KLE Technological University
Creating Value
Leveraging Knowledge
BVB Campus, Vidyanagar, Hubballi – 580031, Karnataka, India

Information Security (20ECSC402)

A Project Report on

A comparative study of DES, AES & ECC Diffie–Hellman cryptographic algorithms over QR code

Submitted by,

Praveen Devadkar	**01FE21BCS125**
Harshakumar R Hunashyal	**01FE20BCS128**
Varun Jakanur	**01FE20BCS149**
Rohit Golabhavi	**01FE20BCS148**

Under the Guidance of,

Ms. Pooja P Shettar

SCHOOL OF COMPUTER SCIENCE & ENGINEERING

HUBLI–580 031 (India)

Table of Contents

1. Introduction

The comparative study of AES (Advanced Encryption Standard), DES (Data Encryption Standard), and ECC (Elliptic Curve Cryptography) with Diffie-Hellman key exchange reveals distinct properties that underscore their strengths and weaknesses. AES, a symmetric key algorithm, excels in speed and security, supporting key sizes of 128, 192, or 256 bits. Its operation through a Substitution-Permutation Network ensures robustness against cryptographic attacks. In contrast, DES, while historically significant, is outdated due to its fixed 56-bit key size, rendering it vulnerable to brute-force attacks. The speed of DES is compromised compared to AES. ECC, an asymmetric key algorithm utilized in Diffie-Hellman key exchange, offers an intriguing alternative. With variable key sizes and dependence on elliptic curves, ECC provides equivalent security with shorter key lengths compared to traditional algorithms. This contributes to faster key exchange operations. Notably, ECC demonstrates resilience against various attacks and is particularly quantum-resistant, offering a promising solution in the era of evolving cryptographic threats. In summary, while AES stands out for its speed and security, ECC presents a unique asymmetric approach, and DES, largely obsolete, highlights the importance of key size in cryptographic strength. The choice among these algorithms hinges on specific application requirements, performance considerations, and the need for quantum-resistant solutions.

In a detailed examination of the key properties of AES, DES, and ECC with Diffie-Hellman, the differences become more apparent, providing nuanced insights into their respective strengths and weaknesses. AES, being a symmetric key algorithm, is characterized by its efficiency and flexibility. Its support for varying key sizes, including 128, 192, and 256 bits, allows for tailoring the security level to specific needs. The Substitution-Permutation Network design of AES contributes to its resistance against various cryptographic attacks, making it a cornerstone for secure communication in numerous applications. However, it's crucial to consider the potential impact of quantum computing, as symmetric key

algorithms like AES are susceptible to quantum attacks, specifically Grover's algorithm, which can halve the effective key length.

On the other hand, DES, once a pioneering encryption standard, has become obsolete in contemporary cryptographic landscapes. Its fixed key size of 56 bits, coupled with an 8-bit parity, makes it vulnerable to exhaustive search attacks, as modern computing capabilities can swiftly brute-force through its limited key space. The reduced speed of DES further diminishes its practicality, rendering it unsuitable for secure communications in today's high-performance computing environments.

ECC, as an asymmetric key algorithm employed in Diffie-Hellman key exchange, introduces a distinct paradigm. Its reliance on elliptic curves allows for shorter key lengths compared to traditional algorithms, offering equivalent security. This becomes particularly advantageous in scenarios with limited computational resources. The efficiency of ECC is especially notable in key exchange operations, contributing to faster establishment of shared secrets. Furthermore, ECC exhibits resilience against various cryptographic attacks and stands out as a quantum-resistant alternative due to the inherent complexity of solving elliptic curve discrete logarithm problems.

In evaluating these cryptographic algorithms, the choice must consider the specific requirements of the application. AES is a stalwart for symmetric key encryption, excelling in speed and security but necessitating attention to quantum vulnerabilities. ECC, with its asymmetric nature, provides a valuable alternative, particularly in resource-constrained environments, and showcases resistance to quantum threats. DES, however, is largely relegated to historical significance, underscoring the importance of key size and algorithmic design in contemporary cryptographic practices. As the landscape evolves, the quest for robust cryptographic solutions demands a careful balance between performance, security, and adaptability to emerging challenges.

2. Motivation

This study is motivated by the imperative to evaluate and understand the security implications of employing cryptographic algorithms, specifically DES, AES, and ECC Diffie-Hellman, over QR codes. While DES serves as a historical benchmark with recognized vulnerabilities, AES stands as a modern and widely adopted symmetric key algorithm, and ECC Diffie-Hellman represents an efficient asymmetric key alternative. With QR codes becoming integral to various applications, from mobile payments to data sharing, the study aims to address the unique security challenges posed by QR codes and explores the real-world implications of using different cryptographic algorithms in this context. The focus is on key exchange efficiency and bridging the gap between theoretical cryptographic principles and practical implementation challenges, ultimately informing best practices for secure data transmission within the QR code ecosystem.

3. Literature Survey

[1] Ticketing System Using AES Encryption Based QR Code

The paper proposes a new ticketing system that uses QR codes to store encrypted ticket information. The system is designed to be more secure than traditional ticketing systems, which are often susceptible to fraud and counterfeiting. The system works by generating a QR code for each ticket. The QR code contains encrypted information about the ticket, including the event name, date, time, seat number, and ticket price. The encryption is performed using the AES algorithm, which is a strong cryptographic algorithm that is resistant to attack.

To scan a ticket, a user simply uses a QR code scanner to read the code. The scanner then decrypts the information in the code and sends it to the ticketing system. The ticketing system then verifies the ticket and allows the user to enter the event. The paper argues that the proposed system has several advantages over

traditional ticketing systems. First, the system is more secure because the ticket information is encrypted. Second, the system is more convenient because users can scan their tickets using their smartphones. Third, the system is more efficient because it eliminates the need to print tickets.

The paper also presents a prototype of the system. The prototype was implemented using a web application and a QR code scanner. The prototype was tested with a variety of events, including concerts, sporting events, and conferences. The results of the testing showed that the system was able to successfully scan tickets and verify their authenticity. Overall, the paper presents a promising new approach to ticketing systems. The system is more secure, convenient, and efficient than traditional ticketing systems. The system is also scalable and can be adapted to a variety of events.

Here are some of the specific benefits of the proposed system: Security: The encrypted ticket information is resistant to attack, making it more difficult to counterfeit or forge tickets. Convenience: Users can scan their tickets using their smartphones, which eliminates the need to carry physical tickets. Efficiency: The system eliminates the need to print tickets, which can save time and money for event organizers. The proposed system is still under development, but it has the potential to revolutionize the ticketing industry.

[2] Design of Intelligent Access Control System Based on DES Encrypted QR Code

This paper describes the design of an intelligent access control system that utilizes DES-encrypted QR codes for user identification and access authorization.
Traditional access control systems often rely on physical keys or cards, which can be lost, stolen, or duplicated. Additionally, managing these physical tokens can be cumbersome and expensive. This paper proposes a solution that addresses these shortcomings by leveraging the convenience and security of QR codes and DES encryption.
The proposed system comprises three main components:

Android Smartphone:
Users store their access credentials in the form of DES-encrypted QR codes on their smartphones.
The smartphone app communicates with the access controller for authorization and access control.
Embedded Access Controller:
This device is located near the access point (e.g., door).
It receives encrypted QR codes from smartphones and decrypts them using DES.
Based on the decrypted information, it grants or denies access.
Server:
Stores user access information and encryption keys.
Communicates with the access controller to manage user access and update encryption keys.

System Operation
User Registration:
Users register with the system through the server application.
The server assigns a unique ID and generates a DES key for each user.
Users download their encrypted QR code containing their ID and access privileges.
Access Request:
Users launch the smartphone app and display their QR code near the access controller.
The access controller scans the QR code and decrypts it using the DES key.
Authorization and Access Control:
The access controller verifies the user's ID and access privileges with the server.
If authorized, the access controller unlocks the door.
The access log is recorded on the server for audit purposes.

Advantages of the Proposed System:
High Security, Convenience, Low Cost, Scalability, Flexibility.
The proposed intelligent access control system based on DES-encrypted QR codes offers a secure, convenient, and cost-effective solution for access control applications. This system has the potential to improve security, reduce costs, and streamline access management in various settings.

[3] Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem

This paper describes a new algorithm for digital image encryption using the Elliptic Curve Public Cryptosystem (ECC). This algorithm aims to address the weaknesses of traditional symmetric encryption methods, such as key distribution and management difficulties.

Motivation:

Traditional image encryption methods often rely on symmetric keys, which need to be shared securely between sender and receiver.

This key management can be cumbersome and prone to attacks.

ECC offers a robust and secure alternative for public key cryptography.

Proposed Algorithm:

Key Generation:

Sender and receiver agree on an elliptic curve and its parameters.

Both parties generate their respective public and private keys.

The agreement on the curve and parameters can be achieved using the Diffie-Hellman key exchange protocol, making key management easier.

Image Encryption:

The sender first converts the image pixels into large integers for efficient encryption.

These integers are then encrypted using a combination of a chaotic system and ECC.

The chaotic system adds randomness and confusion to the encryption process, making it more resistant to cryptanalysis.

The encrypted integers are then used to reconstruct and store the encrypted image.

Image Decryption:

The receiver uses their private key to decrypt the received integers.

The decrypted integers are then used to reconstruct the original image.

Advantages:

Enhanced security, Simplified key management, Improved efficiency, Resistance to cryptanalysis.

4. Problem Statement

To perform a comparative study of AES, DES, and Diffie Hellman cryptographic Algorithms, in order to examine key properties, such as time taken, speed, signature sizes, security levels, and resistance against potential attacks, in order to provide insights into the strengths and weaknesses of each algorithm.

5. Objectives

- To Evaluate the computational efficiency of AES, DES, and ECC Diffie Hellman cryptographic algorithms.
- Compare the security levels and vulnerability to potential attacks among the three algorithms.
- Identify any trade-offs between security, speed, and key management associated with each algorithm.
- Investigate the impact of algorithm choice on the overall performance and resource utilization in cryptographic systems.

6. Methodology

AES (Advanced Encryption Standard)

AES is widely recognized for its robustness and efficiency. It uses symmetric key encryption, meaning the same key is used for both encryption and decryption. AES has varying key lengths, and the longer the key, the more secure the encryption. Its widespread adoption and proven security make it a strong contender for protecting sensitive data in a bus station environment. However, the challenge lies in securely managing and distributing the encryption keys.

DES (Data Encryption Standard)

DES, an older encryption standard, employs a symmetric key approach like AES but with a fixed key length of 56 bits. While historically significant, DES is now considered vulnerable to modern attacks due to its limited key length. In the context of bus station security, DES may not offer the level of protection required in the face of advanced cyber threats.

ECC Diffie Hellman (Elliptic Curve Cryptography with Diffie-Hellman)

ECC Diffie Hellman is an asymmetric key algorithm that offers robust security with shorter key lengths compared to traditional methods. It leverages the mathematical properties of elliptic curves for secure key exchange. In a bus station setting, where efficient key exchange is crucial, ECC Diffie Hellman stands out for its ability to provide strong security with shorter keys, reducing computational overhead.

QR Code Generation for Bus Station Security

In the context of a bus station, QR codes serve as versatile tools for ticketing, scheduling, and information dissemination. Secure QR code generation involves ensuring the integrity of the information encoded. Techniques such as dynamic QR codes, encryption of embedded data, and multi-layered authentication contribute to enhancing security. The choice of encryption algorithm further reinforces the confidentiality of QR code content.

7. Implementation

AES

The AES algorithm is a symmetric encryption algorithm that operates on fixed-size blocks of data (128 bits). The algorithm supports key lengths of 128, 192, and 256 bits. Here is a high-level description of the AES encryption and decryption processes:
AES Encryption:

1. *Key Expansion:*
   - The original key is expanded into a set of round keys using a key expansion algorithm. The number of rounds is determined by the key length (10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys).

2. *Initial Round:*
   - The plaintext block is XORed with the initial round key.

3. *Rounds (for 128-bit key):*
   - SubBytes: Each byte of the block is replaced with a corresponding byte from the S-box.
   - ShiftRows: Bytes in each row are shifted left by an offset.
   - MixColumns: Columns of the block are mixed using a mathematical transformation.
   - AddRoundKey: The block is XORed with the round key.

4. *Final Round:*
   - Similar operations are performed in the final round, excluding the MixColumns step.

5. *Ciphertext:*
   - The resulting block is the ciphertext.

AES Decryption:

1. *Key Expansion (Same as Encryption):*
   - The original key is expanded into a set of round keys.

2. *Initial Round:*
   - The ciphertext block is XORed with the last round key.

3. *Rounds (in reverse order for 128-bit key):*
   - InvShiftRows: Reverse the ShiftRows operation.
   - InvSubBytes: Reverse the SubBytes operation using the inverse S-box.
   - AddRoundKey: XOR the block with the round key.
   - InvMixColumns: Reverse the MixColumns operation.

4. *Final Round:*
   - Similar operations are performed in the final round, excluding the InvMixColumns step.

5. *Decrypted Plaintext:*
   - The resulting block is the decrypted plaintext.

DES

The Data Encryption Standard (DES) is a symmetric-key block cipher that was widely used for secure data transmission and storage. Though DES is now considered obsolete due to its short key length, it played a crucial role in the history of cryptography. Here is an overview of the DES algorithm:

DES Encryption:

1. *Initial Permutation (IP):*
   - The 64-bit plaintext block undergoes an initial permutation.

2. *Key Schedule:*
   - The 56-bit key is used to generate 16 subkeys, one for each round.

3. *Rounds (16 Rounds):*
   - Each round consists of the following operations:
     - *Expansion:* The 32-bit right half is expanded to 48 bits.
     - *Key Mixing:* The expanded half is XORed with the round key.
     - *Substitution (S-boxes):* The result is passed through eight S-boxes, each providing a nonlinear substitution.
     - *Permutation (P-box):* The 32-bit output is permuted.
     - *XOR with Left Half:* The output is XORed with the left half of the block.

4. *Final Permutation (FP):*
   - The 64-bit block undergoes a final permutation.

5. *Ciphertext:*
   - The resulting block is the ciphertext.

DES Decryption:

The decryption process in DES is the reverse of the encryption process. The same subkeys are used in reverse order:

1. *Initial Permutation (IP):*
   - The 64-bit ciphertext block undergoes an initial permutation.

2. *Rounds (in Reverse Order):*
   - The operations in each round are applied in reverse order.

3. *Final Permutation (FP):*
   - The 64-bit block undergoes a final permutation.

4. *Decrypted Plaintext:*
   - The resulting block is the decrypted plaintext.

ECC

The Elliptic Curve Diffie-Hellman (ECDH) algorithm is a key exchange protocol based on elliptic curve cryptography. It allows two parties to securely generate a shared secret over an insecure channel without directly exchanging secret keys. Here is an overview of the ECC Diffie-Hellman algorithm:
ECC Diffie-Hellman Key Exchange:

1. *Curve Selection:*
   - Choose an elliptic curve and a base point (a known point on the curve) that both parties agree upon. The parameters of the elliptic curve are public and can be used by anyone.

2. *Public and Private Key Generation:*
   - Each party generates its public-private key pair. The private key is a random number (typically represented as \(d\)), and the public key is a point on the elliptic curve derived from multiplying the base point by the private key (\(Q_A = d \cdot G\) for party A).

3. *Public Key Exchange:*
   - Both parties exchange their public keys.

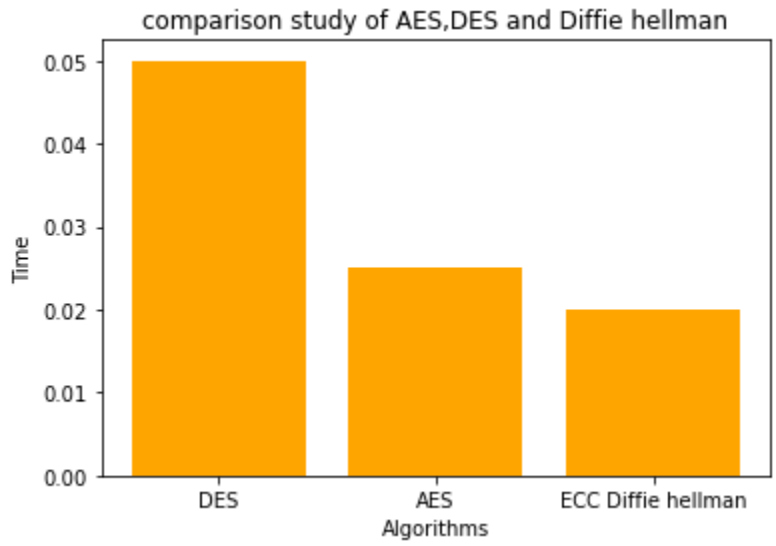
4. *Shared Secret Calculation:*
   - Each party calculates the shared secret using its private key and the other party's public key.
     - Party A: \(S_A = d_A \cdot Q_B\)
     - Party B: \(S_B = d_B \cdot Q_A\)

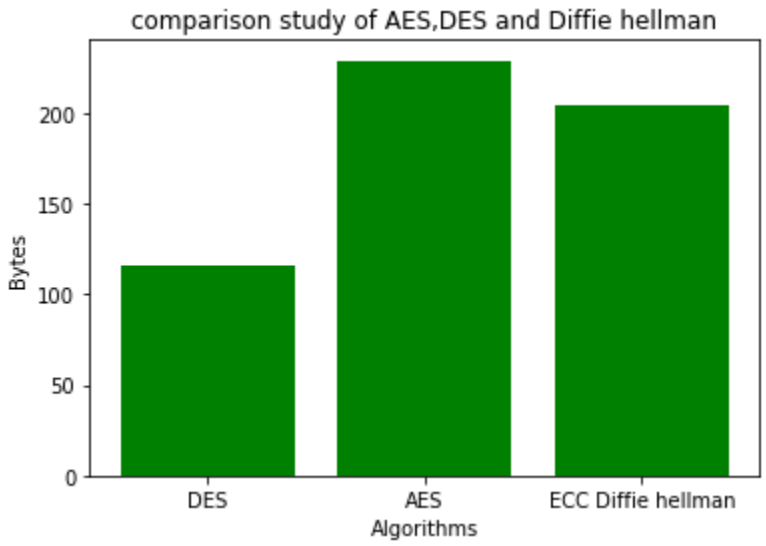
5. *Shared Secret Use:*
   - The shared secret (\(S_A\) for Party A or \(S_B\) for Party B) can be used as a symmetric key for further secure communication, such as encrypting messages using a symmetric encryption algorithm.

8. Results

Comparative study of DES, AES, ECC Diffie Hellman algorithms over metrics like Encryption time, Space used, Efficiency, Security, Key Length, Computational complexity, Key generation.

Metric	DES	AES	ECC Diffie hellman
Time Taken for encryption (seconds)	0.01 – 0.05	0.00 – 0.025	0.0– 0.020
Space Consumed (bytes)	100- 150	200 - 250	180 – 220
Efficiency	Less Efficient	Efficient	Efficient
Security	low	moderate	High
Key Length (bits)	64	128	256
Computational Complexity	Low	Moderate	High
Key Generation	Simple	More simple	Complex





8. Conclusion and Future scope

Conclusion

When considering the encryption algorithms for bus station security, the choice depends on the specific requirements and constraints. AES stands as a robust option for symmetric key encryption, while ECC Diffie Hellman offers efficient key exchange in an asymmetric context. DES, while historically significant, is now less suitable for modern security needs. In QR code generation, a combination of secure encryption practices and dynamic coding techniques ensures a resilient defense against potential threats, making bus station operations more secure and reliable. Ultimately, the selection of encryption methods should align with the unique security demands of the bus station environment.

- ECC Diffie hellman excels in terms of both security and performance. It is best choice for applications requiring high security and efficiency.
- DES, while efficient, has some performance limitations and may not be the best choice for applications requiring high security.
- AES is widely adopted and provides a good balance of security and performance, but it requires careful implementation to mitigate known vulnerabilities.

Future scope

A comparative study of DES, AES, and ECC Diffie-Hellman cryptographic algorithms applied to QR codes provides valuable insights into their performance and suitability for secure communication and data storage. Future research in this field could focus on addressing quantum computing challenges by developing quantum-resistant cryptographic solutions. Exploring hybrid cryptographic schemes that combine symmetric and asymmetric algorithms may enhance overall security. Additionally, integrating blockchain technology with QR codes could improve traceability and data integrity. Dynamic key management, advanced authentication mechanisms, and standardized security features for QR codes are essential areas for further investigation. User-friendly security measures and robust error correction techniques are crucial for encouraging widespread adoption. Finally, ensuring cross-platform compatibility and interoperability will contribute to the seamless integration of secure QR code technologies across diverse devices and applications. The research landscape holds promise for advancements that align with the evolving demands of secure QR code applications and provide resilience against emerging security threats.

References

[1] Ticketing System Using AES Encryption Based QR Code, Nirmit Gangurde; Subendu Ghosh; Akash Giri; Swapnil Gharat, 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)

[2] Design of Intelligent Access Control System Based on DES Encrypted QR Code, Yaoqiu Hong, 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA).

[3] Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem, 2018, Xiaoqiang Zhang; Xuesong Wang