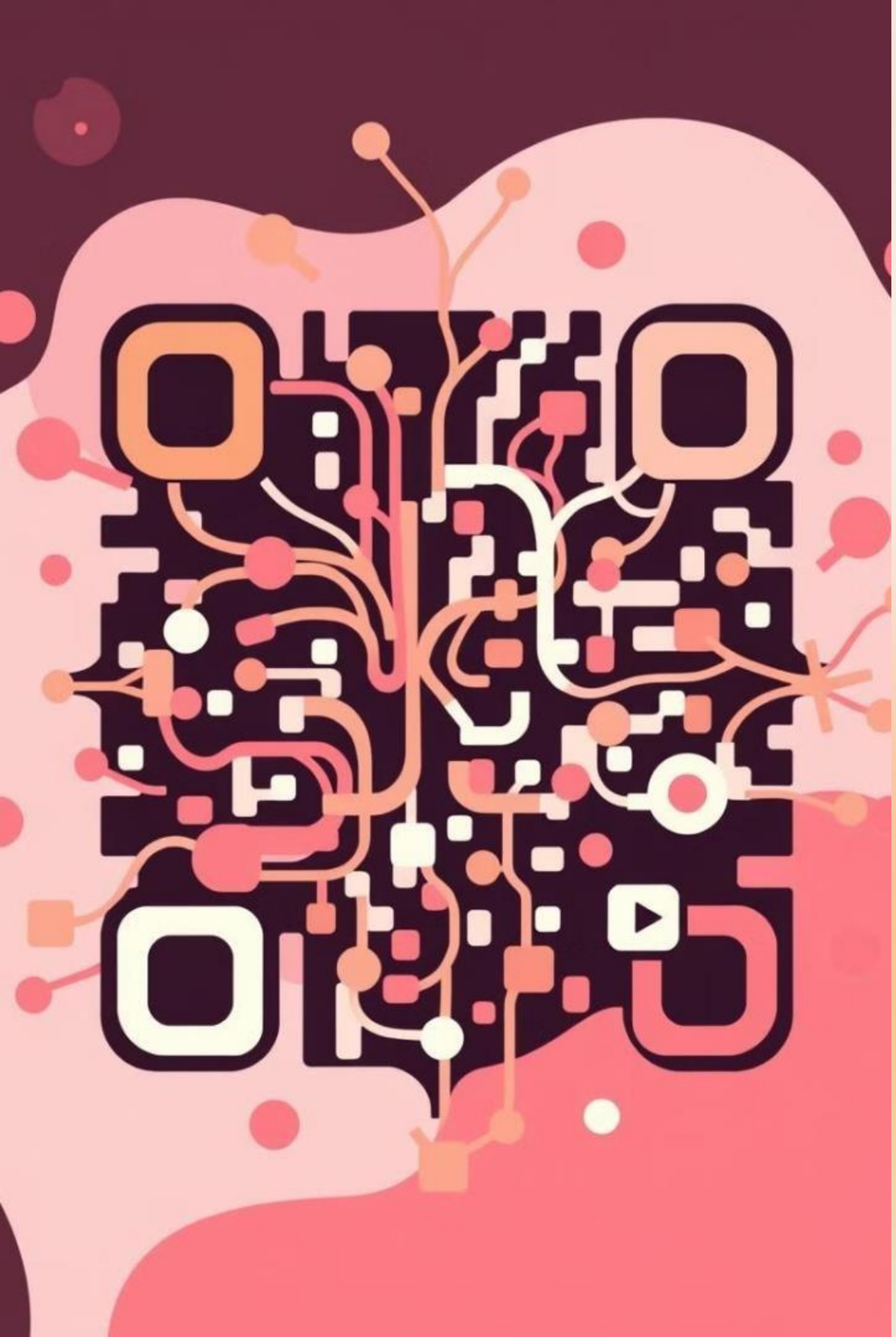
Secure QR Code Detection and Decoding Using Cryptographic Algorithms

By

N. SAI SARANYA(192210441)

V. KAVYANJALI(192210218)

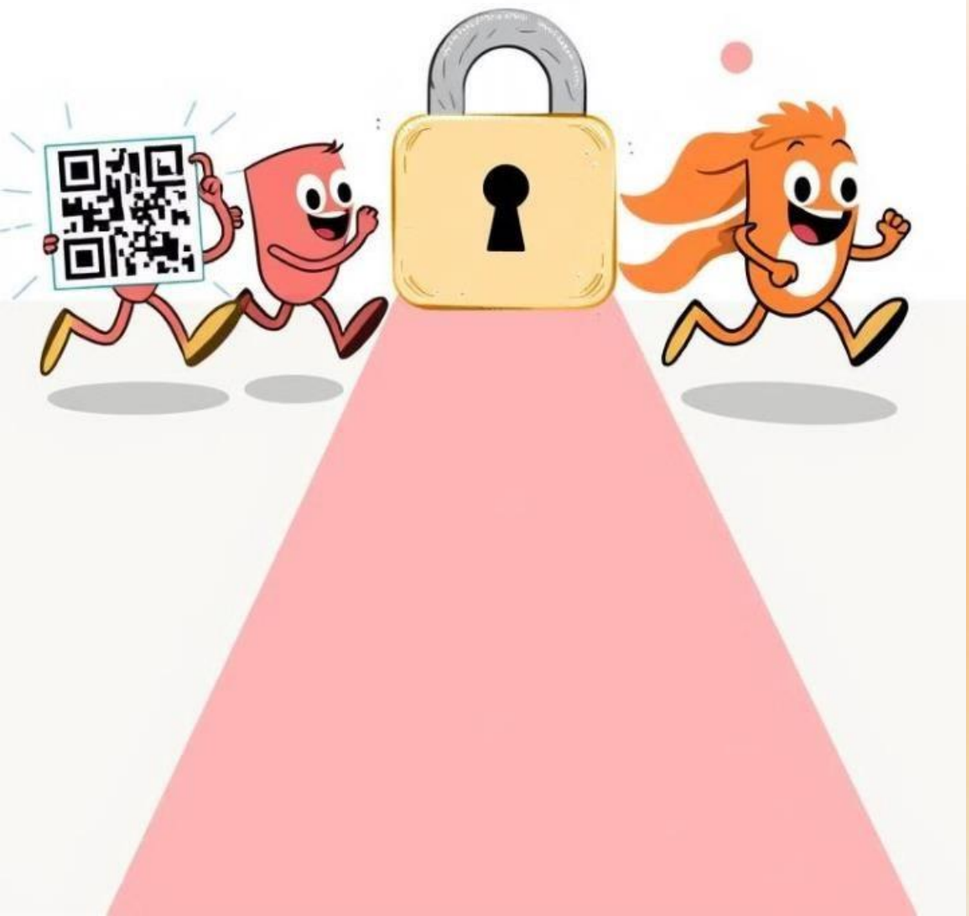


Abstract

- QR codes are extensively used for encoding data due to their efficiency and versatility.
- This study introduces a method combining QR code detection with cryptographic algorithms to enhance security.
- The system employs advanced image processing techniques for accurate QR code recognition under varying conditions.
- Cryptographic algorithms ensure secure decoding, preventing unauthorized access or tampering.
- Experimental results demonstrate improved accuracy, and security of the proposed method.
- The approach is suitable for applications in finance, healthcare, and secure communications.

Introduction

- QR codes are widely used due to their ability to store large amounts of data in a compact and machine-readable format.
- Common applications include payments, product tracking, healthcare, and authentication.
- As QR codes are increasingly used in secure operations (e.g., financial transactions), robust mechanisms are essential to prevent data breaches Cryptographic algorithms ensure secure encoding and decoding, protecting the integrity and confidentiality of QR code data.
- These methods can prevent unauthorized access or tampering during the decoding process.
- This paper explores an integrated approach combining image processing techniques for QR code detection with cryptographic algorithms for secure decoding.
- The proposed system enhances both accuracy and security, addressing existing limitations in traditional QR code systems.



Objective

- **Protect Data**: Ensure sensitive data in QR codes is encrypted and secure.
- **Maintain Integrity**: Prevent data from being altered or tampered with.
- **Ensure Privacy**: Only authorized users can decrypt and access the information.
- **Prevent Misuse**: Avoid QR code tampering or spoofing.
- **Accurate Decoding**: Enable reliable scanning and decryption of QR codes.
- **Support Secure Applications**: Use in payments, authentication, and data sharing safely.

Security Challenges

1 **key management issues**

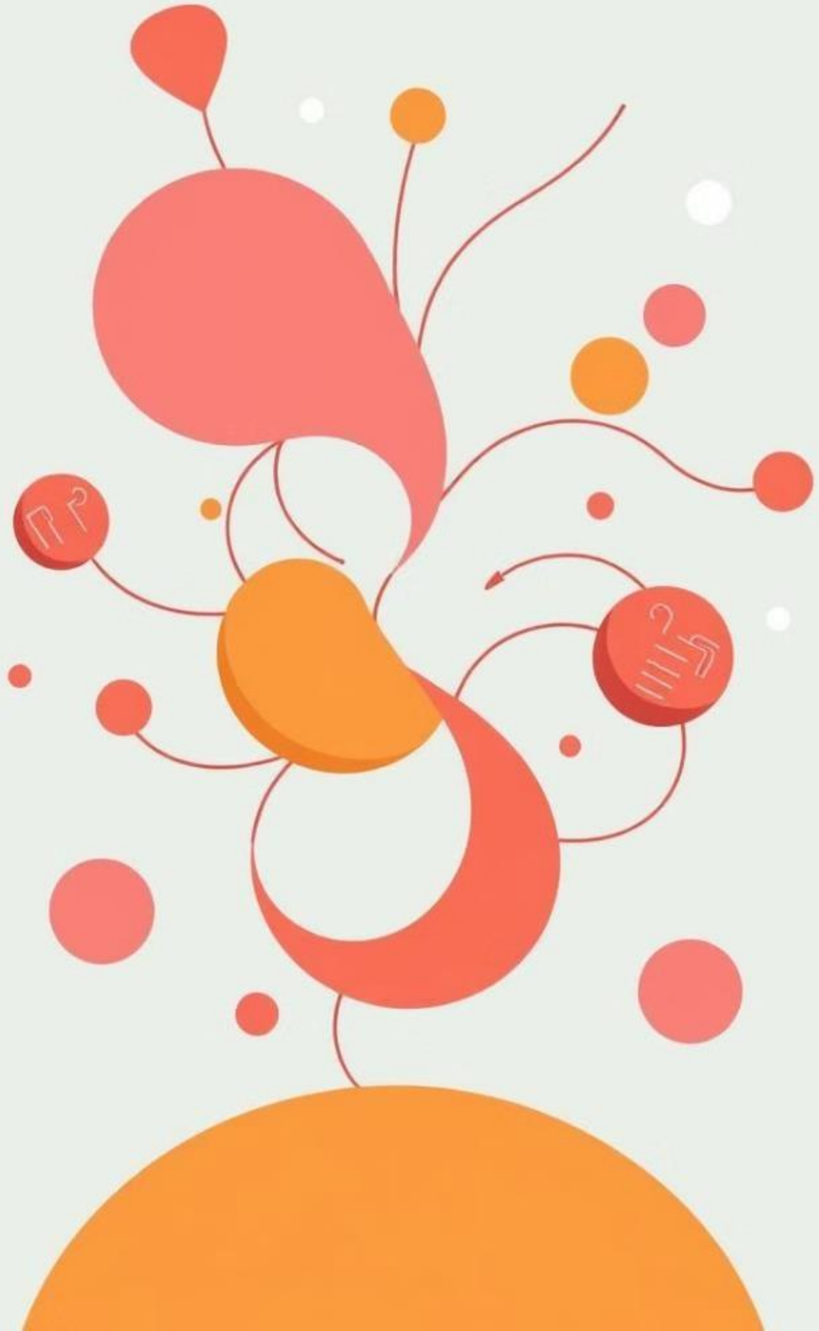
If encryption keys are poorly managed or exposed, attackers could decrypt sensitive information.

2 **Data Leakage**

Without proper security measures, sensitive information stored in QR codes could be intercepted and misused.

3 **Accessibility Challenges**

If QR codes use advanced security mechanisms older devices may fail to decode them.



Cryptographic Algorithms for QR Code Security

Hashing

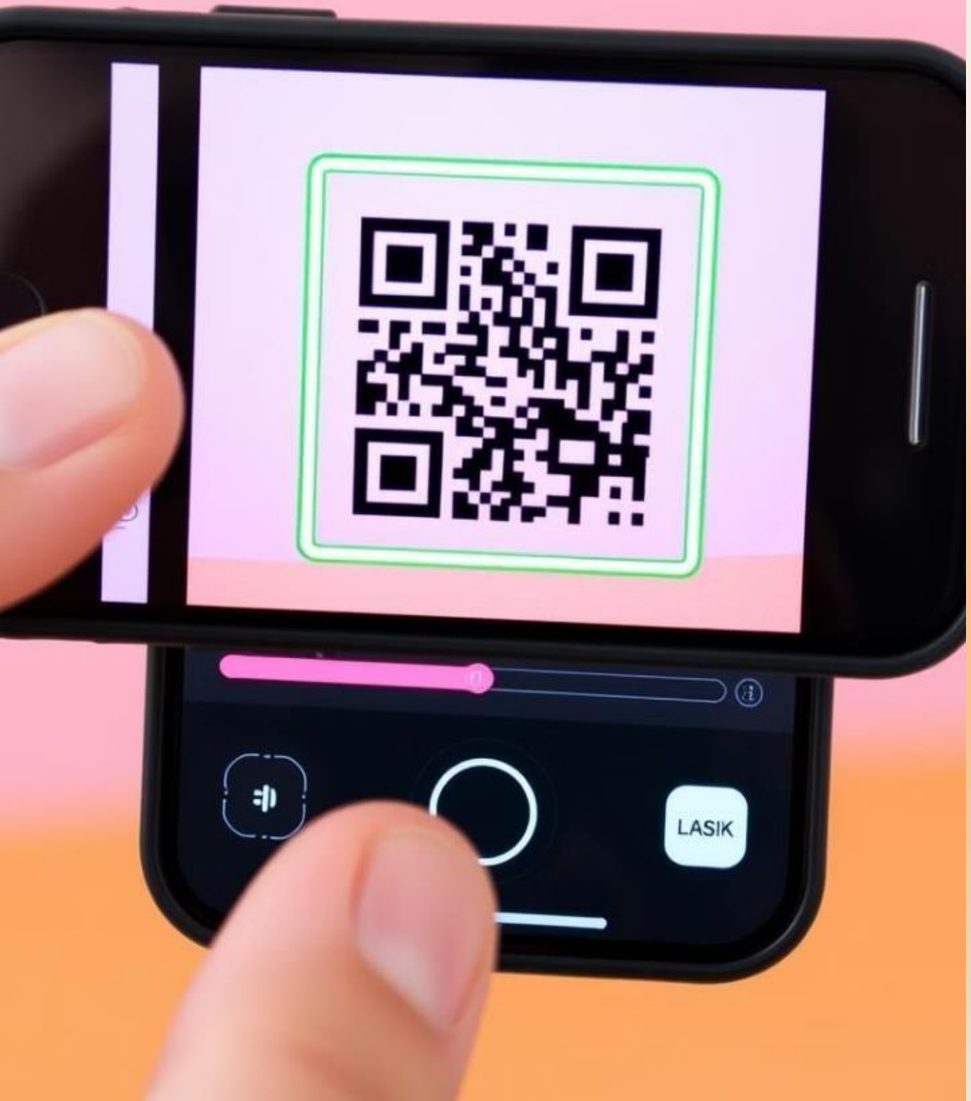
Hash functions generate unique fingerprints of data, ensuring that any alteration will be detected.

Encryption

Encryption transforms data into an unreadable format, protecting it from unauthorized access.

Digital Signatures

Digital signatures provide authentication and integrity verification, ensuring that the QR code data originates from a trusted source.



QR Code Detection Techniques

Camera-Based Detection

Smartphones and other devices use cameras to capture QR codes and process the visual information

Dedicated Scanners

Specialized QR code scanners are designed to quickly and accurately detect codes, optimizing efficiency.

QR Code Decoding Process

1

Verification

First, the QR code is verified using cryptographic algorithms to ensure its integrity and authenticity.

2

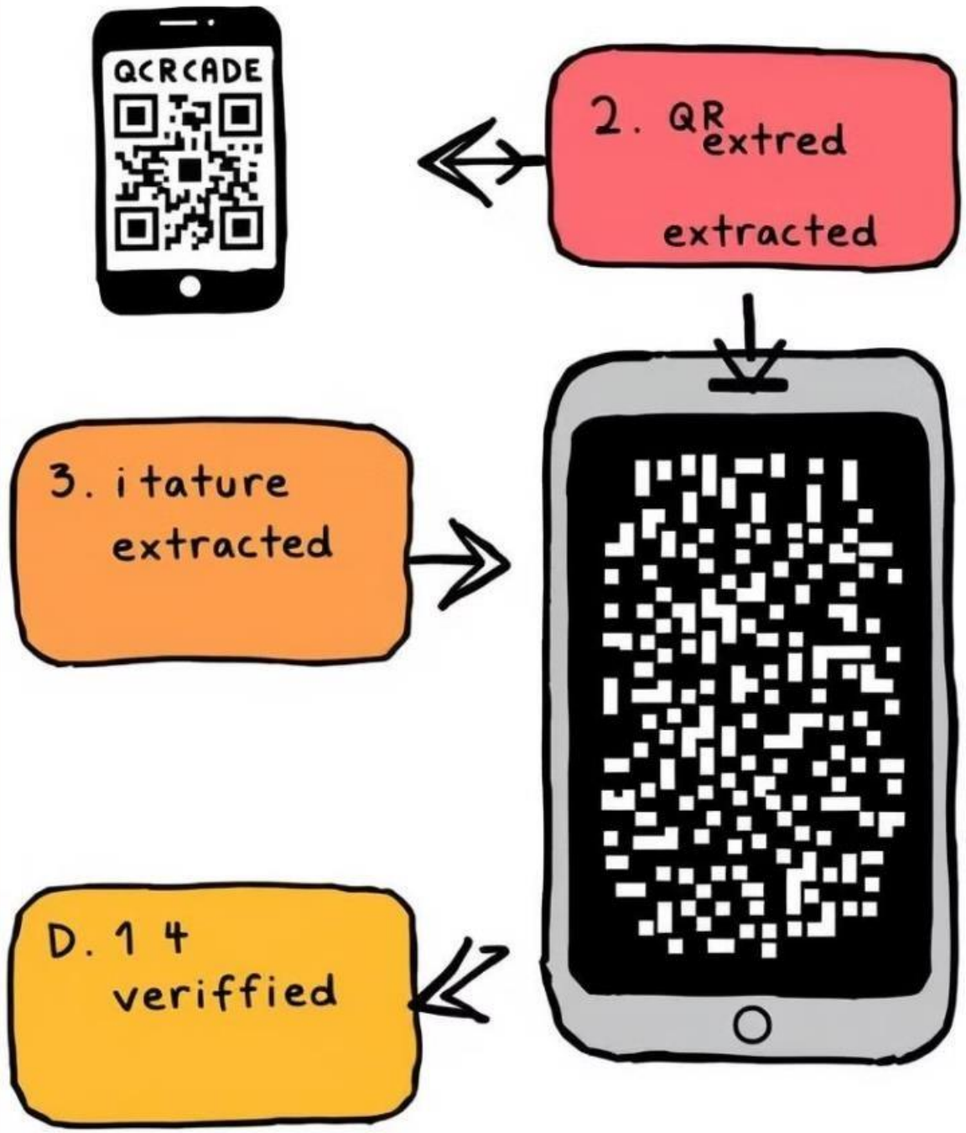
Decryption

If the verification is successful, the encoded data is decrypted using the appropriate algorithm.

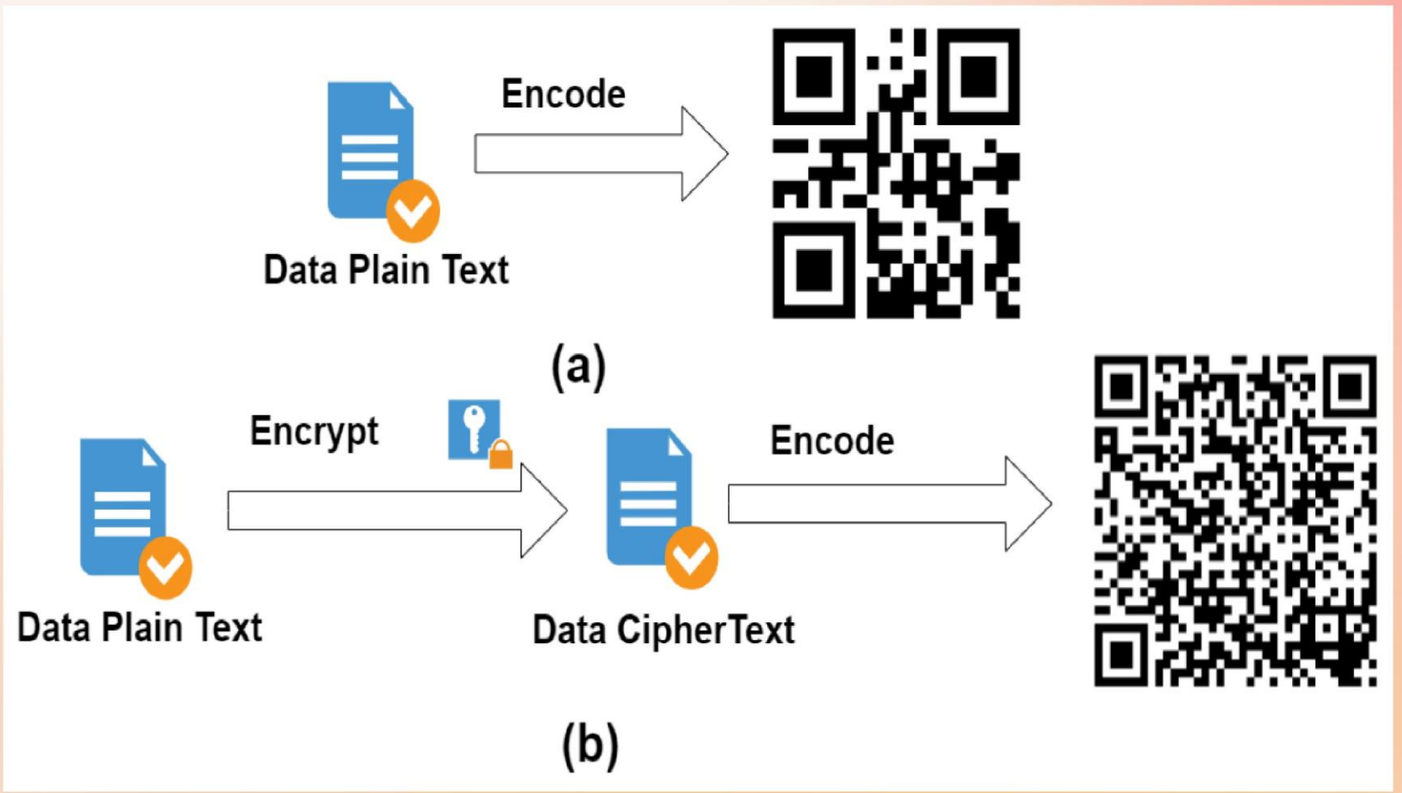
3

Data Extraction

Finally, the decrypted data is extracted and presented to the user, ensuring secure access to the intended information.



Results and Discussion



(a) Direct QR Code Encoding:

1. **Input:** Plain text data is used as the source.
2. **Process:** The plain text data is directly encoded into a QR code.
3. **Output:** A QR code is generated that directly represents the plain text data.

(b) Encrypted QR Code Encoding:

1. **Input:** Plain text data is used as the source.
2. **Process:**
   - The plain text is first encrypted using a cryptographic key.
   - The encrypted data (ciphertext) is then encoded into a QR code.
3. **Output:** A QR code is generated that contains the encrypted data instead of the original plain text.

Future scope

- **Stronger Encryption**: Use advanced encryption methods like AES or ECC for better security.
- **AI for Error Detection**: Use AI to improve QR code scanning in poor conditions and detect fake codes.
- **Dynamic QR Codes**: Create QR codes that change or expire after use for added security.
- **Multi-Factor Authentication**: Combine QR codes with biometric or password authentication.
- **IoT Integration**: Securely connect QR codes to smart devices for better data sharing.
- **Offline Verification**: Develop systems to verify QR codes without internet access.
- **Privacy Protection**: Add encryption to protect user data and comply with privacy laws.

Conclusion

- ✓ Using cryptographic algorithms with QR codes makes data sharing more secure.
- ✓ By encrypting the data before turning it into a QR code, only authorized users with the correct key can read the information, keeping it private.
- ✓ It also ensures that the data hasn’t been changed during transmission.
- ✓ This method keeps QR codes simple and easy to use while adding a strong layer of protection, making it perfect for secure tasks like payments, authentication, or sharing sensitive information.
- ✓ In today’s digital world, this approach provides a safe and reliable way to protect important data from cyber threats.

THANK YOU