iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81816

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Forensic Analysis of Encrypted Communication Using Open SSL Key Structures: A Comparative Study of RSA and Elliptic Curve Cryptography

Divya U[1], Dr. Divya[2]
[1]*Student,* [2]*Professor, Department of forensic Science, Garden City University Bangalore, India 560049*

ABSTRACT: ***The rapid growth of digital communication has significantly increased the need for secure data transmission across modern networks. Cryptographic techniques play a vital role in protecting sensitive information by ensuring confidentiality, integrity, and authenticity. Among the most widely used public-key cryptographic systems, RSA and Elliptic Curve Cryptography (ECC) are extensively applied in areas such as secure web communication, digital certificates, authentication systems, and encrypted messaging platforms.***

While these techniques provide strong security, the processes involved in encryption and decryption often leave behind subtle traces within computing environments. These traces, known as cryptographic artefacts, can include key files, encrypted data, metadata, and command execution logs. Such artefacts can serve as valuable sources of evidence in digital forensic investigations, particularly when direct access to encrypted data is not possible.

This study investigates the forensic artefacts generated during encryption and decryption processes using the OpenSSL toolkit. RSA and ECC key pairs were generated and used to encrypt and decrypt a sample plaintext file. The resulting outputs were analysed through command-line inspection and structural examination of key components.

The findings reveal that encrypted data exhibits a high degree of randomness at the binary level, reflecting strong encryption characteristics. In addition, RSA private keys contain identifiable mathematical components, including modulus values and parameters associated with the Chinese Remainder Theorem. ECC, on the other hand, demonstrates comparable security while requiring significantly smaller key sizes, highlighting its efficiency in modern computing environments.

Overall, this research demonstrates that encryption processes, although designed to protect data, leave behind detectable artefacts that can provide important insights for forensic investigators. These findings reinforce the importance of incorporating cryptographic awareness into digital forensic analysis.

Keywords: Digital Forensics, Cryptographic Artefacts, RSA, Elliptic Curve Cryptography, OpenSSL, Encryption Analysis

I. INTRODUCTION

A. Introduction

The rapid expansion of digital communication technologies has significantly increased the demand for secure methods of data transmission. Sensitive information such as financial transactions, personal communications, and organizational records is continuously exchanged across digital networks, making information security a critical concern. Cryptography plays a fundamental role in protecting such data by converting readable information into encrypted formats, thereby ensuring confidentiality, integrity, and authenticity (Shah and Gor, 2025; Ramakrishna and Shaik, 2025). As digital systems continue to evolve, the importance of implementing robust cryptographic mechanisms has become more evident in both personal and organizational contexts.

Modern cryptographic systems are generally classified into symmetric and asymmetric encryption techniques. Among these, public-key cryptography has become a cornerstone of secure communication systems. It operates using a pair of mathematically related keys—a public key for encryption and a private key for decryption—thus eliminating the need for securely sharing secret keys over insecure communication channels (Ketha, 2024). This approach has significantly improved the practicality and scalability of secure communication across distributed systems.

One of the most widely used public-key cryptographic algorithms is RSA. Its security is based on the computational difficulty of factoring large composite numbers, which makes it resistant to brute-force attacks. Due to its reliability and well-established structure, RSA is extensively used in applications such as digital signatures, authentication systems, and secure communication protocols (Khalaf et al., 2019; Kumar, 2024).

©IJRASET: All Rights are Reserved

However, studies by Cao and Liu (2024) suggest that the performance of RSA may vary depending on system configurations and computational environments, and in some cases, it may still offer advantages over newer cryptographic approaches.

Elliptic Curve Cryptography (ECC) has emerged as a more efficient alternative to traditional algorithms like RSA. ECC is based on the mathematical properties of elliptic curves and provides comparable levels of security while using significantly smaller key sizes. This reduction in key size results in faster computation, lower power consumption, and improved performance, particularly in resource-constrained environments such as mobile devices and Internet of Things (IoT) systems (Yan, 2022; Khan et al., 2023). Additionally, Arunkumar and Kousalya (2021) demonstrated that ECC enhances the efficiency of secure communication protocols such as SSL/TLS by reducing computational overhead without compromising security.

Several comparative studies highlight that the selection of cryptographic algorithms should be based on specific application requirements, system limitations, and evolving security challenges. While ECC is generally preferred for its efficiency, RSA continues to be widely adopted due to its compatibility with existing infrastructures and its long-standing reliability (Mahto and Yadav, 2017; Weng, 2025). This indicates that both algorithms remain relevant, depending on the context in which they are applied.

From a digital forensic perspective, encryption introduces both challenges and opportunities. Encrypted data can prevent direct access to information during investigations, making it difficult for investigators to retrieve useful evidence. However, the processes involved in encryption and decryption often leave behind traces within computing systems. These traces, commonly referred to as cryptographic artefacts, may include key files, encrypted data structures, metadata, and command execution logs (Ramakrishna and Shaik, 2025). Such artefacts can provide indirect evidence of cryptographic activity within a system.

The analysis of these artefacts is becoming increasingly important in digital forensics. Even when encrypted content cannot be accessed, the presence of cryptographic traces can offer valuable insights into system behavior and the use of encryption technologies. Despite extensive research on cryptographic algorithms, relatively few studies have focused on examining the forensic implications of real-world cryptographic implementations.

This study aims to address this gap by analysing the artefacts generated during encryption and decryption processes using the OpenSSL cryptographic toolkit. By generating RSA and ECC key pairs and examining the resulting encrypted files and metadata, the research seeks to provide a practical understanding of how cryptographic operations leave identifiable traces that can support digital forensic investigations.

B. Research Scope

This research investigates the artefacts generated during encryption processes using the OpenSSL command-line tool. It focuses specifically on two public-key algorithms: RSA and Elliptic Curve Cryptography.

The experimental setup involves generating RSA and ECC key pairs, encrypting a sample plaintext file using the RSA public key, and decrypting it with the corresponding private key. The study then examines the artefacts produced, including key files, encrypted outputs, and related metadata.

Additionally, hexadecimal-level analysis is conducted to observe the structure and randomness of encrypted data. The scope of this research is limited to controlled experimental conditions and does not include attempts to break or attack the encryption.

C. Rationale of the Study

The widespread use of encryption in modern systems has introduced significant challenges for digital forensic investigations. Investigators often encounter encrypted files, making it difficult to retrieve meaningful information without access to decryption keys. However, encryption processes do not occur without leaving traces. These processes can generate artefacts such as key files, encrypted data, system logs, and metadata. Such artefacts can provide indirect evidence of cryptographic activity within a system.

This study aims to explore these artefacts by performing encryption experiments using OpenSSL. By analysing the generated outputs and system traces, the research demonstrates how encryption activity can be identified even when the actual data remains inaccessible.

II. REVIEW OF LITERATURE

A. Review of Literature

The field of cryptography has evolved significantly from classical encryption techniques to advanced modern algorithms designed to secure digital communication. Several researchers have contributed to the analysis, comparison, and improvement of cryptographic systems such as RSA, ECC, and AES.

1) Yuhan Yan (2022) provides a comprehensive overview of Elliptic Curve Cryptography (ECC), explaining its mathematical foundation and operational efficiency. The study highlights that ECC offers stronger security with smaller key sizes compared to traditional algorithms like RSA, making it highly suitable for modern applications such as digital signatures and secure communication systems (Yan, 2022).
2) Cao and Liu (2024) examine the performance comparison between RSA and ECC, revealing that although ECC provides equivalent security with smaller key sizes, RSA can outperform ECC in certain computational scenarios. Their findings challenge the common assumption that ECC is always faster and emphasize the importance of selecting algorithms based on specific use cases (Cao & Liu, 2024).
3) Shah and Gor (2025) present a comprehensive survey of symmetric and asymmetric cryptographic algorithms, including AES, RSA, ECC, and ChaCha20. Their work discusses algorithm structures, vulnerabilities, and applications in technologies such as VPNs, blockchain, and IoT systems. The study also highlights emerging trends such as post-quantum cryptography, stressing the need for future-proof security mechanisms (Shah & Gor, 2025).
4) Ramakrishna and Shaik (2025) provide a comparative analysis of cryptographic algorithms based on parameters such as confidentiality, integrity, and efficiency. Their study evaluates algorithms like DES, AES, RSA, and ECC, identifying strengths, weaknesses, and future research challenges in cryptographic design (Ramakrishna & Shaik, 2025).
5) Arunkumar and Kousalya (2021) explore ECC-based cipher suites in SSL/TLS protocols, particularly in applications such as e-commerce and online banking. Their findings demonstrate that ECC improves performance by reducing computational overhead while maintaining strong security (Arunkumar & Kousalya, 2021).
6) Khan et al. (2023) compare RSA and ECC in terms of key size, performance, and security. Their study concludes that ECC provides equivalent security as RSA with significantly smaller key sizes, resulting in better efficiency and reduced memory usage, making it suitable for resource-constrained environments (Khan et al., 2023).
7) Ketha (2024) analyses the evolution of cryptography from classical methods to modern algorithms such as AES, RSA, ECC, and OTP. The study emphasizes how modern cryptographic techniques overcome limitations of classical systems and enhance resistance against attacks such as brute force and frequency analysis (Ketha, 2024).
8) Weng (2025) provides a comparative study of modern encryption algorithms, including symmetric and asymmetric systems. The research highlights differences in performance, scalability, and application areas of RSA, ECC, and AES, emphasizing the importance of selecting appropriate algorithms for specific security requirements (Weng, 2025).
9) Khalaf et al. (2019) compare RSA, ECC, and NTRU algorithms, focusing on security strength and computational performance. Their study demonstrates that ECC provides better efficiency compared to RSA, while also discussing post-quantum alternatives such as NTRU (Khalaf et al., 2019).
10) Mahto and Yadav (2017) present a detailed comparative analysis of RSA and ECC, explaining their underlying mathematical principles. The study highlights that ECC achieves higher security per bit due to the complexity of elliptic curve discrete logarithm problems (Mahto & Yadav, 2017).
11) Kumar (2024) analyses computational performance differences between RSA and ECC implementations. The study demonstrates that ECC offers improved efficiency in encryption and decryption operations, particularly in systems with limited computational resources (Kumar, 2024).
12) Dar et al. (2021) investigate the application of ECC in mobile environments, demonstrating that ECC-based key exchange mechanisms provide secure and efficient communication in resource-constrained devices. Their study reinforces the suitability of ECC for modern lightweight cryptographic applications (Dar et al., 2021).

Despite extensive research on cryptographic algorithms, limited studies focus on analysing forensic artefacts generated during cryptographic operations using real-world tools such as OpenSSL. Since OpenSSL is widely used in secure communication protocols such as SSL and TLS, analysing its implementation provides valuable insights into practical cryptographic processes. Therefore, this study focuses on analysing forensic artefacts generated during RSA and ECC encryption experiments using the OpenSSL toolkit.

B. Research Gap

While many studies have explored cryptographic algorithms in terms of performance and security, fewer have examined the forensic traces generated during their real-world implementation.

In digital forensic investigations, identifying encryption activity can be difficult without understanding the artefacts left behind by cryptographic processes. These artefacts may include key files, encrypted data, system logs, and metadata.
This research addresses this gap by experimentally analysing the artefacts generated during encryption using the OpenSSL toolkit. The study aims to provide practical insights that can assist forensic investigators in recognizing and interpreting cryptographic activity within digital systems.

III. OBJECTIVES

A. AIMS

- To analyse forensic artefacts generated during cryptographic operations using the OpenSSL toolkit, including key files, encrypted data, and metadata.
- To perform encryption and decryption using RSA and Elliptic Curve Cryptography (ECC), and examine ciphertext patterns through hexadecimal analysis.
- To compare RSA and ECC in terms of key structure, size, and forensic traceability to understand how encryption activities can be identified in digital investigations.

B. OBJECTIVES:

- To generate RSA and ECC key pairs and perform encryption and decryption experiments using OpenSSL.
- To analyse encrypted files and associated metadata to identify potential forensic artefacts.
- To compare the structural characteristics of RSA and ECC cryptographic systems for forensic relevance.

IV. METHODOLOGY

A. MATERIALS

The experiments conducted in this study required both hardware and software tools to perform cryptographic operations and forensic analysis. A personal computer running the Windows operating system was used as the primary platform for conducting the experiments. Cryptographic key generation, encryption, and decryption operations were performed using the OpenSSL command-line toolkit, which provides implementations of widely used cryptographic algorithms such as RSA and Elliptic Curve Cryptography (ECC).
The Windows Command Prompt and PowerShell interfaces were used to execute OpenSSL commands and manage the cryptographic files generated during the experiment. A sample plaintext file was created and used as the input data for encryption and decryption procedures. To analyse the structure of encrypted files, a hexadecimal editor was used to examine the binary data and observe ciphertext patterns generated during the encryption process. Additionally, file system metadata such as file creation time, modification time, and file size were examined using Windows file properties in order to identify potential forensic artefacts associated with cryptographic operations. Experimental observations, command outputs, and screenshots were documented using standard documentation software for analysis and reporting purposes.

B. METHODOLOGY

This study conducted an experimental forensic analysis of encrypted communication using the OpenSSL cryptographic toolkit in a Windows command-line environment. The experiment involved generating both RSA and Elliptic Curve Cryptography (ECC) key pairs and using these keys to perform encryption and decryption operations on a sample plaintext file. Initially, a plaintext message file was created within a project directory structure. RSA key pairs were generated using OpenSSL commands, producing both public and private key files. Similarly, ECC key pairs were generated using elliptic curve parameters supported by OpenSSL. The plaintext file was then encrypted using the RSA public key to produce a ciphertext file. The encrypted file was subsequently decrypted using the corresponding RSA private key to verify the correctness of the cryptographic process. Following encryption and decryption, the generated files were examined for forensic artefacts including key structures, encrypted file patterns, and metadata properties. Additional analysis was performed using hexadecimal inspection tools to observe the byte-level structure of encrypted files. Metadata attributes such as file creation time, modification time, file size, and file path location were also extracted using PowerShell commands. These experimental procedures enabled the identification of cryptographic artefacts generated during encryption processes and allowed a comparative observation of RSA and ECC key structures.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

C. Experimental Workflow



Experimental Workflow of Cryptographic Forensic Analysis

V. RESULTAND DISCUSSION

This chapter presents the experimental results obtained during the encryption experiments and discusses the forensic significance of the findings. The experiments were conducted using the OpenSSL command-line toolkit in a Windows environment. RSA and ECC key pairs were generated and used to perform encryption and decryption operations on a sample plaintext file. The resulting artefacts were examined to identify traces of cryptographic activity within the system.

A. Experimental Environment

The experiment was conducted using the **OpenSSL** cryptographic toolkit in a Windows command-line environment.

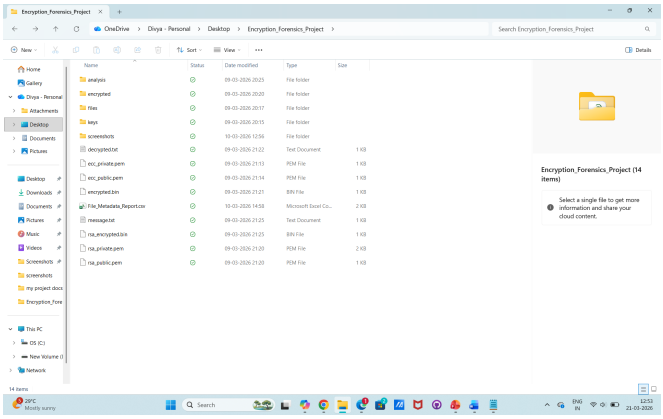


Figure 5.1 – Project Folder Structure

B. RSA Key Generation

```
cd keys
openssl genpkey -algorithm RSA -out rsa_private.pem -pkeyopt rsa_keygen_bits
:2048
openssl rsa -pubout -in rsa_private.pem -out rsa_public.pem
```

Figure 5.2 – RSA Key Generation Command Output

C. ECC Key Generation

```
openssl ecparam -name prime256v1 -genkey -noout -out ecc_private.pem
openssl ec -in ecc_private.pem -pubout -out ecc_public.pem
```

Figure 5.3 – ECC Key Generation

D. Encryption Process

```
openssl pkeyutl -encrypt -pubin -inkey keys\rsa_public.pem -in files\sample.
txt -out encrypted\rsa_encrypted.bin
```

Figure 5.4 – Encryption Process

E. Decryption Process

```
openssl pkeyutl -decrypt -inkey keys\rsa_private.pem -in encrypted\rsa_encry
pted.bin -out decrypted.txt
```

Figure 5.5 – Decryption Process

F. Generated Key Files

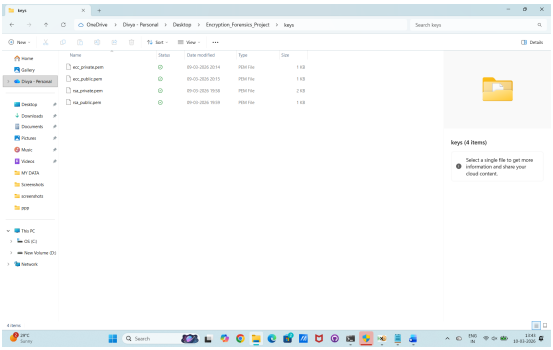


Figure 5.6 – Generated Key Files

Files generated:
rsa_private.pem
rsa_public.pem
ecc_private.pem
ecc_public.pem

G. Encryption Artefacts

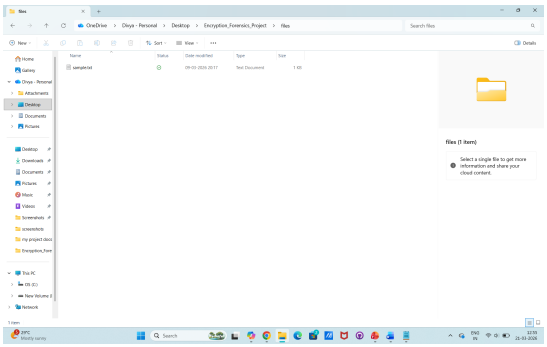


Figure 5.7 sample.txt

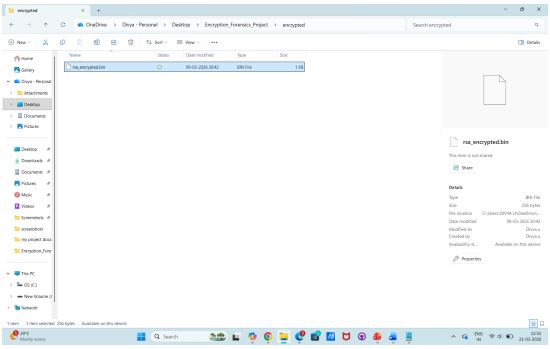


Figure 5.8 – rsa_encrypted.bin

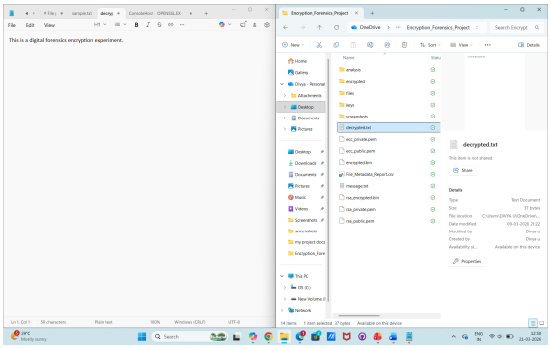


Figure 5.9 – decrypted.txt

H. RSA Key Structure Analysis

```
C:\Users\DIVYA U\OneDrive\Desktop\Encryption_Forensics_Projec
t>openssl rsa -in keys\rsa_private.pem -text -noout
```

Figure 5.10– RSA Key Structure

Parameters identified:

- modulus
- prime1
- prime2
- exponent1
- exponent2
- coefficient

I. Hexadecimal Analysis of Encrypted File

The encrypted file generated during the experiment was examined at the hexadecimal level to observe the binary structure of the ciphertext. Hexadecimal analysis allows investigators to inspect the raw byte representation of files and identify patterns associated with encrypted data.

Encrypted files typically exhibit randomized byte patterns due to the high-entropy nature of modern cryptographic algorithms. Unlike plaintext files, encrypted files do not contain readable characters or recognizable structures.

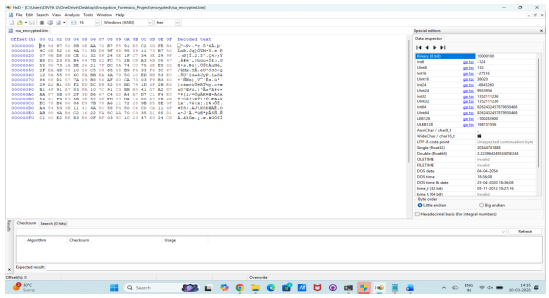


Figure5.11: Hexadecimal Representation of Encrypted File

Thescreenshot illustrates the randomized byte distribution present in the encrypted file. This randomness is a key characteristic of secure encryption algorithms.

J. Metadata Analysis of Generated Files

Metadata analysis was conducted to examine file properties associated with the generated artefacts. Metadata refers to descriptive information about files, including creation time, modification time, file size, and file location.

The following metadata attributes were examined:

- file creation time
- file modification time
- file size
- file path location

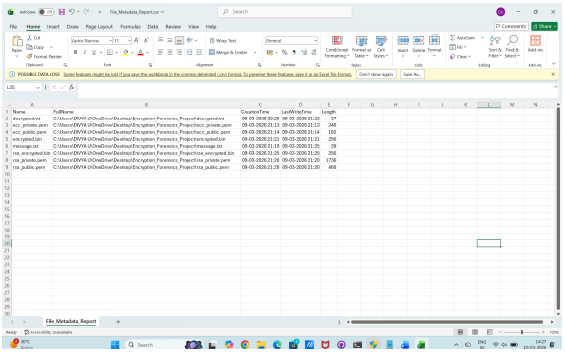


Figure 5.12: Metadata of Cryptographic Artefacts

The metadata analysis confirms that the key files and encrypted files were created during the encryption experiment. Such metadata information may assist digital forensic investigators in reconstructing encryption activity on a system.

K. Comparison of RSA and ECC Key Sizes

One of the most notable observations from the experiment is the difference in key sizes between RSA and ECC cryptographic systems.

Figure5.13 The results demonstrate that ECC keys are significantly smaller than RSA keys while providing comparable levels of cryptographic security. This property makes ECC more efficient for environments with limited computational resources

Algorithm	PrivateKey Size	PublicKey Size
RSA	~1736 bytes	~460 bytes
ECC	~246 bytes	~182 bytes

```
C:\Users\DIVYA U\OneDrive\Desktop\Encryption_Forensics_Project>dir *.pem
 Volume in drive C is OS
 Volume Serial Number is D427-C80B

 Directory of C:\Users\DIVYA U\OneDrive\Desktop\Encryption_Forensics_Project

09-03-2026  21:13               246 ecc_private.pem
09-03-2026  21:14               182 ecc_public.pem
09-03-2026  21:20             1,736 rsa_private.pem
09-03-2026  21:20               460 rsa_public.pem
               4 File(s)          2,624 bytes
               0 Dir(s)  35,869,622,272 bytes free
```

L. Discussion

The experimental results demonstrate that cryptographic operations generate identifiable artefacts within computing systems. These artefacts include key files, encrypted files, command execution records, and associated metadata. The presence of such artefacts can provide valuable indicators of encryption activity during digital forensic investigations, supporting the view that practical cryptographic implementations leave traceable evidence within systems (Ramakrishna & Shaik, 2025).

Hexadecimal analysis revealed that encrypted files exhibit randomized byte patterns due to the high-entropy properties of modern cryptographic algorithms.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

This randomness ensures the confidentiality of encrypted data while also allowing investigators to identify encrypted content through entropy or pattern analysis. Similar observations have been reported in studies analysing encryption behaviour and ciphertext characteristics (Weng, 2025).

Furthermore, the examination of RSA key structures revealed identifiable internal parameters, including prime numbers and Chinese Remainder Theorem (CRT) components. These parameters confirm the internal structure of the RSA cryptographic system and are consistent with the mathematical foundations of RSA discussed in comparative cryptographic studies (Mahto & Yadav, 2017; Khalaf et al., 2019).

The comparative analysis also confirmed that Elliptic Curve Cryptography provides strong security while requiring significantly smaller key sizes compared to RSA. This efficiency makes ECC suitable for modern computing environments, particularly mobile devices and embedded systems. These findings align with existing research highlighting ECC's advantages in terms of computational efficiency and reduced resource consumption (Yan, 2022; Khan et al., 2023; Dar et al., 2021).

In addition, the results support prior studies which emphasize that the selection of cryptographic algorithms should depend on specific system requirements and operational contexts. While ECC provides efficiency advantages, RSA continues to remain relevant due to its widespread implementation and compatibility across systems (Cao & Liu, 2024; Shah & Gor, 2025).

Overall, the findings of this study highlight the importance of understanding cryptographic artefacts within digital forensic investigations. Even when encrypted data cannot be decrypted directly, the presence of cryptographic artefacts may provide investigators with valuable evidence of encryption activity within a system. This reinforces the need for integrating cryptographic awareness into forensic analysis methodologies and tools.

VI. CONCLUSION

This study examined the forensic artefacts generated during encryption experiments using the OpenSSL cryptographic toolkit. The primary objective of the research was to analyze how cryptographic operations leave identifiable traces within computing systems and to compare the structural characteristics of two widely used public-key cryptographic algorithms, RSA and Elliptic Curve Cryptography (ECC).

The experimental procedure involved generating RSA and ECC key pairs, encrypting a plaintext file using the RSA public key, and subsequently decrypting the encrypted file using the corresponding private key. The successful completion of the encryption and decryption processes confirmed the correctness of the implemented cryptographic operations. During the experiment, several artefacts were generated including cryptographic key files, encrypted binary files, decrypted output files, and associated metadata.

The forensic examination of these artefacts demonstrated that encryption processes leave identifiable traces within the file system. Files such as rsa_private.pem, rsa_public.pem, ecc_private.pem, and ecc_public.pem represent important indicators of cryptographic activity within a system. Additionally, encrypted files such as rsa_encrypted.bin exhibit high-entropy randomized byte patterns when examined at the hexadecimal level. These characteristics distinguish encrypted data from normal plaintext files and may assist digital forensic investigators in identifying encrypted evidence during investigations.

Metadata analysis further revealed useful information including file creation time, modification time, file size, and file path location. Such metadata attributes can assist investigators in reconstructing timelines of cryptographic operations and determining when encryption activities occurred within a system environment.

The comparative analysis between RSA and Elliptic Curve Cryptography also highlighted significant differences in key size efficiency. While both algorithms provide strong cryptographic security, ECC achieves comparable levels of security with significantly smaller key sizes compared to RSA. This efficiency makes ECC particularly suitable for modern computing environments including mobile devices, embedded systems, and resource-constrained platforms.

Overall, the findings of this research emphasize the importance of understanding cryptographic artefacts in digital forensic investigations. Even when encrypted data cannot be directly decrypted, the presence of key files, encrypted data structures, and associated metadata may provide valuable indicators of encryption activity. The ability to identify and analyze such artefacts can assist investigators in reconstructing digital events and understanding the use of encryption within a system.

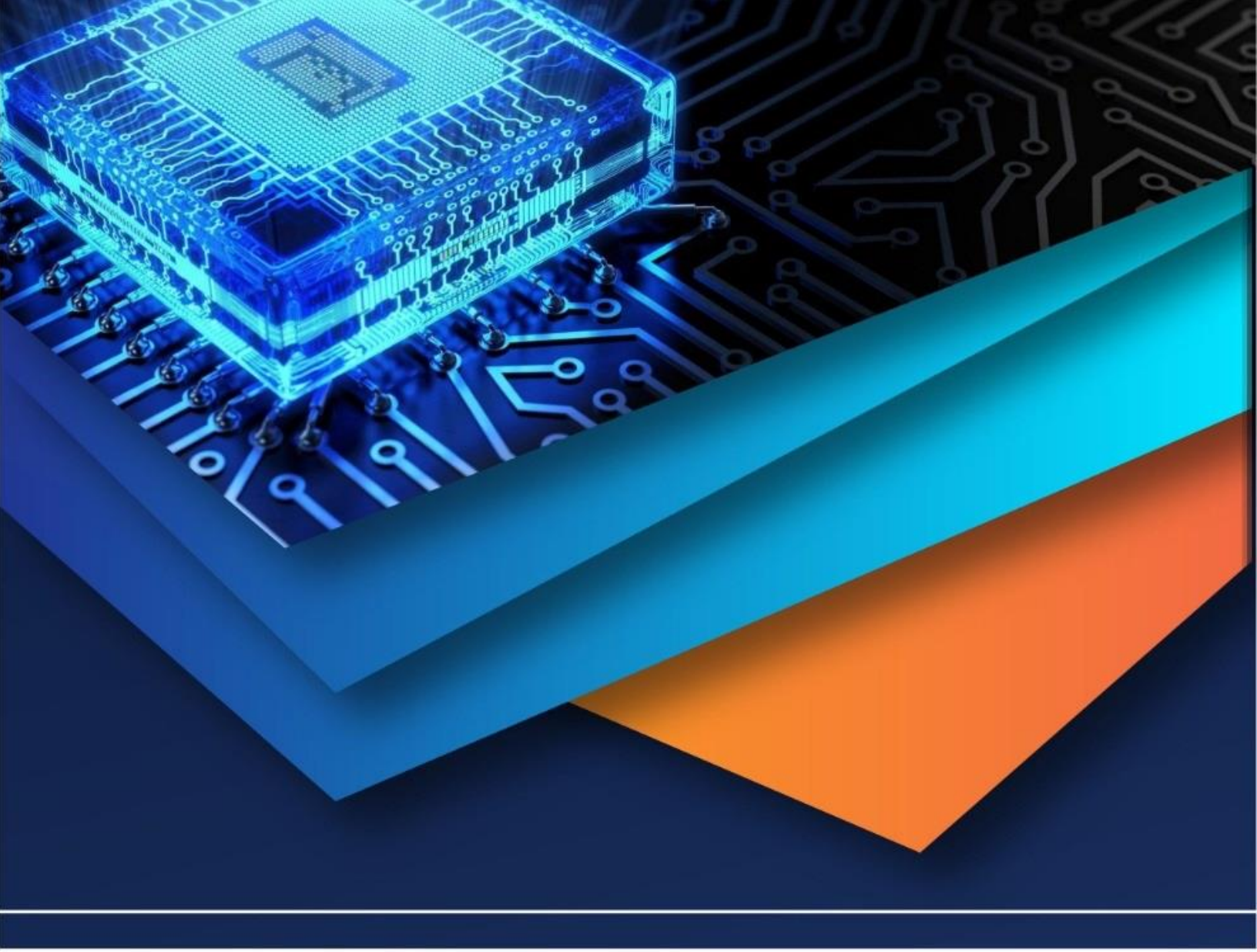
Future research may explore automated detection of encrypted artefacts using entropy analysis tools, forensic frameworks for analyzing cryptographic key structures, and the integration of cryptographic artefact detection into digital forensic investigation workflows

REFERENCES

[1] Yan, Y. (2022). The overview of elliptic curve cryptography (ECC). Journal of Physics: Conference Series, 2386(1).

[2] Cao, Z., & Liu, L. (2024). The practical advantage of RSA over ECC and pairings.
[3] Shah, A. M., & Gor, A. (2025). Comprehensive survey of symmetric and public-key cryptographic algorithms: Foundations, attacks, and applications. International Journal of Informative & Futuristic Research, 12(10).
[4] Ramakrishna, D., & Shaik, M. A. (2025). A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. IEEE Access, 13.
[5] Arunkumar, B., & Kousalya, G. (2021). Secure and lightweight elliptic curve cipher suites in SSL/TLS. Computer Systems Science & Engineering.
[6] Khan, M. R., et al. (2023). Analysis of elliptic curve cryptography & RSA. Journal of ICT Standardization, 11(4).
[7] Ketha, A. (2024). The evolution of cryptography and a contextual analysis of the major modern schemes.
[8] Weng, Z. (2025). Modern encryption algorithms comparative study: From symmetric to asymmetric systems. Academic Journal of Science and Technology.
[9] Khalaf, A. O., Salah, S. K., Sartep, H. J., &Abdalrdha, Z. K. (2019). Comparison between RSA, ECC & NTRU algorithms. International Journal of Engineering Research and Advanced Technology, 5(11). https://doi.org/10.31695/IJERAT.2019.3582
[10] Mahto, D., & Yadav, D. K. (2017). RSA and ECC: A comparative analysis. International Journal of Applied Engineering Research.
[11] Kumar, R. (2024). Design and analysis of computations using ECC and RSA. International Journal of Intelligent Systems and Applications in Engineering.
[12] Dar, M. A., Askar, A., Alyahya, D., & Bhat, S. A. (2021). Lightweight and secure ECC key exchange for mobile phones. International Journal of Interactive Mobile Technologies. https://doi.org/10.3991/ijim.v15i23.26337

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)