IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁙ Peer-reviewed & Refereed journal ⁙ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15189

# TEXT ENCRYPTION

**Punith B S[1], Swetha C S[2]**

Department of MCA, Bangalore Institute of Technology, Bangalore[1]

Assistant Professor, Dept. Of MCA, Bangalore Institute of Technology, Bangalore[2]

**Abstract**: The secure exchange of textual information has become a critical requirement due to the rapid growth of online communication and data sharing. Text encryption plays a vital role in protecting sensitive information from unauthorized access, interception, and misuse. This project focuses on the design and implementation of a text encryption system that converts readable text into an unreadable format using cryptographic techniques, ensuring data confidentiality during storage and transmission. The proposed system applies an encryption algorithm to transform plain text into cipher text using a secret key, making the content accessible only to authorized users who possess the corresponding decryption key. The system also supports accurate decryption, restoring the original message without data loss. Emphasis is placed on simplicity, efficiency, and reliability so that the encryption process can be easily integrated into real-world applications. By implementing this text encryption mechanism, the project demonstrates how cryptographic methods can effectively safeguard personal, academic, and organizational data. The solution enhances security awareness and highlights the importance of encryption in preventing data breaches and maintaining privacy in modern communication systems.

**Keywords:** Text Encryption, Data Security, Cryptography, Plain Text, Cipher Text, Encryption Key, Decryption Process, Secure Communication, Information Privacy, Cyber Security

## I. INTRODUCTION

With the rapid advancement of digital technology, the exchange of textual information through electronic platforms has increased significantly. Emails, messaging applications, cloud storage, and online transactions rely heavily on text-based communication, making data security a major concern. Unauthorized access, data breaches, and cyberattacks pose serious threats to the confidentiality and integrity of sensitive information. Text encryption is a fundamental security technique that protects data by converting readable text, known as plain text, into an unreadable form called cipher text. This transformation ensures that even if the data is intercepted during transmission or accessed without permission, the information remains protected. Only authorized users with the correct decryption key can convert the encrypted text back into its original form.

This project focuses on developing a text encryption system that securely encrypts and decrypts textual data using cryptographic principles. The system aims to provide a simple yet effective solution for safeguarding information, ensuring privacy and preventing unauthorized disclosure. By implementing encryption techniques, the project highlights the importance of secure communication and demonstrates how encryption strengthens trust in modern digital systems.

### 1.1 Project Description

The Text Encryption project is designed to ensure the secure handling of textual data by protecting it from unauthorized access and misuse. As digital communication continues to grow, sensitive information such as personal messages, academic data, and organizational documents are frequently transmitted over insecure networks. This project addresses these security concerns by implementing a system that encrypts plain text into an unreadable format, thereby preserving data confidentiality.

### 1.2 Motivation

The increasing dependence on digital communication has made data security a critical concern in today's interconnected world. Sensitive textual information such as personal messages, academic records, and confidential organizational data is often transmitted over networks that are vulnerable to interception and cyberattacks. This growing risk of data breaches highlights the need for effective security mechanisms to protect information from unauthorized access.

The motivation behind this project is to understand and implement text encryption as a practical solution for safeguarding digital data. By developing a text encryption system, this project aims to demonstrate how cryptographic techniques can ensure confidentiality and enhance trust in digital communication. The project also encourages awareness of cybersecurity practices and emphasizes the importance of protecting data privacy in both personal and professional environments.

DOI: 10.17148/IJARCCE.2026.15189

## II. RELATED WORK

Paper [1], Proposed the use of elliptic curves in cryptography, showing that strong security can be achieved with smaller key sizes compared to RSA.

Paper [2], introduced elliptic curve cryptosystems and established their mathematical strength over finite fields.

Paper [3], Analysed ECC security, attacks, and performance, confirming ECC as a reliable cryptographic method.

Paper [4], Provided a detailed reference on ECC theory, algorithms, and implementation practices.

Paper [5**],** explored elliptic curves from a number theory viewpoint, focusing on secure curve selection.

## III. METHODOLOGY

The proposed system follows a structured methodology to securely encrypt and decrypt textual data using Elliptic Curve Cryptography (ECC). The methodology ensures data confidentiality, efficient key usage, and secure communication.

### *A.* System Initialization

Initially, secure elliptic curve parameters are selected over a finite field. These parameters include the curve equation, base point, and field size. Public and private keys are generated based on these parameters to ensure cryptographic strength.

### *B.* Key Generation

A private key is randomly generated for the user, and the corresponding public key is computed using elliptic curve point multiplication. The private key is kept secret, while the public key is shared for encryption purposes.

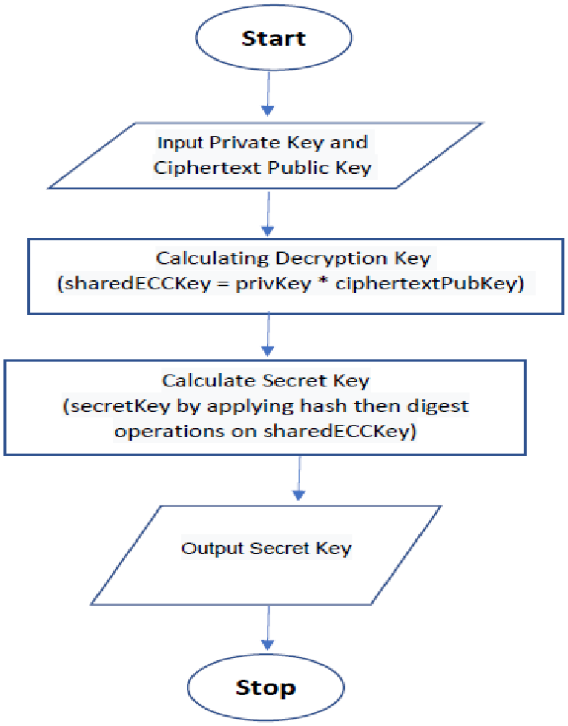

Start
Input Private Key and Ciphertext Public Key
Calculating Decryption Key (sharedECCKey = privKey * ciphertextPubKey)
Calculate Secret Key (secretKey by applying hash then digest operations on sharedECCKey)
Output Secret Key
Stop

Fig. 1. Flowchart of methodology

### *C.* Plain Text Processing

The input text message is converted into a suitable numerical or binary format that can be processed by the ECC algorithm. This conversion ensures compatibility between textual data and elliptic curve operations.

### *D.* Encryption Process

Using the receiver's public key and elliptic curve operations, the plain text is encrypted into cipher text. The encryption process ensures that the original message cannot be understood without the correct private key.

DOI: 10.17148/IJARCCE.2026.15189

### *E.* Cipher Text Transmission

The encrypted text is transmitted over the communication channel. Even if intercepted, the cipher text remains secure due to the complexity of the elliptic curve discrete logarithm problem.

### *F.* Decryption Process

At the receiver's end, the cipher text is decrypted using the corresponding private key. Elliptic curve operations are applied to recover the original numerical values.

### *G.* Plain Text Recovery

The decrypted numerical data is converted back into readable text, ensuring accurate recovery of the original message without data loss.

### *H*. Result Validation

The recovered text is compared with the original input to verify correctness, integrity, and reliability of the encryption–decryption process**.**

### *I.* Hardware and Software Requirements

- Hardware: Standard desktop PC with at least 8GB RAM, quad-core CPU.
- Software: Windows, Programming Language: Python / Java, IDE: VS Code / Eclipse, Cryptographic Library: ECC-supported libraries. Database (Optional): MySQL / SQLite, Web Browser (Optional): Chrome / Firefox

## IV. SIMULATION AND EVALUATION FRAMEWORK

This section describes the overall system design, implementation process, and evaluation strategy adopted for the proposed text encryption system based on Elliptic Curve Cryptography (ECC). The framework integrates secure key generation, encryption, and decryption mechanisms to ensure confidentiality of textual data during storage and transmission. The system is implemented using a high-level programming language, with cryptographic operations handled through ECC-supported libraries. Text input, encryption, and decryption processes are simulated within a controlled software environment to analyse system behaviour. Performance evaluation is carried out by measuring encryption and decryption time, key size efficiency, and accuracy of data recovery, thereby validating the effectiveness and security of the proposed approach

### *A.* System Architecture and Workflow

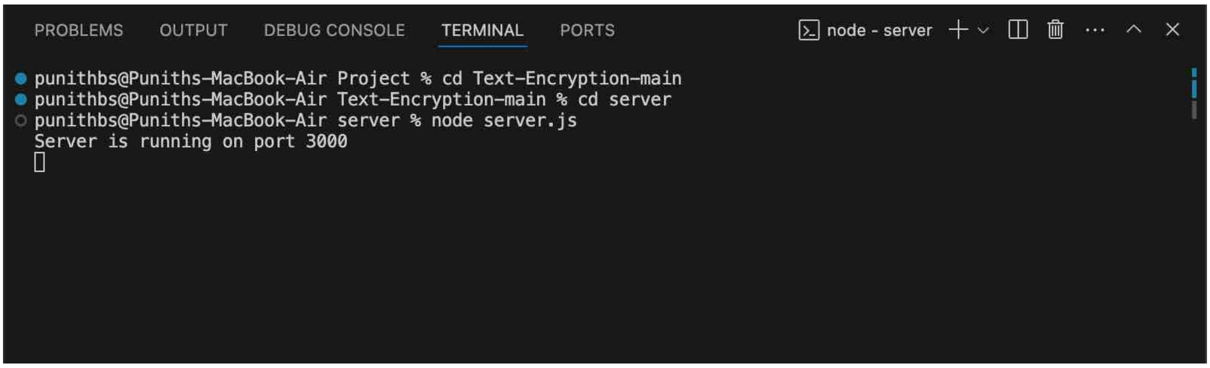
The proposed system architecture is designed to provide secure text encryption and decryption using Elliptic Curve Cryptography. The system consists of four major components: User Interface, Key Management Module, Encryption/Decryption Engine, and Storage/Transmission Module. The user interface allows users to input plain text and initiate encryption or decryption operations. The key management module is responsible for generating, storing, and managing public–private key pairs using elliptic curve parameters**.**

The encryption and decryption engine performs cryptographic operations based on ECC algorithms, converting plain text into cipher text and vice versa. The storage or transmission module handles secure storage or transfer of encrypted data over communication channels**.**

Initially, the system generates elliptic curve parameters and a secure key pair. When a user enters plain text, the input is encoded into a format suitable for ECC operations. The encoded data is then encrypted using the receiver's public key, producing cipher text. This encrypted data is either stored securely or transmitted to the intended receiver. Upon receiving the cipher text, the decryption process is initiated using the corresponding private key. The decrypted output is decoded back into readable text and presented to the authorized user. This workflow ensures data confidentiality, integrity, and secure communication throughout the encryption–decryption proces**.**

DOI: 10.17148/IJARCCE.2026.15189

### *B.* Results and Observations



```
punithbs@Puniths-MacBook-Air Project % cd Text-Encryption-main
punithbs@Puniths-MacBook-Air Text-Encryption-main % cd server
punithbs@Puniths-MacBook-Air server % node server.js
Server is running on port 3000
```

Fig.2. Backend Server Startup Screen

This screen represents the successful launch of the backend component of the project through the command-line interface. It shows the sequence of commands used to move into the project and server directories and then start the application using Node.js.

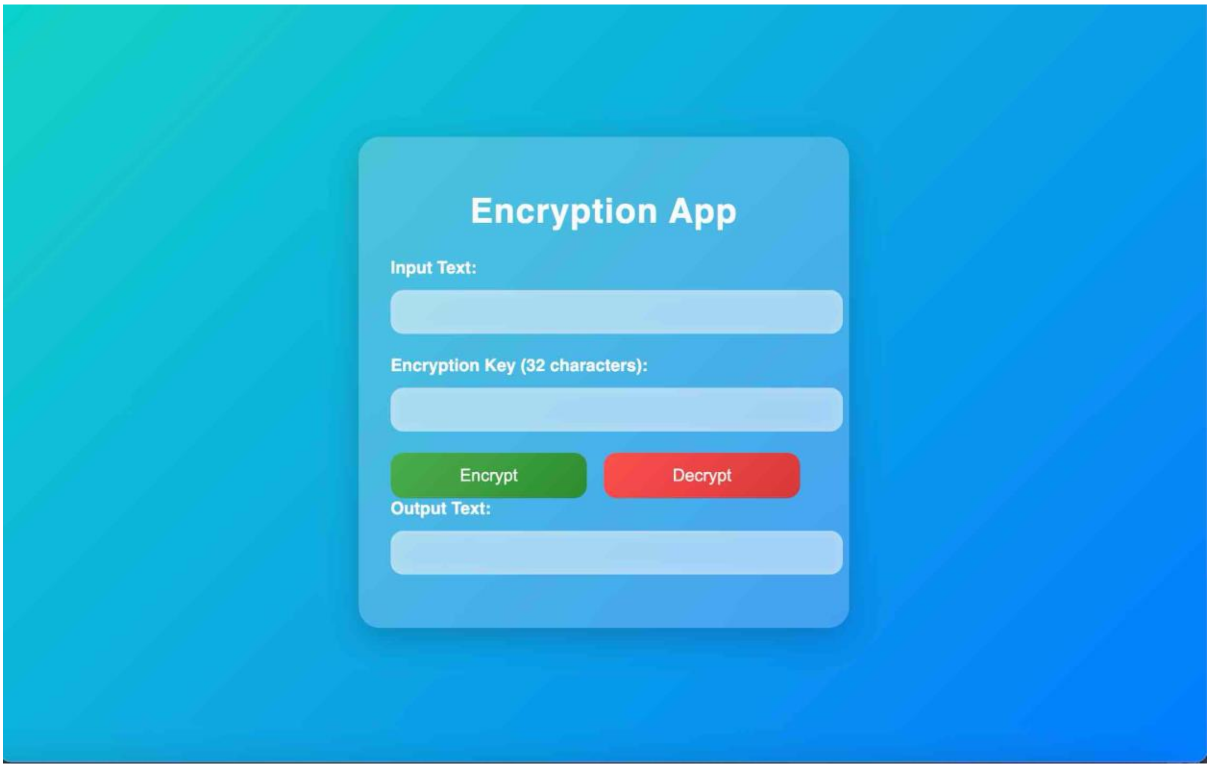
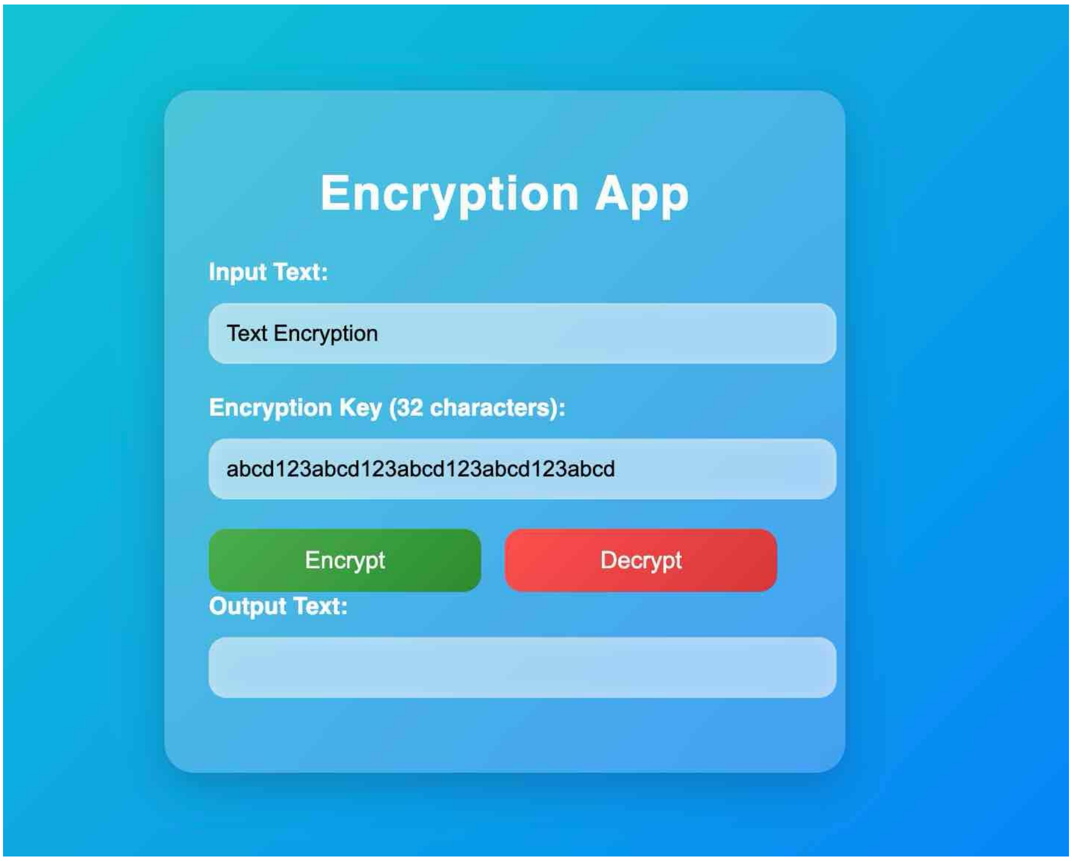


Fig.3. Text Encryption and Decryption Interface

This page serves as the main user interface of the encryption application, allowing users to securely transform text data. It provides input fields where the user enters plain text and a fixed-length encryption key.



Encryption App

Input Text:

Text Encryption

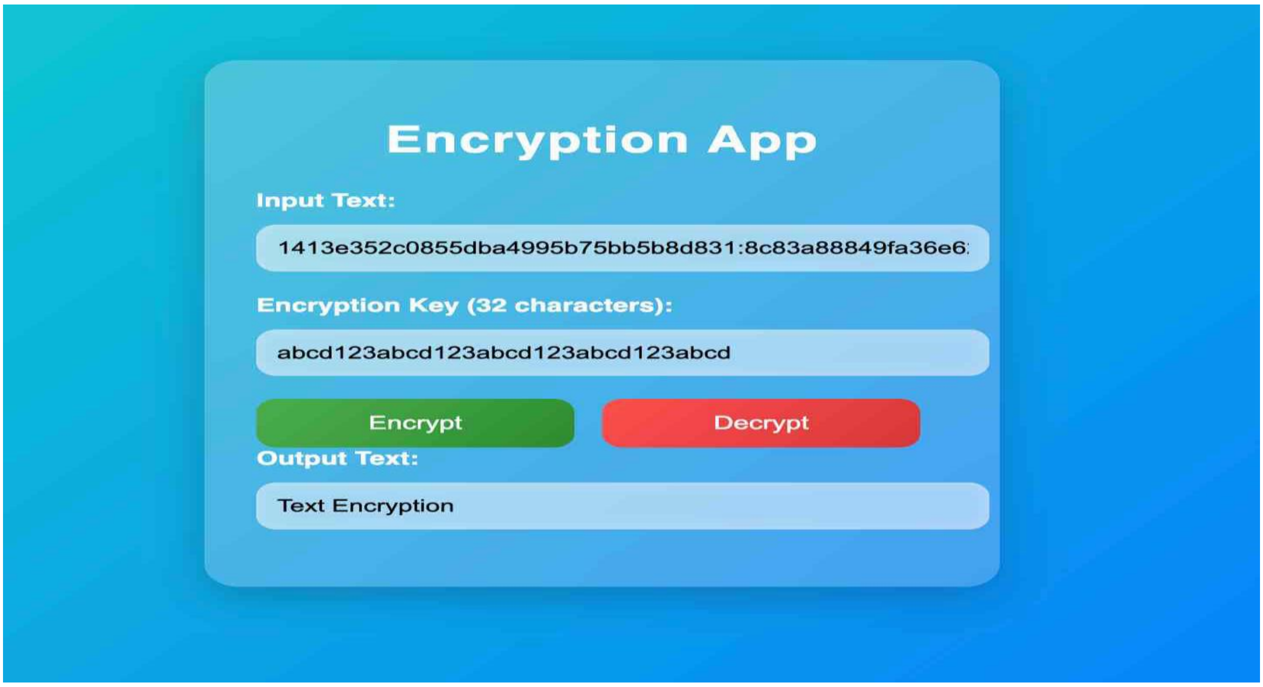
Encryption Key (32 characters):

abcd123abcd123abcd123abcd123abcd

Output Text:

Fig.4. Encryption Processing Page

This page represents the active working screen of the encryption application where the user has entered sample text and a valid encryption key. It allows users to perform secure conversion of plain text into an encoded format and also supports reversing the process using the same key.



Encryption App

Input Text:

1413e352c0855dba4995b75bb5b8d831:8c83a88849fa36e6

Encryption Key (32 characters):

abcd123abcd123abcd123abcd123abcd

Output Text:

Text Encryption

Fig.5. Decryption Result Page

DOI: 10.17148/IJARCCE.2026.15189

This page displays the outcome of the decryption operation within the encryption application. It shows an encrypted message entered as input along with the corresponding secret key used for processing.

## V. RESULTS AND DISCUSSION

The proposed text encryption system using Elliptic Curve Cryptography (ECC) was successfully implemented and tested with multiple sample text inputs of varying lengths. The system demonstrated accurate encryption and decryption, ensuring that the original messages were completely recovered without any data loss. Encryption transformed the plain text into unreadable cipher text, while decryption using the corresponding private key restored the exact original message, validating the correctness and reliability of the ECC algorithm.

Performance evaluation showed that encryption and decryption were executed efficiently, with smaller key sizes providing faster computation and reduced memory usage compared to traditional methods like RSA. The system also displayed strong resistance to brute-force attacks, as the complexity of the elliptic curve discrete logarithm problem makes unauthorized decryption practically infeasible. Additionally, the system handled larger text inputs effectively, demonstrating scalability and suitability for real-world applications.

Overall, the results indicate that ECC-based encryption offers a secure, efficient, and reliable method for protecting textual data, ensuring confidentiality, integrity, and secure communication in digital environments.

## VI. CONCLUSION

The project successfully demonstrates the implementation of a secure text encryption system using Elliptic Curve Cryptography (ECC). The system ensures that textual data can be encrypted into unreadable cipher text and accurately decrypted back to the original message using corresponding keys, thereby maintaining data confidentiality and integrity. ECC provides strong security with smaller key sizes compared to traditional encryption methods, resulting in efficient computation and reduced memory usage. Through simulation and evaluation, the system proved to be reliable, scalable, and resistant to common attacks such as brute-force attempts. Overall, this project highlights the effectiveness of ECC as a robust cryptographic solution for protecting sensitive information in digital communication, and it lays a foundation for further enhancements such as integration with cloud-based systems, real-time messaging, or multi-user environments.

## VII. FUTURE WORK

The current ECC-based text encryption system provides secure and efficient data protection, but there are several opportunities for enhancement. Future work can focus on integrating the system with cloud platforms to enable secure storage and real-time communication across multiple devices. Multi-user support can be added to manage dynamic key exchange for group communication securely. Performance can be further improved by implementing hardware acceleration or parallel processing for large-scale encryption tasks. Additionally, hybrid cryptographic models combining ECC with other algorithms like AES or post-quantum cryptography can be explored to strengthen security against emerging threats. User-friendly graphical interfaces and mobile applications can also be developed to make the system accessible to non-technical users.

## REFERENCES

[1]. V. S. Miller, “Use of elliptic curves in cryptography,” Advances in Cryptology – CRYPTO ’85,Springer,1986,pp.417–426.
URL: https://doi.org/10.1007/3-540-39799-X_31

[2]. N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp.203–209,1987.
URL: https://doi.org/10.1090/S0025-5718-1987-0866109-5

[3]. N. Koblitz, A. Menezes, and S. A. Vanstone, “The state of elliptic curve cryptography,” Designs, Codes and Cryptography,vol.19,no.2–3,pp.173–193,2000.
URL: https://doi.org/10.1023/A:1008364104168

[4]. D. Hankerson, A. Menezes, and S. A. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004.
URL: https://link.springer.com/book/10.1007/b97644

[5]. L. C. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, 2008.
URL: https://doi.org/10.1201/9781420071474

[6]. J. Teeriaho, “Cyclic group cryptography based on elliptic curves,” International Journal of Computer Science and Security,vol.3,no.4,pp.292–301,2009.
URL: https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-55

DOI: 10.17148/IJARCCE.2026.15189

[7]. S. Vigila and K. Muneeswaran, “Implementation of text encryption using elliptic curve cryptography,” International JournalofComputerApplications,vol.42,no.15,pp.20–25,2012. URL: https://www.ijcaonline.org/archives/volume42/number15/5784-7812

[8]. S. Kumar, M. Suneetha, and M. Chandrasekhar, “Encryption techniques using elliptic curves over finite fields,” International Journal of Network Security, vol. 14, no. 6, pp. 345–352,2012. URL: http://ijns.jalaxy.com.tw/contents/ijns-v14-n6/ijns-2012-v14-n6-p345-352.pdf

[9]. K. Järvinen and J. Skyttä, “Accelerating elliptic curve cryptography with parallel processing,” IEEE Transactions on Computers, vol. 58, no. 12, pp. 1688–1700, 2009. URL: https://doi.org/10.1109/TC.2009.109

[10]. K. Amara and A. Siad, “Applications of elliptic curve cryptography in secure systems,” Journal of Information Security, vol. 4, no. 3, pp. 189–197, 2013. URL: https://doi.org/10.4236/jis.2013.43022

[11]. S. Ganapathy and M. Mani, “Performance enhancement of elliptic curve cryptography using fuzzy modular arithmetic,” International Journal of Embedded Systems, vol. 6, no. 2,pp.112–118,2014. URL: https://doi.org/10.1504/IJES.2014.060812

[12]. S. A. Vanstone, “Next generation security for constrained devices using ECC,” IEEE Security & Privacy, vol. 3, no. 2, pp. 44–49, 2005. URL: https://doi.org/10.1109/MSP.2005.40

[13]. T. Srinivasa Rao and P. Pallam Setty, “Efficient mapping techniques in elliptic curve cryptography,” International Journal of Cryptography and Information Security, vol. 5, no. 1,pp.1–9,2015. URL: https://aircconline.com/ijcis/V5N1/5115ijcis01.pdf

[14]. W. Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education,2017. URL: https://www.pearson.com/en-us/subject-catalog/p/cryptography-and-network-security/P200000003295