khandare, Sanjay Deokar, and Aarti Dixit, "Improvement of Traditional Protection System in the Existing Hybrid Microgrid with Advanced Intelligent Method," *International Journal of Data Science*, vol. 1, no. 2, pp. 72–81, 2020. [CrossRef] [Google Scholar] [Publisher Link]
[39] Philip R Zimmermann, *The official PGP user's guide*, MIT Press, vol. 5, 1995. [Online]. Available : https://web.pa.msu.edu/reference/pgpdoc1.html
[40] Rara Audia Utami et al., "Web-Based of The Regency Apparatus Work Unit Application at the Communications, Informatics, and Encryption Service of Bireuen Regency in Aceh Province," *International Journal of Engineering, Science and Information Technology*, vol. 2, no. 4, pp. 162–171, 2022. [Google Scholar] [Publisher Link]
[41] Ludmila Babenko, and Ekaterina Maro, "Algebraic Cryptanalysis of GOST Encryption Algorithm," *Journal of Computer and Communications*, vol. 2, pp. 10–17, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[42] Tonni Limbong et al., "The Implementation of Computer-Based Instruction Model on Gost Algorithm Cryptography Learning," *IOP Conference Series: Materials Science and Engineering*, vol. 420, pp. 012094, 2018. [CrossRef] [Google Scholar] [Publisher Link]
[43] Pratiksha Sethi, and V. Kapoor, "A Proposed Novel Architecture for Information Hiding in Image Steganography by using Genetic Algorithm and Cryptography," *Procedia Computer Science*, vol. 87, pp. 61–66, 2016. [CrossRef] [Google Scholar] [Publisher Link]
[44] Vincent Rijmen, and Elisabeth Oswald, "Update on SHA-1," *Topics in Cryptology – CT-RSA 2005*, pp. 58–71, 2005. [CrossRef] [Google Scholar] [Publisher Link]
[45] Nicolas T. Courtois, "Cryptanalysis of Two GOST Variants with 128-Bit Keys," *Cryptologia*, vol. 38, no. 4, pp. 348–361, 2014. [CrossRef] [Google Scholar] [Publisher Link]
[46] Bingke Ma et al., "Improved Cryptanalysis on Reduced-Round GOST and Whirlpool Hash Function," *Applied Cryptography and Network Security*, pp. 289–307, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[47] Ardabek Khompysh et al., "Design of Substitution Nodes (S-Boxes) of a Block Cipher Intended for Preliminary Encryption of Confidential Information," *Cogent Engineering*, vol. 9, no. 1, pp. 1-14, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[48] P.Priya, and R.Jayakumar, "Cryptography Based Privacy Preserving Data Transmission in Hybrid Wireless Networks," *International Journal of Computer & organization Trends (IJCOT)*, vol. 6, no. 6, pp. 5-9, 2016. [Publisher Link]

[49] Koji Nagata, Do Ngoc Diep, and Tadao Nakamura, "Quantum Cryptography Based on An Algorithm of Determining all the Mappings of a Function," *International Journal of P2P Network Trends and Technology*, vol. 9, no. 6, pp. 1-4, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[50] Hamza Faham et al., "A New Fast Iterative Decoder of Product Codes Based on Hash and Syndromes and Optimized by Genetic Algorithms," *International Journal of Engineering Trends and Technology*, vol. 70, no. 12, pp. 289-295, 2022. [CrossRef] [Publisher Link]

[51] Abdülkadir Çakir, and Seyit Akpancar, "ROS-Based Control of the DJI Matrice 100 Robot with QR Images Obtained from DJI Guidance," *International Journal of Engineering Trends and Technology*, vol. 68, no. 1, pp. 45-50, 2020. [CrossRef] [Google Scholar] [Publisher Link]