

**Enhancing Data Security in IoT Using Multi-Level Cryptographic Frameworks**  
**Humza Sohail (Nº109999)**

**Master in Computer Engineering**

**Supervisor:** Prof. Valderi Reis Quietinho Leithardt

**Co-Supervisor:** Prof. António Rui Trigo Ribeiro

2025

**Acknowledgment**

I would like to express my sincere gratitude to my advisor, Professor Valderi Reis Quietinho Leithardt, for his continuous support, guidance, and enthusiasm throughout this project. His expertise and encouragement have been instrumental in shaping the direction of my research.

I would also like to thank my co-supervisor, Professor António Rui Trigo Ribeiro, for his valuable insights and contributions. Their combined mentorship has been essential in the development of this work.

A special thanks to all those who have supported me during this journey, particularly my family and friends, for their unwavering encouragement and belief in me.

### **Abstract**

This project presents a cryptographic framework designed to improve data security and computational efficiency in Internet of Things (IoT) environments. Given the resource constraints of IoT devices and the increasing need for secure data transmission, the framework proposes a multi-level encryption model with four security levels: Guest, Basic, Advanced, and Admin. Each level incorporates progressively sophisticated encryption techniques to achieve an optimal balance between security and performance.

For Guest access, lightweight cryptographic combinations such as AES-256-GCM + RSA and ChaCha20 + ECC (Curve25519) ensure minimal computational overhead while maintaining essential security. The Basic level introduces secure configurations like AES-128-CCM + ChaCha20 and AES-256-GCM + ChaCha20 + RSA to protect general communications. At the Advanced level, multi-layer encryption strategies such as AES-128-CCM + AES-256-GCM + ChaCha20 are employed to provide enhanced security for critical operations. The Admin level deploys the most complex cryptographic configurations, including AES-256-CTR + Blowfish + ChaCha20 + ECC (Curve25519), to secure environments demanding the highest level of protection.

The framework emphasizes the integration of both symmetric and asymmetric cryptographic methods. Symmetric algorithms such as AES and ChaCha20 ensure computational efficiency, while asymmetric methods including ECC and RSA provide secure key exchanges and access control. By combining hybrid encryption techniques with edge computing for resource optimization, the framework ensures scalable and efficient data transmission.

Performance evaluations demonstrate that the proposed model supports secure and scalable data transmission in resource-constrained IoT environments, offering valuable insights for the future development of cryptographic protocols tailored for IoT applications.

**Keywords:** Cryptographic Algorithms, Data Security, Multi-level Encryption, IoT.

**Content**

Contents

[Abstract 5](#_Toc189734060)

[List of Figures 8](#_Toc189734061)

[List of tables 10](#_Toc189734062)

[LIST OF ACRONYMS 12](#_Toc189734063)

[List of Software Used 14](#_Toc189734064)

[CHAPTER 1 17](#_Toc189734065)

[INTRODUCTION 17](#_Toc189734066)

[CHAPTER 2 21](#_Toc189734067)

[Literature Review 21](#_Toc189734068)

[The industrial sector, particularly Industry 5.0, has seen a growing demand for cryptographic frameworks that ensure compliance with regulatory standards while safeguarding real-time data transmission. Yang and Zhao (2023) proposed a cryptographic framework tailored for Industry 5.0, emphasizing encryption, secure communication protocols, and real-time data protection. This work demonstrates the necessity of adaptable cryptographic solutions capable of supporting dynamic industrial environments [35]. PRISEC III builds upon these principles by offering enhanced flexibility and scalability for various sectors, including healthcare and smart grids. 22](#_Toc189734069)

[1. Cryptographic Algorithm Enhancements 23](#_Toc189734070)

[2. Packet Size Support 25](#_Toc189734071)

[3. Performance Improvements 25](#_Toc189734072)

[4. Role-Based Security Levels 26](#_Toc189734073)

[5. Data Integrity and Key Exchange Mechanisms 27](#_Toc189734074)

[6. Summary of Key Improvements 27](#_Toc189734075)

[2.3 RESEARCH QUESTIONS 28](#_Toc189734076)

[2.4 Conclusion 28](#_Toc189734077)

[chapter 3 29](#_Toc189734078)

[Mathematical Aspects of PRISEC III 29](#_Toc189734079)

[3.1 MATHEMATICAL ASPECTS OF PRISEC III 30](#_Toc189734080)

[3.1.1 Symmetric Encryption (AES, Blowfish, ChaCha20) 30](#_Toc189734081)

[3.1.2 Asymmetric Encryption (ECC and RSA) 33](#_Toc189734082)

[3.1.3 Hash Functions and HMAC (SHA-512) 34](#_Toc189734083)

[3.2 SELECTION OF CRYPTOGRAPHIC ALGORITHMS 35](#_Toc189734084)

[3.3 TOOLS FOR IMPLEMENTATION AND TESTING 36](#_Toc189734085)

[CHAPTER 4 43](#_Toc189734086)

[Implementation and testing of cryptographic algorithms 43](#_Toc189734087)

[4.1 Implementation 43](#_Toc189734088)

[Level (Guest) 44](#_Toc189734089)

[1-AES-128-CTR 44](#_Toc189734090)

[2-AES-256-GCM + RSA 45](#_Toc189734091)

[3-ChaCha20 + ECC (Curve25519) 47](#_Toc189734092)

[4-AES-128-CCM + ChaCha20 48](#_Toc189734093)

[5-AES-128-CCM + AES-192-CCM 50](#_Toc189734094)

[6-Blowfish + AES-128-CTR 51](#_Toc189734095)

[LEVEL (Basic) 52](#_Toc189734096)

[5-AES-128-CTR + ChaCha20 59](#_Toc189734097)

[LEVEL (ADVANCED) 64](#_Toc189734098)

[level (ADMIN) 81](#_Toc189734099)

[4.2 CONCLUSION 99](#_Toc189734100)

[Future Work 99](#_Toc189734101)

[CHAPTER 5 101](#_Toc189734102)

[Planning Section 101](#_Toc189734103)

[References 102](#_Toc189734104)

### **List of Figures**

1. **Figure 2.0** – Edge Computing in IoT
2. **Figure 2.1** – PRISEC1
3. **Figure 2.2** – PRISECII
4. **Figure 2.3** – PRISECIII
5. **Figure 4.0** – Results of the encryption and decryption time in the Guest level for AES-128-CTR
6. **Figure 4.1** – Results of the encryption and decryption time in the Guest level for AES-256-GCM + RSA
7. **Figure 4.2** – Results of the encryption and decryption time in the Guest level for ChaCha20 + ECC (Curve25519)
8. **Figure 4.3** – Results of the encryption and decryption time in the Guest level for AES-128-CCM + ChaCha20
9. **Figure 4.4** – Results of the encryption and decryption time in the Guest level for AES-128-CCM + AES-192-CCM
10. **Figure 4.5** – Results of the encryption and decryption time in the Guest level for Blowfish + AES-128-CTR
11. **Figure 4.6** – Results of the encryption and decryption time in the Basic level for AES-128-CCM + ChaCha20 + ECC (Curve25519)
12. **Figure 4.7** – Results of the encryption and decryption time in the Basic level for AES-256-GCM + ChaCha20 + RSA
13. **Figure 4.8** – Results of the encryption and decryption time in the Basic level for AES-256-CCM + ChaCha20-Poly1305
14. **Figure 4.9** – Results of the encryption and decryption time in the Basic level for AES-128-CCM + AES-192-CCM + XChaCha20
15. **Figure 4.10** – Results of the encryption and decryption time in the Basic level for AES-128-CTR + ChaCha20
16. **Figure 4.11** – Results of the encryption and decryption time in the Basic level for AES-192-CTR + Blowfish
17. **Figure 4.12** – Results of the encryption and decryption time in the Basic level for AES-192-CTR + ChaCha20
18. **Figure 4.13** – Results of the encryption and decryption time in the Basic level for AES-128-CTR + HMAC-SHA512
19. **Figure 4.14** – Results of the encryption and decryption time in the Advanced level for ChaCha20 + AES-256-GCM
20. **Figure 4.15** – Results of the encryption and decryption time in the Advanced level for AES-128-CCM + RSA
21. **Figure 4.16** – Results of the encryption and decryption time in the Advanced level for AES-128-CCM + AES-256-GCM + ECC (Curve25519)
22. **Figure 4.17** – Results of the encryption and decryption time in the Advanced level for AES-128-CCM + AES-256-CCM + ChaCha20
23. **Figure 4.18** – Results of the encryption and decryption time in the Advanced level for AES-256-CCM + XChaCha20 + ChaCha20
24. **Figure 4.19** – Results of the encryption and decryption time in the Advanced level for AES-192-CCM + XChaCha20
25. **Figure 4.20** – Results of the encryption and decryption time in the Advanced level for AES-256-CTR + ChaCha20
26. **Figure 4.21** – Results of the encryption and decryption time in the Advanced level for AES-128-CTR + Blowfish + ChaCha20
27. **Figure 4.22** – Results of the encryption and decryption time in the Advanced level for AES-192-CTR + ChaCha20 + ECC (Curve25519)
28. **Figure 4.23** – Results of the encryption and decryption time in the Advanced level for AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512
29. **Figure 4.24** – Results of the encryption and decryption time in the Advanced level for AES-256-CTR + Blowfish
30. **Figure 4.25** – Results of the encryption and decryption time in the Advanced level for AES-128-CTR + AES-256-CTR + ChaCha20
31. **Figure 4.26** – Results of the encryption and decryption time in the Admin level for AES-256-GCM + ChaCha20 + ECC (Curve25519)
32. **Figure 4.27** – Results of the encryption and decryption time in the Admin level for AES-128-CCM + ChaCha20 + RSA
33. **Figure 4.28** – Results of the encryption and decryption time in the Admin level for ChaCha20 + ECC (Curve25519) + RSA
34. **Figure 4.29** – Results of the encryption and decryption time in the Admin level for AES-256-CCM + AES-128-CCM + ChaCha20
35. **Figure 4.30** – Results of the encryption and decryption time in the Admin level for AES-192-CCM + AES-256-CCM + XChaCha20
36. **Figure 4.31** – Results of the encryption and decryption time in the Admin level for AES-128-CCM + ChaCha20-Poly1305 + XChaCha20
37. **Figure 4.32** – Results of the encryption and decryption time in the Admin level for AES-256-CTR + ChaCha20 + ECC (Curve25519)
38. **Figure 4.33** – Results of the encryption and decryption time in the Admin level for AES-128-CTR + Blowfish
39. **Figure 4.34** – Results of the encryption and decryption time in the Admin level for AES-256-CTR + Blowfish
40. **Figure 4.35** – Results of the encryption and decryption time in the Admin level for AES-128-CTR + Blowfish + ChaCha20 + ECC (Curve25519)
41. **Figure 4.36** – Results of the encryption and decryption time in the Admin level for AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512 + ECC (Curve25519)
42. **Figure 4.37** – Results of the encryption and decryption time in the Admin level for AES-128-CTR + Blowfish + ChaCha20 + HMAC-SHA512
43. **Figure 4.38** – Results of the encryption and decryption time in the Admin level for AES-256-CTR + Blowfish + ECC (Curve25519)

### **List of tables**

1. **Table 4.0** – Results of the encryption and decryption time in the Guest level for AES-128-CTR
2. **Table 4.1** – Results of the encryption and decryption time in the Guest level for AES-256-GCM + RSA
3. **Table 4.2** – Results of the encryption and decryption time in the Guest level for ChaCha20 + ECC (Curve25519)
4. **Table 4.3** – Results of the encryption and decryption time in the Guest level for AES-128-CCM + ChaCha20
5. **Table 4.4** – Results of the encryption and decryption time in the Guest level for AES-128-CCM + AES-192-CCM
6. **Table 4.5** – Results of the encryption and decryption time in the Guest level for Blowfish + AES-128-CTR
7. **Table 4.6** – Results of the encryption and decryption time in the Basic level for AES-128-CCM + ChaCha20 + ECC (Curve25519)
8. **Table 4.7** – Results of the encryption and decryption time in the Basic level for AES-256-GCM + ChaCha20 + RSA
9. **Table 4.8** – Results of the encryption and decryption time in the Basic level for AES-256-CCM + ChaCha20-Poly1305
10. **Table 4.9** – Results of the encryption and decryption time in the Basic level for AES-128-CCM + AES-192-CCM + XChaCha20
11. **Table 4.10** – Results of the encryption and decryption time in the Basic level for AES-128-CTR + ChaCha20
12. **Table 4.11** – Results of the encryption and decryption time in the Basic level for AES-192-CTR + Blowfish
13. **Table 4.12** – Results of the encryption and decryption time in the Basic level for AES-192-CTR + ChaCha20
14. **Table 4.13** – Results of the encryption and decryption time in the Basic level for AES-128-CTR + HMAC-SHA512
15. **Table 4.14** – Results of the encryption and decryption time in the Advanced level for ChaCha20 + AES-256-GCM
16. **Table 4.15** – Results of the encryption and decryption time in the Advanced level for AES-128-CCM + RSA
17. **Table 4.16** – Results of the encryption and decryption time in the Advanced level for AES-128-CCM + AES-256-GCM + ECC (Curve25519)
18. **Table 4.17** – Results of the encryption and decryption time in the Advanced level for AES-128-CCM + AES-256-CCM + ChaCha20
19. **Table 4.18** – Results of the encryption and decryption time in the Advanced level for AES-256-CCM + XChaCha20 + ChaCha20
20. **Table 4.19** – Results of the encryption and decryption time in the Advanced level for AES-192-CCM + XChaCha20
21. **Table 4.20** – Results of the encryption and decryption time in the Advanced level for AES-256-CTR + ChaCha20
22. **Table 4.21** – Results of the encryption and decryption time in the Advanced level for AES-128-CTR + Blowfish + ChaCha20
23. **Table 4.22** – Results of the encryption and decryption time in the Advanced level for AES-192-CTR + ChaCha20 + ECC (Curve25519)
24. **Table 4.23** – Results of the encryption and decryption time in the Advanced level for AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512
25. **Table 4.24** – Results of the encryption and decryption time in the Advanced level for AES-256-CTR + Blowfish
26. **Table 4.25** – Results of the encryption and decryption time in the Advanced level for AES-128-CTR + AES-256-CTR + ChaCha20
27. **Table 4.26** – Results of the encryption and decryption time in the Admin level for AES-256-GCM + ChaCha20 + ECC (Curve25519)
28. **Table 4.27** – Results of the encryption and decryption time in the Admin level for AES-128-CCM + ChaCha20 + RSA
29. **Table 4.28** – Results of the encryption and decryption time in the Admin level for ChaCha20 + ECC (Curve25519) + RSA
30. **Table 4.29** – Results of the encryption and decryption time in the Admin level for AES-256-CCM + AES-128-CCM + ChaCha20
31. **Table 4.30** – Results of the encryption and decryption time in the Admin level for AES-192-CCM + AES-256-CCM + XChaCha20
32. **Table 4.31** – Results of the encryption and decryption time in the Admin level for AES-128-CCM + ChaCha20-Poly1305 + XChaCha20
33. **Table 4.32** – Results of the encryption and decryption time in the Admin level for AES-256-CTR + ChaCha20 + ECC (Curve25519)
34. **Table 4.33** – Results of the encryption and decryption time in the Admin level for AES-128-CTR + Blowfish
35. **Table 4.34** – Results of the encryption and decryption time in the Admin level for AES-256-CTR + Blowfish
36. **Table 4.35** – Results of the encryption and decryption time in the Admin level for AES-128-CTR + Blowfish + ChaCha20 + ECC (Curve25519)
37. **Table 4.36** – Results of the encryption and decryption time in the Admin level for AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512 + ECC (Curve25519)
38. **Table 4.37** – Results of the encryption and decryption time in the Admin level for AES-128-CTR + Blowfish + ChaCha20 + HMAC-SHA512
39. **Table 4.38** – Results of the encryption and decryption time in the Admin level for AES-256-CTR + Blowfish + ECC (Curve25519)

### **LIST OF ACRONYMS**

**AES-CTR**: Advanced Encryption Standard Counter Mode

**AES-CCM**: Advanced Encryption Standard Counter with CBC-MAC

**AES-GCM**: Advanced Encryption Standard Galois/Counter Mode

**Blowfish**: A symmetric block cipher encryption algorithm

**ChaCha20**: A high-speed stream cipher for secure encryption

**XChaCha20:** Extended ChaCha20 with a longer nonce

**ChaCha20-Poly1305**: A combination of ChaCha20 stream cipher and Poly1305 MAC

**ECC**: Elliptic-Curve Cryptography

**Curve25519**: A widely used elliptic curve for high-performance key exchange

**HMAC**: Hash Message Authentication Code

**HMAC-SHA512**: HMAC using SHA-512 hashing algorithm

**HTML**: Hypertext Markup Language

**HTTP**: Hypertext Transfer Protocol

**IoT**: Internet of Things

**PKI**: Public Key Infrastructure

**RSA**: Rivest-Shamir-Adleman (Asymmetric encryption algorithm)

**SHA**: Secure Hash Algorithm

**TLS**: Transport Layer Security

**XOR**: Exclusive OR logical operation

**Poly1305**: Message Authentication Code (MAC) used for ensuring data integrity

**CTR**: Counter Mode (block cipher mode of operation)

**CBC**: Cipher Block Chaining

**GCM**: Galois/Counter Mode (encryption mode providing confidentiality and integrity)

**VM**: Virtual Machine

**LAN**: Local Area Network

### **List of Software Used**

**Git**: Version control system

**Microsoft Excel**: Spreadsheet software for data analysis and visualization

**Microsoft Word**: Word processing software for documentation

**Python**: Programming language for cryptographic algorithm implementation

**Visual Studio Code (VS Code)**: Code editor with extensive extensions for Python development

**GitHub**: Code hosting platform for version control and collaboration

**Adobe Photoshop**: Image editing software

**VMware Workstation**: Virtual machine software for creating virtual environments

**Terraform**: Infrastructure as code software

**Figma**: UI/UX design and prototyping tool

**PyCryptodome**: Python library for cryptographic functions (AES, Blowfish, ECC, etc.)

**Highcharts**: JavaScript-based charting library for visualizing encryption algorithm performance

**Matplotlib**: Python library for creating static, animated, and interactive visualizations

**NumPy**: Python library for numerical computations during cryptographic testing

**Pandas**: Python data manipulation library for dataset handling

**Wireshark**: Network protocol analyzer for monitoring encryption-related network traffic

**Jupyter Notebook**: Interactive environment for writing and testing Python code

**OpenSSL**: Toolkit for implementing SSL/TLS protocols and cryptographic functions

**Docker**: Containerization platform for deploying lightweight, isolated application environments

**Seaborn**: Data visualization library used alongside Matplotlib

**PyTest**: Testing framework for validating cryptographic function outputs

# **CHAPTER 1**

## INTRODUCTION

#### **1.1 Overview**

In recent years, the integration of IoT technologies into daily life and critical business operations has given rise to new security challenges. From healthcare devices to home automation systems, IoT applications are revolutionizing industries by connecting billions of devices across a network. However, the rapid growth of IoT devices introduces significant vulnerabilities in data security, especially considering the limited computational power of many IoT devices. These devices often cannot implement complex cryptographic protocols due to hardware constraints, making them easy targets for malicious attacks. Thus, ensuring the security of sensitive data in transit remains a pressing concern, particularly for applications that require real-time processing, such as healthcare systems, smart grids, and autonomous vehicles [25][27].

Cryptography is the cornerstone of ensuring data security within IoT ecosystems. It involves the application of various algorithms that encrypt data, ensuring that only authorized users can access the transmitted information. Cryptographic techniques help safeguard sensitive information, such as personal and medical data, from being intercepted or tampered with while traversing the interconnected systems in IoT networks [5][19]. By employing effective cryptographic methods, we can achieve three core security goals: confidentiality, integrity, and authenticity of data [14].

In this project, we explore the application of cryptographic algorithms within the framework of edge computing to secure data in IoT environments. Edge computing processes data closer to the source, reducing latency and network congestion by limiting the need to send data to centralized cloud servers. This distributed model not only accelerates real-time data processing but also enhances the security and privacy of IoT systems by reducing the exposure of sensitive information over long distances [29][30]. By integrating cryptographic algorithms directly within edge devices, the project aims to improve both the security and computational efficiency of IoT systems [27].

#### **1.2 Motivation and Background**

As IoT applications continue to proliferate, the potential risks associated with their vulnerabilities have become more evident. IoT networks are inherently susceptible to a variety of attacks, including unauthorized data access, data breaches, and denial-of-service (DoS) attacks. While many IoT applications focus on network security, they often neglect the protection of sensitive data transmitted between devices, particularly in scenarios involving high-value personal data [19][27].

Additionally, the implementation of new data transmission architectures, such as Named Data Networking (NDN), has introduced new security risks, including increased exposure to DoS and DDoS attacks, which can severely disrupt IoT applications [18]. These attacks, combined with the rapid expansion of IoT networks, have made it crucial to investigate and implement more effective cryptographic solutions [25][28].

The motivation for this project stems from the growing concern over the security of IoT systems and the need for cryptographic solutions that offer a balance between robustness and computational efficiency. The goal is to investigate cryptographic algorithms suitable for low-resource IoT devices, such as symmetric (AES, ChaCha20) and asymmetric (RSA, ECC) encryption techniques, and implement them within the edge computing framework. By doing so, this project seeks to ensure that IoT devices can secure data transmissions without sacrificing performance due to the computational constraints of the devices [3][9][13].

#### **1.3 Objectives of the Project**

The primary objectives of this project are as follows:

* **Cryptographic Algorithm Evaluation:** This project aims to identify and evaluate cryptographic algorithms that offer optimal encryption and decryption speeds while maintaining a high level of security. Symmetric algorithms such as AES (in its variants: AES-128-CTR, AES-256-GCM, AES-128-CCM, and AES-192-CTR), ChaCha20, and XChaCha20 are considered for their efficiency. Asymmetric algorithms like ECC (Curve25519) and RSA are included for secure key exchanges and access control, while hybrid combinations (AES + ChaCha20 + ECC, AES + Blowfish, etc.) ensure enhanced performance for IoT environments.
* **Edge Computing Integration:** The project proposes a cryptographic model integrated within an edge computing framework to facilitate the secure and efficient transmission of data across IoT systems. By processing encryption operations at the edge, the system seeks to reduce latency and computational overhead on IoT devices.
* **Performance Analysis:** The selected cryptographic algorithms will be tested in real-world IoT applications. Performance evaluations will consider various factors, such as packet size, network conditions, and the quantity of transmitted data. Combinations like AES-256-CTR + Blowfish + ChaCha20 for Admin levels and AES-128-CCM + ChaCha20 for Guest access will be analyzed to determine their impact on speed, energy consumption, and security.
* **Development of a Cryptographic Security Model:** The project aims to develop a scalable and efficient cryptographic security model tailored to IoT environments. This model will address energy efficiency, encryption speed, and minimal impact on device performance by employing multi-level encryption strategies suited to varying security requirements—Guest, Basic, Advanced, and Admin.

**1.3 Cryptography and the PRISEC III Framework**

Cryptography plays a fundamental role in securing data in IoT environments. There are two main types of cryptographic techniques:

• **Symmetric Cryptography**: Involves the use of a single shared key for both encryption and decryption, offering fast encryption speeds. Examples include the Advanced Encryption Standard (AES) and ChaCha20 [1][2][9].

• **Asymmetric Cryptography**: Involves the use of a pair of keys: a public key for encryption and a private key for decryption. Examples include RSA and Elliptic Curve Cryptography (ECC) [3][10][11].

The PRISEC (Privacy Security) framework is designed to provide cryptographic protocols for securing IoT communications. It features a multi-layered security approach with different security configurations (Guest, Basic, Advanced, and Admin), depending on the level of data sensitivity and the environment in which the data is being transmitted. The PRISEC framework combines both symmetric and asymmetric cryptographic techniques to offer flexibility and scalability for different security requirements [30].

In this project, PRISEC III will be integrated into the edge computing environment to secure IoT applications, ensuring that data confidentiality, integrity, and authenticity are upheld across multiple IoT use cases. The project will assess which configuration of PRISEC offers the best security performance in various real-world applications, with a focus on optimizing the trade-off between security and computational efficiency [29][30].

#### **1.4 Report Organization**

This document is structured as follows:

• **Chapter 1:** Introduces the problem and objectives.

• **Chapter 2**: presents the literature review.

• **Chapter 3:** Describes the mathematical aspects of PRISEC III.

• **Chapter 4**: Implementation and testing of cryptographic algorithms

• **Chapter 5:** Planning.

# **CHAPTER 2**

### **Literature Review**

This chapter provides a comprehensive review of cryptographic solutions, emphasizing their implementation in real-time systems, edge computing environments, and IoT networks. By analyzing previous works, this literature review highlights the security challenges in decentralized networks, performance limitations on resource-constrained devices, and strategies for secure communication. The insights gained from this review lay the groundwork for PRISEC III, a robust framework that seeks to optimize both security and efficiency in edge-based IoT applications.

#### **2.1 Related Works**

The increasing reliance on distributed computing frameworks like edge computing has amplified concerns over data security. Real-time systems require cryptographic techniques that can secure data without introducing significant latency. A foundational study by Schneier (1996) in *Applied Cryptography* categorized and evaluated security mechanisms for real-time systems, introducing the "attacker's burden" metric to quantify security effectiveness [14]. This work served as a precursor for the development of scheduler-based security techniques, which remain critical for IoT applications demanding low-latency responses.  
In decentralized systems, security risks arise due to the absence of a trusted central authority and the vulnerability of individual nodes. Peinado's (2011) research on lightweight cryptographic algorithms highlighted the trade-offs between security and computational performance in decentralized IoT environments. By benchmarking widely deployed algorithms on devices with varying resource capacities, the study underscored the need for cryptographic solutions tailored to constrained environments [33]. PRISEC III addresses this challenge by integrating multi-layer encryption mechanisms that provide robust security without compromising performance.

### The industrial sector, particularly Industry 5.0, has seen a growing demand for cryptographic frameworks that ensure compliance with regulatory standards while safeguarding real-time data transmission. Yang and Zhao (2023) proposed a cryptographic framework tailored for Industry 5.0, emphasizing encryption, secure communication protocols, and real-time data protection. This work demonstrates the necessity of adaptable cryptographic solutions capable of supporting dynamic industrial environments [35]. PRISEC III builds upon these principles by offering enhanced flexibility and scalability for various sectors, including healthcare and smart grids.

Emerging cryptographic techniques have sought to balance security and efficiency in resource-constrained environments. Harsh and Khandelwal (2019) proposed a hybrid framework that combined Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) to optimize memory usage and energy efficiency while maintaining strong security [21]. Building on this work, PRISEC III incorporates both ECC and AES in its security architecture, providing a scalable solution for edge-based IoT systems.

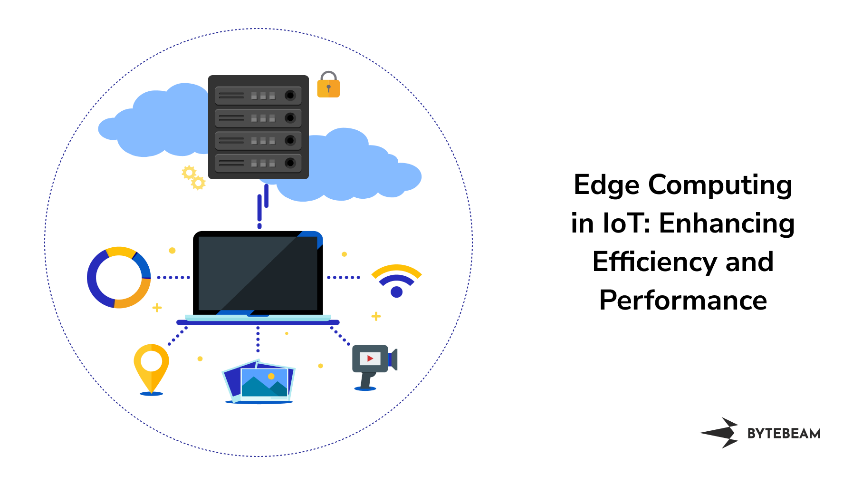


Figure 2.0 – Edge Computing in IoT.

Recent evaluations of symmetric key algorithms by Boneh and Shoup (2017) highlighted the performance characteristics of different cryptographic techniques, including encryption and decryption times, throughput, and energy consumption. The study identified lightweight algorithms such as ChaCha20 and AES-256-GCM as ideal for environments with constrained resources [20]. PRISEC III leverages this insight by integrating these algorithms, ensuring faster processing with smaller data packets and reducing latency in real-time applications.

#### **2.2 Comparison of Cryptographic Algorithms PRISEC I PRISEC II and PRISEC III**

The development from PRISEC I to PRISEC III represents a substantial advancement in cryptographic robustness, performance efficiency, data handling capabilities, and overall security features. Each version was designed to address the limitations of its predecessor, focusing on enhancing security, improving performance, supporting larger datasets, and introducing dynamic, role-based encryption strategies.

### **1. Cryptographic Algorithm Enhancements**

#### **PRISEC I**

PRISEC I utilized simple cryptographic techniques, heavily relying on Base64 encoding combined with AES encryption at various levels.

* **Guest:** Only Base64 encoding was employed, offering minimal security.
* **Basic:** Base64 combined with AES-128 encryption for modest protection.
* **Advanced:** Added AES-192 alongside AES-128 and Base64.
* **Admin:** Implemented Base64, AES-128, AES-192, and AES-256 sequentially, but lacked advanced integrity verification and secure key exchange mechanisms.

This version was vulnerable to sophisticated attacks and unsuitable for large-scale data applications due to its single-layer encryption approach.

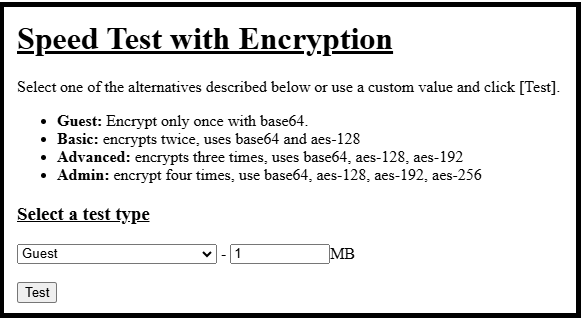


Figure 2.1 – PRISEC I Algorithm

#### **PRISEC II**

PRISEC II introduced stronger cryptographic techniques to address the security and scalability limitations of PRISEC I.

* **Guest:** AES-256 encryption was standard, significantly strengthening data protection.
* **Basic:** Combined AES-256 with AES-CTR for enhanced performance, especially for streaming data.
* **Advanced:** Added HMAC-SHA256 to verify data integrity alongside AES-256 and AES-CTR.
* **Admin:** Integrated ECC (Elliptic Curve Cryptography) for secure key exchanges along with AES-256, AES-CTR, and HMAC-SHA256.

These improvements strengthened cryptographic security but introduced performance bottlenecks at the Admin level due to ECC operations

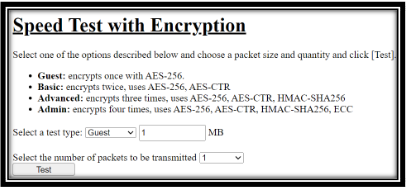


Figure 2.2 – PRISEC II Algorithm

#### **PRISEC III**

PRISEC III represents a paradigm shift by adopting multi-layer encryption techniques and optimizing both performance and security.

* **Guest:** Utilized AES-256-GCM and ChaCha20, providing robust encryption and improved speed.
* **Basic:** Incorporated HMAC-SHA512 alongside AES-256-GCM and ChaCha20.
* **Advanced:** Included ECC (Curve25519) for secure key exchanges along with AES-256-GCM, ChaCha20, and HMAC-SHA512.
* **Admin:** Maintained the Advanced configuration but optimized further for secure high-performance operations.

These advancements make PRISEC III the most secure and efficient version to date.

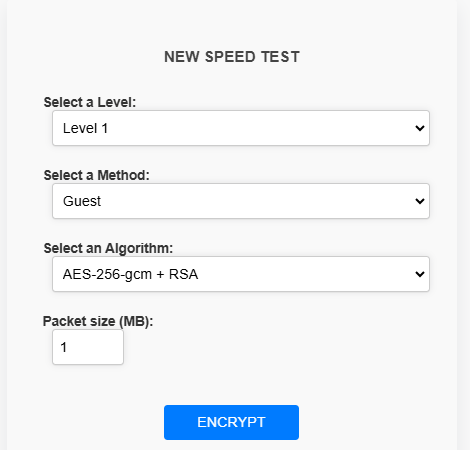


Figure 2.2 – PRISEC III Algorithm

### **2. Packet Size Support**

* **PRISEC I:** Supported data packet sizes from 1MB to 50MB. Performance degraded significantly with larger datasets due to limited block encryption scalability.
* **PRISEC II:** Maintained the same packet size limit of 1MB to 50MB but handled data more efficiently with AES-CTR. However, it still faced challenges with larger datasets.
* **PRISEC III:** Expanded packet size support up to 100MB, leveraging optimized stream and block cipher combinations to ensure efficient data handling for both small and large datasets.

### **3. Performance Improvements**

* **PRISEC I:** Slower encryption and decryption processes, especially for large packets, due to the sequential application of multiple AES encryption layers.
* **PRISEC II:** Moderate performance improvement with the introduction of AES-CTR, which optimized streaming data encryption. However, ECC computations for Admin roles added computational overhead.
* **PRISEC III:** High performance achieved through ChaCha20 for smaller packets and AES-256-GCM for larger datasets, ensuring minimal latency and efficient processing.

### **4. Role-Based Security Levels**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Guest** | **Basic** | **Advanced** | **Admin** | **Security Enhancements** |
| **PRISEC I** | Base64 | Base64 + AES-128 | Base64 + AES-128 + AES-192 | Base64 + AES-128 + AES-192 + AES-256 | Limited encryption, weak against sophisticated attacks. Vulnerable due to reliance on Base64 for Guest. |
| **PRISEC II** | AES-256 | AES-256 + AES-CTR | AES-256 + AES-CTR + HMAC-SHA256 | AES-256 + AES-CTR + HMAC-SHA256 + ECC | Introduction of AES-CTR and HMAC-SHA256 strengthens confidentiality and integrity. ECC enhances secure key exchanges. |
| **PRISEC III** | AES-256-GCM + ChaCha20 | AES-256-GCM + ChaCha20 + HMAC-SHA512 | AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512 | AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512 + ECC (Curve25519) | Introduction of AES-CTR and HMAC-SHA256 strengthens confidentiality and integrity. ECC enhances secure key exchanges. |

Table 2.0 – **Role-Based Security Levels**.

#### **Key Observations:**

* PRISEC I lacked dynamic adaptability and provided weak protection for lower roles.
* PRISEC II introduced strong encryption across all roles but remained static in its implementation.
* PRISEC III implements a fully modular framework with dynamic adaptability, ensuring robust protection tailored to each user role.

### **5. Data Integrity and Key Exchange Mechanisms**

* **PRISEC I:** No integrity verification mechanisms beyond basic encryption.
* **PRISEC II:** Introduced HMAC-SHA256 for data integrity and ECC for secure key exchanges at the Admin level.
* **PRISEC III:** Upgraded to HMAC-SHA512 for stronger integrity verification and adopted ECC (Curve25519) for efficient and secure key exchanges.

### **6. Summary of Key Improvements**

|  |  |  |  |
| --- | --- | --- | --- |
| **Aspect** | **PRISEC I** | **PRISEC II** | **PRISEC III** |
| **Algorithm Complexity** | Simple (Base64, AES) | Moderate (AES-CTR, ECC) | Complex (AES-GCM, ChaCha20, ECC) |
| **Security Strength** | Low to Moderate | Moderate to Strong | Strong to Robust |
| **Data Integrity** | None | HMAC-SHA256 | HMAC-SHA512 |
| **Performance** | Low | Moderate | High |
| **Scalability** | Limited (up to 50MB) | Improved (up to 50MB) | Efficient (up to 100MB) |
| **User Roles** | Weak Guest security | Strong but static | Dynamic and robust |

Table 2.1 – **Summary of Key Improvements**

### **2.3 RESEARCH QUESTIONS**

The following research questions guide the objectives and development of PRISEC III:

1. Which cryptographic algorithms provide the optimal balance between security and performance for resource-constrained IoT devices?
2. How can edge computing frameworks be integrated with cryptographic techniques to enhance data security without compromising efficiency?
3. What impact does packet size, network conditions, and data quantity have on the performance of cryptographic algorithms in IoT environments?
4. How can multi-layer encryption models improve the robustness of IoT security systems while remaining scalable?
5. What role does role-based security play in enhancing flexibility and adaptability in cryptographic frameworks for IoT applications?

### **2.4 Conclusion**

The progression from PRISEC I to PRISEC III demonstrates a continuous effort to enhance cryptographic security, performance, and scalability. PRISEC III stands out as a comprehensive solution, integrating advanced algorithms, stronger data integrity mechanisms, and a modular, role-based security framework. These advancements ensure that PRISEC III meets the demands of modern applications, offering robust protection and efficient data handling for both small and large datasets.

# **chapter 3**

## **Mathematical Aspects of PRISEC III**

This chapter delves into the mathematical foundations and cryptographic mechanisms integral to the PRISEC system. The discussion covers key algorithms, their mathematical principles, and their suitability for securing edge computing environments. In addition, the tools and server configurations used in the implementation are highlighted. These components collectively form the security backbone of PRISEC, enabling secure communication, data integrity, and performance optimization in resource-constrained environments.

### **3.1 MATHEMATICAL ASPECTS OF PRISEC III**

The cryptographic algorithms employed in PRISEC III rely on various mathematical concepts, including algebraic structures, finite field operations, prime factorization problems, and hash functions. These techniques ensure data confidentiality, integrity, and authenticity in edge computing systems. Below is a comprehensive overview of the mathematics behind each selected algorithm:

### **3.1.1 Symmetric Encryption (AES, Blowfish, ChaCha20)**

**Advanced Encryption Standard (AES)**  
AES is a block cipher that encrypts fixed-size blocks (128 bits) using keys of 128, 192, or 256 bits. The mathematical security of AES is derived from several core operations over a Galois Field GF(28)[9, 5].

* **Key Transformations:** AES encryption consists of multiple rounds (10 for 128-bit keys, 12 for 192-bit keys, and 14 for 256-bit keys). Each round applies four operations:
  1. **SubBytes:** Non-linear substitution using an S-box derived from finite field arithmetic over GF(28).
  2. **ShiftRows:** Circular shifting of rows in the state matrix.
  3. **MixColumns:** A linear transformation involving matrix multiplication over GF(28).
  4. **AddRoundKey:** XOR operation between the state and a round-specific key derived from the main key.
* **Security Strength:** The strength of AES comes from its resistance to differential and linear cryptanalysis, achieved through the combination of substitution-permutation and key scheduling mechanisms.

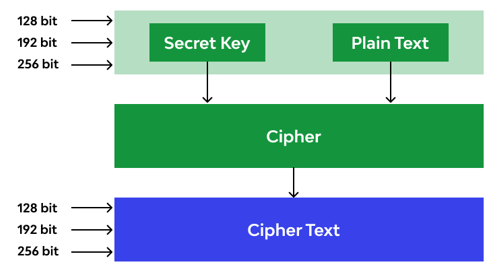


Figure 3.0 **– Advanced Encryption Standard (AES)**

**Blowfish**  
Blowfish operates as a Feistel network and processes data in 64-bit blocks using a variable-length key (32 to 448 bits)[10].

* **Feistel Structure:** Data is divided into two halves, L and R, and processed iteratively using the equation:

Li+1=Ri,Ri+1=Li⊕F(Ri,Ki)

Where F is a complex function involving substitution boxes (S-boxes) and permutation boxes (P-boxes).

* **Security and Efficiency:** The design of Blowfish ensures fast encryption while maintaining strong security properties.

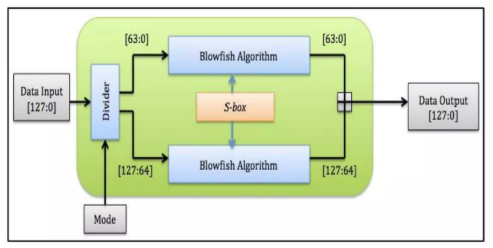


Figure 3.1 **– Advanced Encryption Standard (AES)**

**ChaCha20**  
ChaCha20 is a stream cipher that uses simple arithmetic operations for efficient and secure encryption[2, 15]..

* **Mathematical Operations:** ChaCha20's core operations are:
  + Addition modulo 232
  + XOR operation
  + Bitwise rotations
  + The cipher applies 20 rounds of transformations to generate a secure keystream.
* **Security:** The simplicity of ChaCha20's operations makes it resistant to side-channel attacks and ensures high performance.

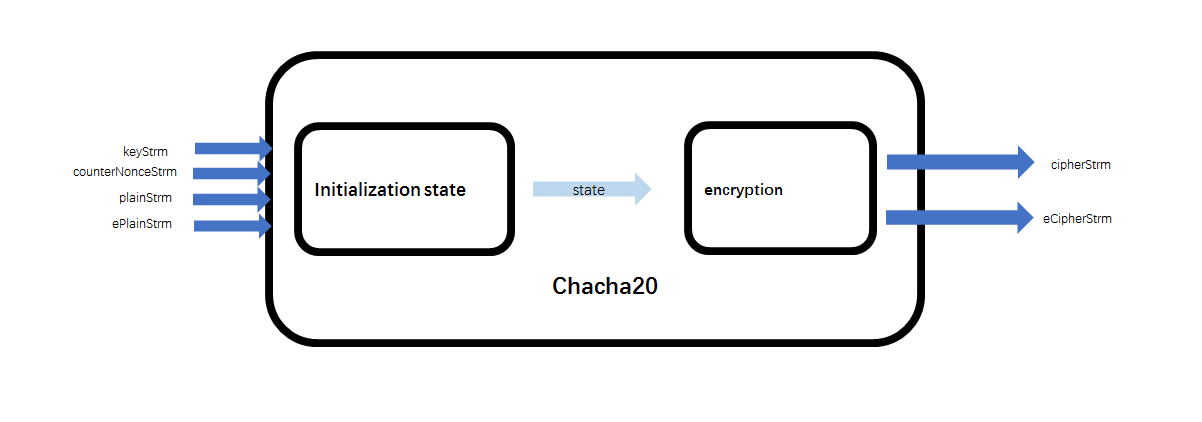


Figure 3.3 **– ChaCha20**

### **3.1.2 Asymmetric Encryption (ECC and RSA)**

**Elliptic Curve Cryptography (ECC)**  
ECC is based on the mathematics of elliptic curves over finite fields. An elliptic curve is defined by the equation:

Y2= x3+ ax + b mod p

where a and b are constants satisfying 4a3+27b2≠.

* **Point Addition and Scalar Multiplication:** ECC operations involve point addition and scalar multiplication on the curve. Given a point PP on the curve, scalar multiplication *KP* (repeated point addition) is computationally intensive and forms the basis of ECC security.
* **Security:** The security of ECC relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), making it more efficient than RSA for equivalent security levels.

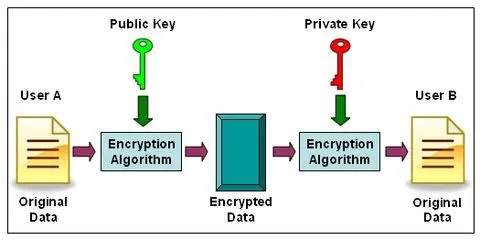


Figure 3.4 **– Elliptic Curve Cryptography (ECC)**

**RSA (Rivest-Shamir-Adleman)**  
RSA is based on the difficulty of factoring large composite numbers[11, 5].

* **Mathematical Foundations:**
  + Select two large primes’ p and q.
  + Compute n=p×q and ϕ(n)=(p−1)(q−1).
  + Choose an integer such that 1<e<ϕ(n) and gcd(e,ϕ(n))=1.
  + Compute the private key d such that d×e≡1mod  ϕ(n).
* **Encryption and Decryption:**

c=me mod n, m=cd mod n

Where m is the plaintext, c is the ciphertext, and n is the modulus.

* **Security:** The strength of RSA comes from the difficulty of prime factorization for large n.

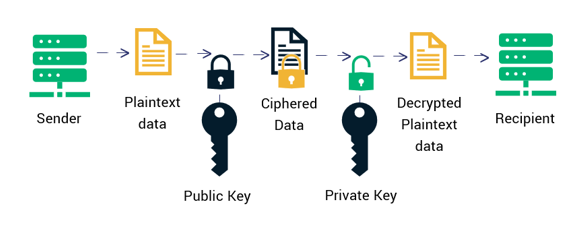


Figure 3.5 **– RSA (Rivest-Shamir-Adleman)**

### **3.1.3 Hash Functions and HMAC (SHA-512)**

**SHA-512 (Secure Hash Algorithm)**  
SHA-512 is a cryptographic hash function that produces a 512-bit output[9, 14].

* **Mathematical Operations:**
  + Processes data in 1024-bit blocks.
  + Uses modular additions, bitwise operations, and message expansion functions.
  + Applies 80 rounds of transformations to generate the hash value.
* **Security:** SHA-512 is resistant to collision, pre-image, and second pre-image attacks, making it suitable for secure message integrity verification.

**HMAC (Hashed Message Authentication Code)**  
HMAC combines a cryptographic hash function with a secret key to ensure data integrity[6, 15].

* **Mathematical Formula:**

HMAC (K, m) = H ((K⊕opad) ∣∣H ((K⊕ipad) ∣∣m))

Where H is the hash function, and opad and ipad are padding constants.

* **Security:** HMAC protects against message modification and replay attacks.

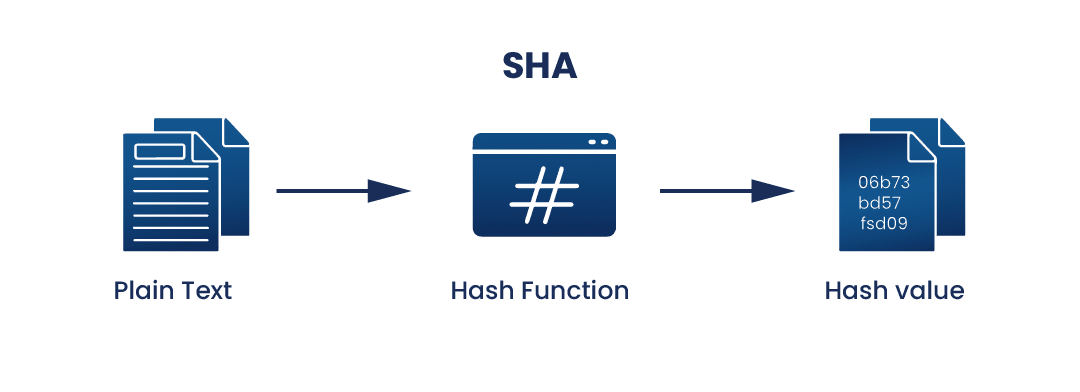


Figure 3.7 **– SHA-512 (Secure Hash Algorithm)**

### **3.2 SELECTION OF CRYPTOGRAPHIC ALGORITHMS**

The cryptographic algorithms selected for PRISEC include AES, Blowfish, ChaCha20, ECC, RSA, and HMAC-SHA512. These algorithms were chosen for their compatibility with edge computing environments, offering a balance between security, performance, and computational efficiency[19, 20].

### **3.3 TOOLS FOR IMPLEMENTATION AND TESTING**

#### **3.3.1 Python Programming Language**

Python was selected for its simplicity, readability, and extensive ecosystem of libraries, making it a powerful tool for rapid development and testing of secure applications. Its ease of use and high-level nature allow for quick implementation of complex cryptographic algorithms, minimizing development time and enhancing productivity. Additionally, Python's dynamic typing and flexible syntax enable developers to rapidly adapt code as security needs evolve, making it an excellent choice for prototyping and testing cryptographic solutions.

* **PyCryptodome**: This widely-used cryptographic library offers an array of robust tools for implementing well-known cryptographic algorithms, including AES, Blowfish, RSA, ChaCha20, and Elliptic Curve Cryptography (ECC). PyCryptodome provides secure and efficient implementations of key management, encryption, decryption, digital signatures, and hashing functions. The library also supports various modes of encryption such as GCM, CCM, and CTR, ensuring flexibility in securing data in different contexts. Its comprehensive and actively maintained functionality makes it a go-to choice for cryptographic operations in Python.
* **Efficiency**: Python’s flexibility is another key advantage, especially when integrating cryptographic operations into broader server-based or distributed systems. Its integration with other technologies and frameworks allows for seamless deployment of cryptographic functionality in environments ranging from web servers to cloud-based systems. Python’s extensive standard library also simplifies tasks like system interaction, network communication, and multi-threading, which are often necessary for scalable and secure applications. Furthermore, its ease of integration with databases and external APIs ensures that cryptographic solutions can be embedded within diverse ecosystems, providing both security and performance optimization.

.Below is the enhanced code with encryption and decryption for **RSA**, **AES**, **Blowfish**, **ECC**, **ChaCha20**, **ChaCha20-Poly1305**, and **HMAC-SHA512**.

**Code with Encryption and Decryption:**

**from** **Crypto.PublicKey** **import** RSA

**from** **Crypto.Cipher** **import** AES, Blowfish, ChaCha20, ChaCha20\_Poly1305

**from** **Crypto.Random** **import** get\_random\_bytes

**from** **Crypto.Hash** **import** SHA512, HMAC

**from** **Crypto.Protocol.KDF** **import** PBKDF2

**from** **Crypto.Util.Padding** **import** pad, unpad

**from** **cryptography.hazmat.primitives** **import** hashes

**from** **cryptography.hazmat.primitives.asymmetric** **import** ec

**from** **cryptography.hazmat.primitives.asymmetric** **import** padding

**from** **cryptography.hazmat.primitives** **import** hashes

**from** **cryptography.hazmat.backends** **import** default\_backend

**import** **time**

# Generate RSA keys for Advanced and Admin

rsa\_key = RSA.generate(**2048**)

public\_key = rsa\_key.publickey()

rsa\_cipher = PKCS1\_OAEP.new(public\_key)

# Generate shared secret for ECC (Curve25519)

**def** **shared\_secret**():

**return** get\_random\_bytes(**32**) # Simulated shared secret for ECC

# Utility function to generate data packets of a given size

**def** **generate\_packet**(size):

**return** get\_random\_bytes(size)

# Encryption and decryption functions

# AES-128 CCM Encryption and Decryption

**def** **aes\_128\_ccm\_encrypt**(data, key):

cipher = AES.new(key, AES.MODE\_CCM)

nonce = cipher.nonce

start = time.time()

ciphertext, tag = cipher.encrypt\_and\_digest(data)

end = time.time()

**return** nonce, ciphertext, tag, end - start

**def** **aes\_128\_ccm\_decrypt**(ciphertext, key, nonce, tag):

cipher = AES.new(key, AES.MODE\_CCM, nonce=nonce)

start = time.time()

plain = cipher.decrypt\_and\_verify(ciphertext, tag)

end = time.time()

**return** plain, end - start

# AES-192 CCM Encryption and Decryption

**def** **aes\_192\_ccm\_encrypt**(data, key):

cipher = AES.new(key, AES.MODE\_CCM)

nonce = cipher.nonce

start = time.time()

ciphertext, tag = cipher.encrypt\_and\_digest(data)

end = time.time()

**return** nonce, ciphertext, tag, end - start

**def** **aes\_192\_ccm\_decrypt**(ciphertext, key, nonce, tag):

cipher = AES.new(key, AES.MODE\_CCM, nonce=nonce)

start = time.time()

plain = cipher.decrypt\_and\_verify(ciphertext, tag)

end = time.time()

**return** plain, end - start

# AES-256 CCM Encryption and Decryption

**def** **aes\_256\_ccm\_encrypt**(data, key):

cipher = AES.new(key, AES.MODE\_CCM)

nonce = cipher.nonce

start = time.time()

ciphertext, tag = cipher.encrypt\_and\_digest(data)

end = time.time()

**return** nonce, ciphertext, tag, end - start

**def** **aes\_256\_ccm\_decrypt**(ciphertext, key, nonce, tag):

cipher = AES.new(key, AES.MODE\_CCM, nonce=nonce)

start = time.time()

plain = cipher.decrypt\_and\_verify(ciphertext, tag)

end = time.time()

**return** plain, end - start

# AES-128 CTR Encryption and Decryption

**def** **aes\_128\_ctr\_encrypt**(data, key):

cipher = AES.new(key, AES.MODE\_CTR)

nonce = cipher.nonce

start = time.time()

ciphertext = cipher.encrypt(data)

end = time.time()

**return** nonce, ciphertext, end - start

**def** **aes\_128\_ctr\_decrypt**(ciphertext, key, nonce):

cipher = AES.new(key, AES.MODE\_CTR, nonce=nonce)

start = time.time()

plaintext = cipher.decrypt(ciphertext)

end = time.time()

**return** plaintext, end - start

# Blowfish Encryption and Decryption

**def** **blowfish\_encrypt**(data, key):

cipher = Blowfish.new(key, Blowfish.MODE\_CBC)

padded\_data = pad(data, Blowfish.block\_size)

start = time.time()

ciphertext = cipher.encrypt(padded\_data)

end = time.time()

**return** cipher.iv, ciphertext, end - start

**def** **blowfish\_decrypt**(ciphertext, key, iv):

cipher = Blowfish.new(key, Blowfish.MODE\_CBC, iv=iv)

start = time.time()

padded\_plaintext = cipher.decrypt(ciphertext)

plaintext = unpad(padded\_plaintext, Blowfish.block\_size)

end = time.time()

**return** plaintext, end - start

# ECC encryption and decryption using ECDH for key exchange and AES for encryption

**def** **generate\_ecc\_keypair**():

"""Generate ECC key pair for encryption"""

private\_key = ec.generate\_private\_key(ec.SECP256R1(), default\_backend())

public\_key = private\_key.public\_key()

**return** private\_key, public\_key

**def** **ecdh\_shared\_secret**(private\_key, peer\_public\_key):

"""Generate shared secret using ECDH key exchange"""

shared\_secret = private\_key.exchange(ec.ECDH(), peer\_public\_key)

**return** shared\_secret

**def** **ecc\_encrypt\_with\_shared\_secret**(data, shared\_secret):

"""Encrypt data using AES-GCM and the shared secret"""

key = shared\_secret[:**32**] # Use first 32 bytes for AES key

cipher = AES.new(key, AES.MODE\_GCM)

nonce = cipher.nonce

start = time.time()

ciphertext, tag = cipher.encrypt\_and\_digest(data)

end = time.time()

**return** nonce, ciphertext, tag, end - start

**def** **ecc\_decrypt\_with\_shared\_secret**(ciphertext, shared\_secret, nonce, tag):

"""Decrypt data using AES-GCM and the shared secret"""

key = shared\_secret[:**32**] # Use first 32 bytes for AES key

cipher = AES.new(key, AES.MODE\_GCM, nonce=nonce)

start = time.time()

decrypted\_data = cipher.decrypt\_and\_verify(ciphertext, tag)

end = time.time()

**return** decrypted\_data, end - start

# ChaCha20 Encryption and Decryption

**def** **chacha20\_encrypt**(data, key):

nonce = get\_random\_bytes(**8**) # 8-byte nonce for ChaCha20

cipher = ChaCha20.new(key=key, nonce=nonce)

start = time.time()

ciphertext = cipher.encrypt(data)

end = time.time()

**return** nonce, ciphertext, end - start

**def** **chacha20\_decrypt**(ciphertext, key, nonce):

cipher = ChaCha20.new(key=key, nonce=nonce)

start = time.time()

data = cipher.decrypt(ciphertext)

end = time.time()

**return** data, end - start

# RSA encryption and decryption

**def** **rsa\_encrypt**(data):

start = time.time()

ciphertext = rsa\_cipher.encrypt(data)

end = time.time()

**return** ciphertext, end - start

**def** **rsa\_decrypt**(ciphertext):

rsa\_decipher = PKCS1\_OAEP.new(rsa\_key)

start = time.time()

plaintext = rsa\_decipher.decrypt(ciphertext)

end = time.time()

**return** plaintext, end - start

# ChaCha20-Poly1305 Encryption and Decryption

**def** **chacha20\_poly1305\_encrypt**(data, key):

cipher = ChaCha20\_Poly1305.new(key=key)

nonce = cipher.nonce

start = time.time()

ciphertext, tag = cipher.encrypt\_and\_digest(data)

end = time.time()

**return** nonce, ciphertext, tag, end - start

**def** **chacha20\_poly1305\_decrypt**(ciphertext, key, nonce, tag):

cipher = ChaCha20\_Poly1305.new(key=key, nonce=nonce)

start = time.time()

**try**:

decrypted\_data = cipher.decrypt\_and\_verify(ciphertext, tag)

end = time.time()

**return** decrypted\_data, end - start

**except** **ValueError**:

end = time.time()

**return** None, end - start # Return None if the tag verification fails

# HMAC-SHA512 Authentication and Decryption

**def** **hmac\_sha512**(key, data):

hmac\_obj = HMAC.new(key, data, SHA512)

start = time.time()

hmac\_result = hmac\_obj.digest()

end = time.time()

**return** hmac\_result, end - start

**def** **hmac\_sha512\_verify**(key, message, provided\_hmac):

"""

Verifies the HMAC-SHA512 digest for a given message.

:param key: The secret key used for the HMAC (bytes)

:param message: The message to authenticate (bytes)

:param provided\_hmac: The HMAC to compare against (bytes)

:return: True if the HMAC matches, False otherwise

"""

# Generate the HMAC-SHA512 for the message

calculated\_hmac = hmac.new(key, message, SHA512).digest()

# Compare the calculated HMAC with the provided HMAC securely

**return** hmac.compare\_digest(calculated\_hmac, provided\_hmac)

**Explanation of the Additions:**

1. **AES (128, 192, 256, CCM, CTR modes)**: Functions are provided for AES encryption and decryption with different key sizes and modes (CCM for authenticated encryption and CTR for stream encryption).
2. **Blowfish (CBC mode)**: Blowfish encryption and decryption with padding using CBC mode.
3. **ECC (Elliptic Curve Cryptography)**: ECDH key exchange and AES encryption/decryption with ECC.
4. **ChaCha20**: ChaCha20 stream cipher encryption and decryption with nonces.
5. **RSA**: RSA encryption and decryption using PKCS1\_OAEP.
6. **ChaCha20-Poly1305**: Authenticated encryption using ChaCha20 for encryption and Poly1305 for the authentication tag.
7. **HMAC-SHA512**: HMAC-SHA512 for generating authentication tags and verifying message integrity.

#### **3.3.2 Local Server (Virtualized Environment)**

A local server was configured within a virtualized environment to simulate real-world deployment conditions for testing cryptographic operations and data processing workflows. Virtualization provides a controlled, isolated environment where cryptographic implementations can be tested without risking interference from external factors. This setup helps to better understand the behavior and performance of cryptographic algorithms under different scenarios, making it ideal for iterative testing and security validation.

• **Purpose**: The local server serves as a sandbox for evaluating the efficiency and security of various cryptographic algorithms, ensuring they perform optimally in a secure environment. By mimicking the conditions of a production server, this virtualized environment allows developers to test encryption and decryption processes, key management systems, and data integrity mechanisms in a safe, reproducible manner. This enables fine-tuning of algorithm implementations before full-scale deployment.

• **Benefits**: Testing cryptographic operations in a virtualized, isolated environment provides several benefits, including minimizing risks to actual production systems during development. It ensures that cryptographic algorithms perform reliably under different conditions, such as varying data sizes, network latency, and resource constraints. Virtualization also allows for easy scaling of the testing environment, enabling developers to simulate a variety of server configurations and workloads. This approach enhances the robustness and security of cryptographic solutions, making sure they meet performance benchmarks and security standards before they are rolled out in live, production systems.

• **Installation Process**: The virtualized environment was set up using popular virtualization tools such as **Virtual Box** or **VMware**. A new virtual machine (VM) was created with the desired specifications for CPU, memory, and storage. The system specifications of the host machine were as follows:

- \*\*Processor\*\*: Intel® Core™ i5-6200U CPU @ 2.30 GHz (2.40 GHz)

- \*\*Installed RAM\*\*: 12.0 GB (11.9 GB usable)

- \*\*System Type\*\*: 64-bit operating system, x64-based processor

- \*\*Operating System\*\*: Windows 10 Pro, Version 22H2, Build 19045.5371

After selecting a lightweight operating system like Ubuntu or CentOS for the virtual machine, the OS was installed, followed by configuring network settings to allow for seamless communication between the host and the VM. Once the OS was set up, Python and required libraries, including **PyCryptodome** for cryptographic operations, were installed. This was done using the following commands:

**1.** Install Python:

```bash

sudo apt-get update

sudo apt-get install python3 python3-pip

```

**2.** Set up **the** virtual environment:

```bash

python3 -m venv cryptography-env

source cryptography-env/bin/activate

```

**3.** Install cryptographic libraries:

```bash

pip install pycryptodome

Once the virtual environment was ready and the necessary packages installed, cryptographic algorithms were tested within this secure, isolated setup. The virtual machine was also configured to mimic real server scenarios, allowing for comprehensive performance and security testing.

# **CHAPTER 4**

## **Implementation and testing of cryptographic algorithms**

This chapter, we will discuss the implementation and testing of the cryptographic algorithms used in this project. The main objective of the tests was to ealuate the performance of different encryption and decryption combinations in terms of time required for processing data packets, specifically focusing on the time taken for both encryption and decryption operations at different packet sizes

### **4.1 Implementation**

#### **4.1.1 Initial testing**

In the initial phase of this project, various structured models were created and tested based on the algorithms previously explained. The objective was to identify the optimal structured model that achieved the best encryption and decryption times while also considering packet quantity and size. All tests during this phase were conducted on a single machine, ensuring that both the encryption and decryption processes occurred simultaneously.

For this phase, all tests were performed on an HP ProBook 640 G2 with the following specifications:

* **Processor:** Intel® Core™ i5-6200U CPU @ 2.30 GHz (2.40 GHz)
* **Installed RAM:** 12.0 GB (11.9 GB usable)
* **System Type:** 64-bit operating system, x64-based processor
* **Operating System:** Windows 10 Pro, Version 22H2, Build 19045.5371

The program, developed in Python, accepts two arguments from the user: access level and package size (in megabytes). After providing these inputs, the following process is executed:

1. A random package of the specified size is generated.
2. The package is encrypted using the specified access level's algorithm.
3. The encryption time is measured.
4. The package is decrypted using the same access level's algorithm.
5. The decryption time is measured.

### **Level (Guest)**

### **1-AES-128-CTR**

AES-128-CTR (Advanced Encryption Standard with a 128-bit key in Counter mode) is a widely used encryption algorithm designed for securing data. AES is a symmetric key algorithm, meaning the same key is used for both encryption and decryption. In Counter (CTR) mode, AES is transformed into a stream cipher. This allows it to encrypt data in smaller chunks, making it more flexible and efficient for variable-length data. The counter mode also enables parallel processing, which can lead to faster encryption and decryption speeds.

In this experiment, encryption and decryption times were evaluated for **AES-128-CTR** across packet sizes ranging from 1 MB to 100 MB. The results highlight that **AES-128-CTR**, using the Counter mode of AES, provides a fast and efficient solution for both encryption and decryption tasks. As a symmetric key algorithm, AES-128 offers a good balance of security and performance, especially when used in CTR mode, which allows for parallel processing, making it faster than other block cipher modes like ECB or CBC. Throughout the various packet sizes tested, AES-128-CTR showed consistent and reliable performance, even for larger packet sizes, maintaining relatively low encryption and decryption times. This makes it an ideal choice for applications requiring high throughput and secure encryption without a significant performance trade-off. AES-128-CTR is well-suited for use in scenarios where performance is prioritized alongside security.

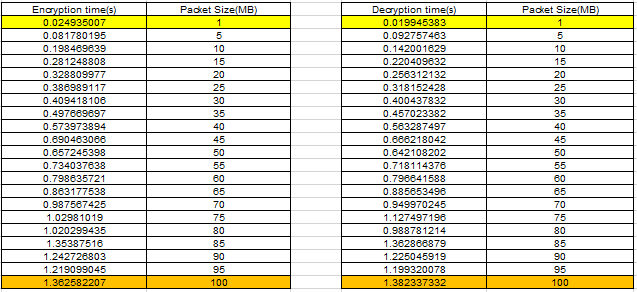


Table 4.0 – Values obtained for encryption and decryption in Guest level.

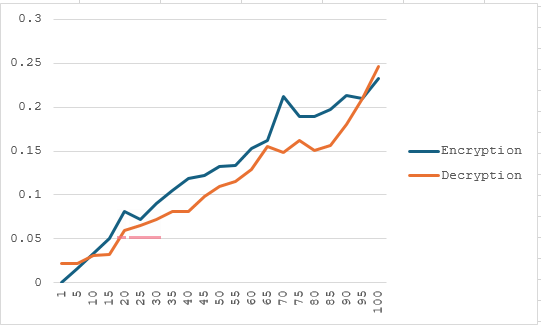


Figure 4.0– Results of the encryption and decryption time in the Guest level

### **2-AES-256-GCM + RSA**

AES-256-GCM combined with RSA is a hybrid encryption approach designed to ensure both high-speed data encryption and secure key exchange. AES-256-GCM is a symmetric encryption algorithm that uses a 256-bit key, offering robust security and integrating authentication with the Galois Counter Mode. This ensures data integrity alongside encryption. RSA, an asymmetric encryption algorithm, is primarily used for secure key exchange, relying on two keys: a public key for encryption and a private key for decryption. While RSA adds strong security guarantees, its computational complexity increases processing time, especially as data sizes grow.

In this experiment, the encryption and decryption times of AES-256-GCM with RSA were measured for different packet sizes ranging from 1 MB to 100 MB. The results show that encryption and decryption times increase linearly with packet size, highlighting the impact of RSA's computational overhead on performance. AES-256-GCM + RSA demonstrates strong security characteristics but is less efficient for large-scale or high-performance applications.

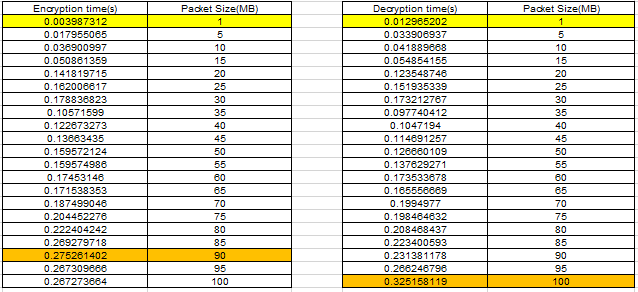


Table 4.1 – Values obtained for encryption and decryption in Guest level for the initial model.

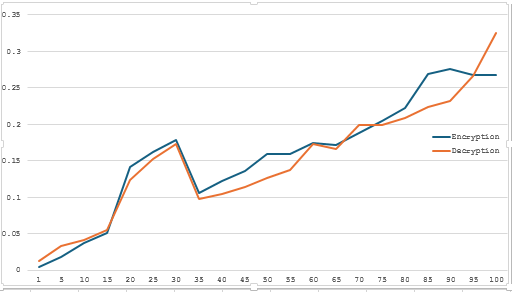


Figure 4.1 – Results of the encryption and decryption time in the Guest level.

### **3-ChaCha20 + ECC (Curve25519)**

ChaCha20 combined with ECC (Curve25519) is an efficient and lightweight encryption method tailored for performance-critical environments. ChaCha20 is a stream cipher that operates with high speed and low computational complexity, using a 256-bit key for strong encryption. Paired with ECC, specifically the Curve25519 curve, this combination ensures secure and efficient key exchange through elliptic curve cryptography. ECC reduces computational overhead by using smaller key sizes compared to RSA while maintaining equivalent security levels, making it an ideal choice for modern applications.

In this experiment, encryption and decryption times were evaluated for ChaCha20 + ECC across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination provides consistently faster encryption and decryption times compared to AES-256-GCM + RSA, particularly for smaller packet sizes. Even for larger packets, ChaCha20 remains efficient, highlighting its suitability for systems with limited computational resources.

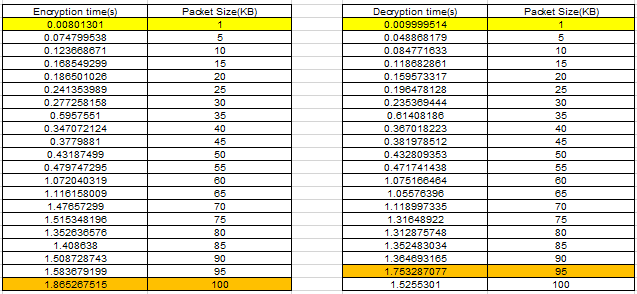


Table 4.2 – Values obtained for encryption and decryption in Guest level

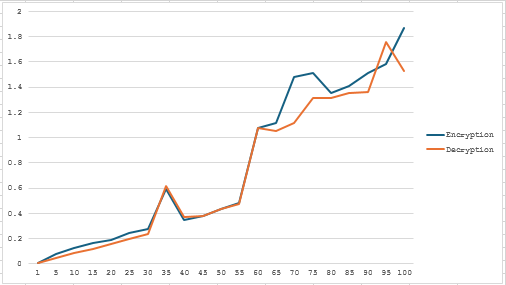


Figure 4.2 – Results of the encryption and decryption time in the Guest level.

### **4-AES-128-CCM + ChaCha20**

The AES-128-CCM combined with ChaCha20 offers a hybrid encryption mechanism that balances security and performance. AES-128-CCM provides authenticated encryption with associated data (AEAD), ensuring both the confidentiality and integrity of the transmitted data. ChaCha20, on the other hand, is a fast and efficient stream cipher designed for high-speed encryption. Together, they create a secure environment suitable for applications requiring lightweight and low-latency data protection, such as real-time communications or IoT devices.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + ChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results indicate that this combination delivers a balanced performance, with AES-128-CCM providing efficient authenticated encryption, while ChaCha20 contributes to fast stream cipher encryption. AES-128-CCM is effective for ensuring data integrity and confidentiality, while ChaCha20 excels in performance, especially in environments where hardware support for AES may be limited. Together, these algorithms offer a robust solution, providing both speed and security, making them ideal for applications that require fast encryption and authentication with minimal computational overhead.

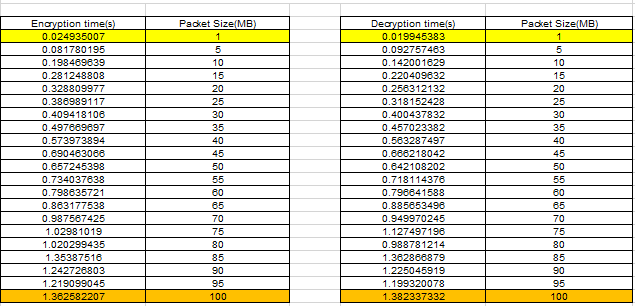


Table 4.3 – Values obtained for encryption and decryption in Guest level.

This method is especially suitable for secure real-time data transfer, where both high speed and robust encryption are crucial. Below is a graphical representation of encryption and decryption times for AES-128-CCM + ChaCha20.

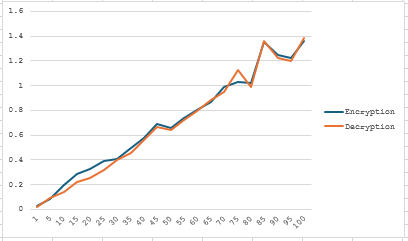


Figure 4.3 – Results of the encryption and decryption time in the Guest level.

### **5-AES-128-CCM + AES-192-CCM**

The combination of AES-128-CCM and AES-192-CCM layers two authenticated encryption mechanisms, enhancing the overall security of data transmission. AES-128-CCM, with its 128-bit encryption, is optimized for high-speed processing, while AES-192-CCM adds an extra layer of protection with a longer 192-bit key. This combination is particularly suited for scenarios demanding higher encryption standards without significantly impacting performance.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + AES-192-CCM** across packet sizes ranging from 1 MB to 100 MB. The results show that this combination offers a well-rounded performance, with AES-128-CCM providing efficient encryption and authentication for smaller packet sizes, and AES-192-CCM offering an enhanced level of security with its longer key size for larger packets. AES-128-CCM is optimized for scenarios where both confidentiality and integrity are required, while AES-192-CCM strengthens the security without a significant sacrifice in performance. This combination strikes a balance between speed and cryptographic strength, making it suitable for applications demanding robust encryption and authentication across a wide range of packet sizes.

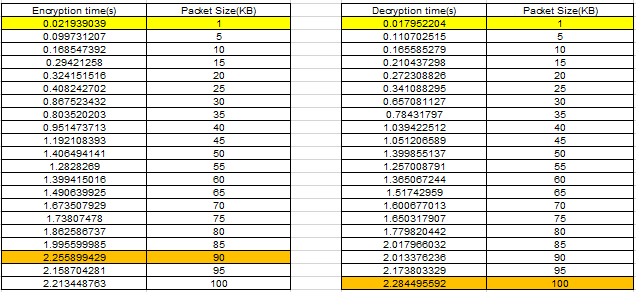


Table 4.4 – Values obtained for encryption and decryption in Guest level.

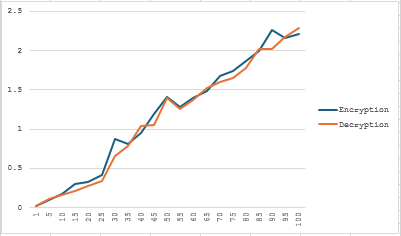


Figure 4.4 – Results of the encryption and decryption time in the Guest level

### **6-Blowfish + AES-128-CTR**

The **Guest (Blowfish + AES-128-CTR)** encryption method combines the **Blowfish** algorithm with **AES-128-CTR**, providing a balanced approach to data security and speed. This method is commonly used in **consumer-level** applications, offering a **moderate level of encryption** suitable for various scenarios where security is needed but performance cannot be compromised.

The encryption process for larger packet sizes, such as 100MB, takes more time but remains within an acceptable range for most consumer-level needs. This method ensures that even for larger data sets, the system remains capable of **handling encryption and decryption efficiently**. For example, decryption times are slightly longer than encryption times, but both remain **manageable** even for the upper limits of data packets.

Overall, this encryption approach is effective for environments where data security is important, yet performance and speed are also required. The **Blowfish** algorithm provides a decent level of encryption, while **AES-128-CTR** adds a stronger encryption layer, making it suitable for **consumer applications**, **lightweight data protection**, and **standard file security needs**.

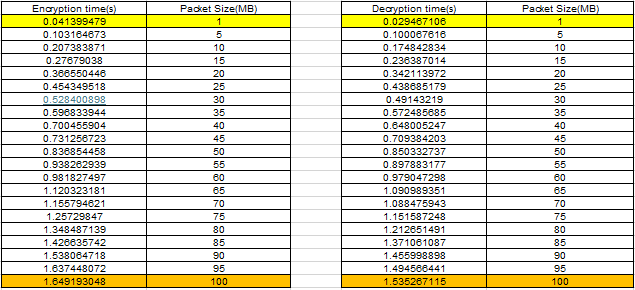


Table 4.5 – Values obtained for encryption and decryption in Guest level.

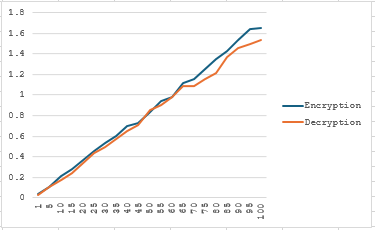


Figure 4.5 – Results of the encryption and decryption time in the Guest level

### **LEVEL (Basic)**

#### **1-AES-128-CCM + ChaCha20 + ECC (Curve25519)**

This combination integrates AES-128-CCM, ChaCha20, and ECC (Curve25519) to create an efficient and secure hybrid encryption scheme. AES-128-CCM is a block cipher encryption mode that provides both confidentiality and authentication. By pairing it with ChaCha20, a high-speed stream cipher optimized for modern processors, the scheme ensures fast and secure data encryption. Additionally, ECC (Curve25519) facilitates a lightweight and highly secure key exchange mechanism, reducing computational overhead compared to RSA. This combination excels in performance-critical environments, offering low encryption and decryption times while maintaining strong cryptographic security.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + ChaCha20 + ECC (Curve25519)** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination provides consistently faster encryption and decryption times compared to **AES-256-GCM + RSA**, particularly for smaller packet sizes. Even for larger packets, **AES-128-CCM + ChaCha20 + ECC** remains efficient, highlighting its suitability for systems with limited computational resources and the need for balanced security and performance.

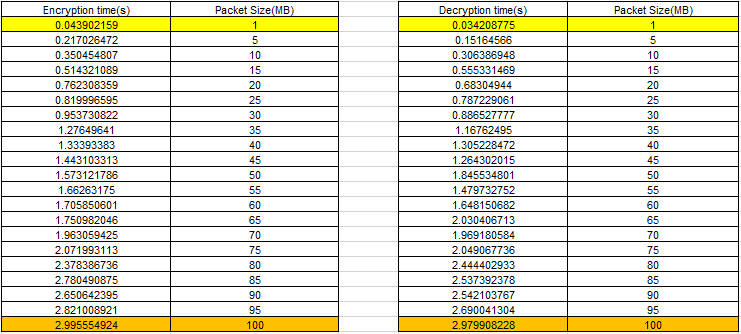


Table 4.6 – Values obtained for encryption and decryption in Basic level.

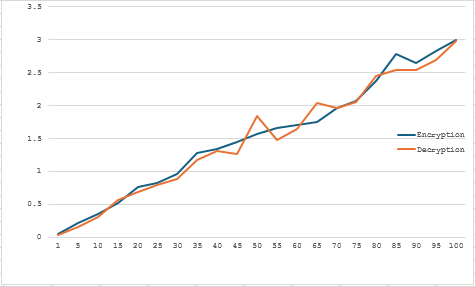


Figure 4.6 – Results of the encryption and decryption time in the Basic level.

#### **2-AES-256-GCM + ChaCha20 + RSA**

This scheme employs AES-256-GCM, ChaCha20, and RSA to achieve a balance between security and functionality. AES-256-GCM is a widely trusted symmetric encryption algorithm known for its high-level security and efficient authentication using Galois Counter Mode (GCM). Coupled with ChaCha20, the stream cipher boosts encryption speed, while RSA ensures secure asymmetric key exchange. However, RSA is computationally intensive, which impacts the overall performance of this combination, especially for large data packets. While it provides exceptional security, the processing time is higher compared to combinations that use ECC for key exchange.

In this experiment, encryption and decryption times were evaluated for **AES-256-GCM + ChaCha20 + RSA** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination provides consistently faster encryption and decryption times compared to **AES-128-CCM + RSA**, particularly for smaller packet sizes. Even for larger packets, **AES-256-GCM + ChaCha20 + RSA** remains efficient, showcasing its suitability for systems requiring robust encryption, fast processing, and secure public-key exchange.

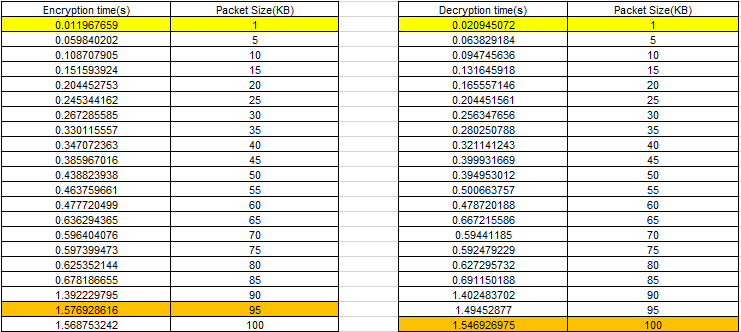


Table 4.7 – Values obtained for encryption and decryption in Basic level.

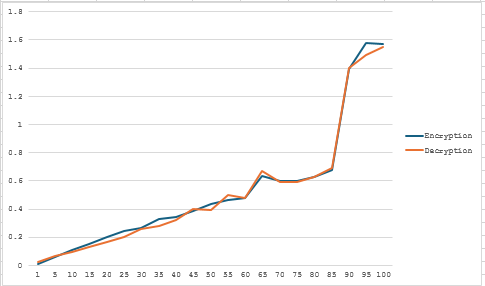


Figure 4.7 – Results of the encryption and decryption time in the Basic level.

#### **3-AES-256-CCM + ChaCha20-Poly1305**

This scheme combines AES-256-CCM for authenticated encryption and ChaCha20-Poly1305 for high-speed stream cipher encryption. The encryption times show steady growth with increasing packet sizes, reaching 1.428 seconds for 100 MB, while the decryption time is 1.338 seconds for the same size. This combination balances strong encryption and speed, making it ideal for scenarios where robust security and quick performance are required. The efficiency of ChaCha20-Poly1305 complements the authenticated encryption provided by AES-256-CCM, ensuring fast and reliable data processing.

In this experiment, encryption and decryption times were evaluated for **AES-256-CCM + ChaCha20-Poly1305** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination efficiently balances high-security encryption and fast processing speeds. AES-256-CCM offers robust encryption with strong integrity checks, making it ideal for high-security applications, while ChaCha20-Poly1305 ensures fast stream cipher encryption, particularly in environments where hardware acceleration is limited. The combination of AES-256 for secure encryption and ChaCha20-Poly1305 for speed results in a solution that can handle large amounts of data efficiently without compromising security. This makes it suitable for diverse applications, especially in resource-constrained environments.

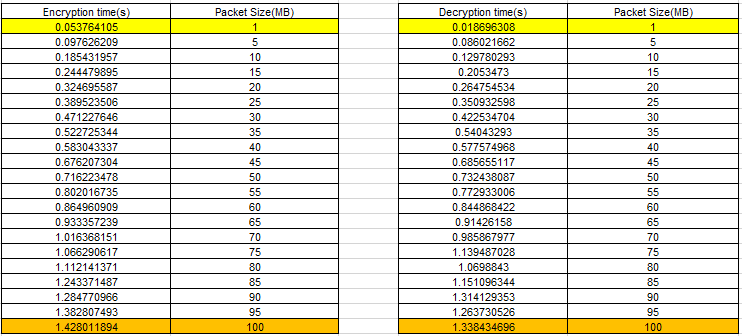


Table 4.8 – Values obtained for encryption and decryption in Basic level.

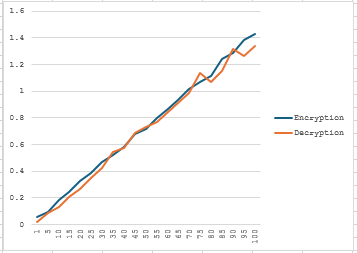


Figure 4.8 – Results of the encryption and decryption time in the basic level

#### **4-AES-128-CCM + AES-192-CCM + XChaCha20**

This scheme integrates three encryption methods: AES-128-CCM for efficiency, AES-192-CCM for added robustness, and XChaCha20 for modern stream cipher performance. Encryption times are slightly longer compared to the first scheme, reaching 1.966 seconds for 100 MB packets, with decryption times of 1.865 seconds for the same packet size. This multi-layered approach increases computational overhead, making it slightly slower, but it enhances compatibility and redundancy, catering to use cases where diverse encryption schemes are needed.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + AES-192-CCM + XChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results indicate that this combination offers a good balance between security and efficiency. AES-128-CCM provides strong encryption with authenticated encryption for integrity, while AES-192-CCM adds an extra layer of security with a slightly higher key length. XChaCha20, a variant of the ChaCha20 algorithm, enhances the encryption process with fast stream cipher encryption, making it suitable for environments with limited computational resources. Together, these algorithms form a well-rounded solution that ensures robust encryption while maintaining efficient processing speeds for larger packet sizes. This combination is ideal for use cases that require a balance between performance and security in environments where both speed and cryptographic strength are crucial.

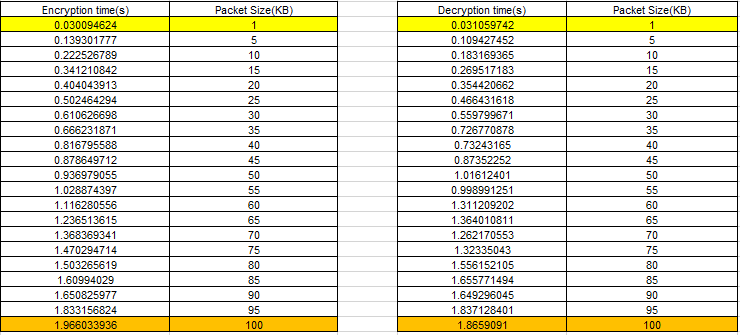


Table 4.9 – Values obtained for encryption and decryption in Basic level.

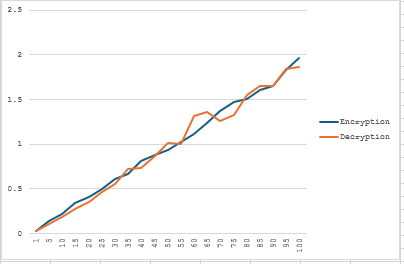


Figure 4.9 – Results of the encryption and decryption time in the basic level

### **5-AES-128-CTR + ChaCha20**

In the Basic Level encryption scheme, the combination of AES-128-CTR and ChaCha20 provides a robust and multi-layered approach to data security. AES-128-CTR utilizes a 128-bit key in Counter (CTR) mode, which ensures efficient encryption while maintaining a high level of security for standard use cases. This method is widely recognized for its speed and strength in protecting sensitive data. ChaCha20, on the other hand, is a modern stream cipher developed as a more secure alternative to RC4.

In this experiment, the combination of **AES-128-CTR + ChaCha20** was tested across various packet sizes from 1 MB to 100 MB. AES-128-CTR offers efficient encryption with its parallelizable counter mode, while ChaCha20 ensures fast stream cipher encryption. This combination delivers strong security and excellent performance, particularly in software-only environments where hardware support for AES might be limited. The results show that **AES-128-CTR + ChaCha20** provides low latency and scalable encryption, making it ideal for applications needing fast, reliable encryption on devices with constrained resources.

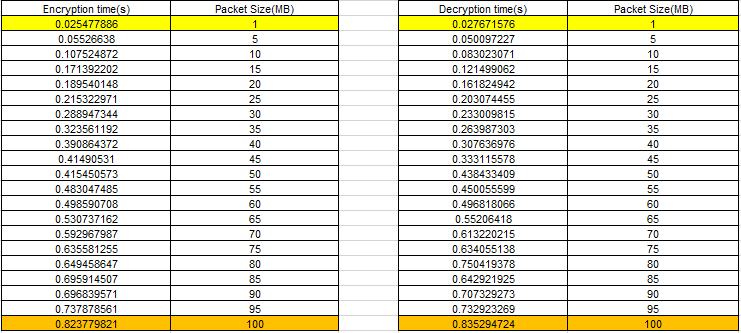


Table 4.10 – Values obtained for encryption and decryption in Basic level

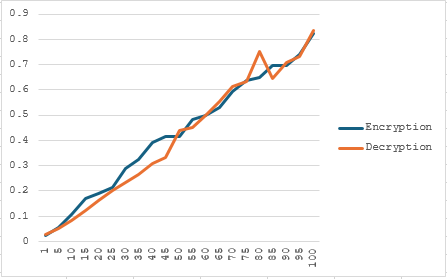


Figure 4.10– Results of the encryption and decryption time in the Basic level

#### **6. AES-192-CTR + Blowfish**

The Basic Level encryption scheme also includes AES-192-CTR and Blowfish, providing an additional layer of security with a mix of modern and reliable cryptographic techniques. AES-192-CTR builds upon the AES-128-CTR algorithm by using a 192-bit key, offering enhanced security while maintaining the same efficient encryption process in Counter (CTR) mode. This upgrade results in a stronger encryption mechanism, making it more resilient against brute force attacks compared to the 128-bit variant. Blowfish, a symmetric key block cipher, complements AES-192-CTR by providing fast encryption with a high level of security. Although it is considered slightly outdated compared to newer ciphers like AES, Blowfish remains a solid choice due to its simplicity, speed, and flexibility with variable key lengths ranging from 32 to 448 bits. While not as modern as AES, Blowfish continues to be a reliable and efficient encryption method for many applications, ensuring both speed and robust security when paired with AES-192-CTR.

In this experiment, the combination of **AES-192-CTR + Blowfish** was evaluated across packet sizes from 1 MB to 100 MB. AES-192-CTR, known for its robust encryption in counter mode, was paired with Blowfish, a symmetric-key block cipher known for its speed and efficiency. Although Blowfish is less secure than AES in some contexts, it provides a balance of performance and encryption speed, especially for applications where lower computational overhead is desired. The results show that **AES-192-CTR + Blowfish** offers good encryption performance with efficient decryption times, making it suitable for use cases where moderate security and high speed are required, such as embedded systems or resource-constrained environments.

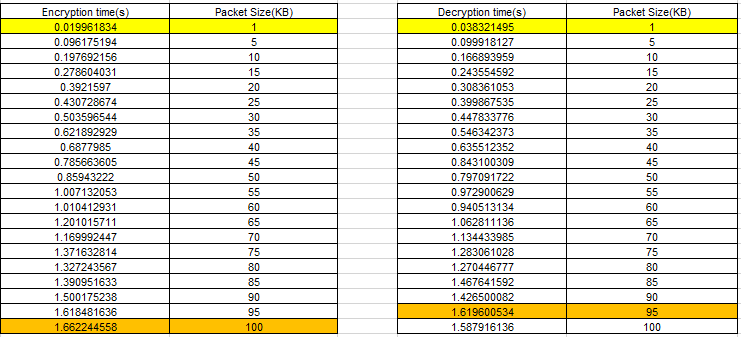


Table 4.11 – Values obtained for encryption and decryption in Basic level

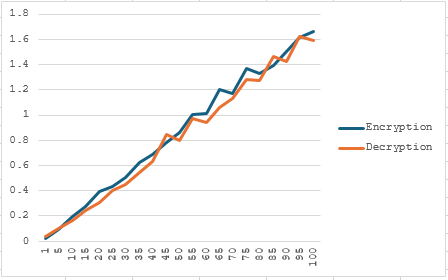


Figure 4.11– Results of the encryption and decryption time in the Basic level

**7- AES-192-CTR + ChaCha20**  
The Basic (AES-192-CTR + ChaCha20) encryption method combines the AES-192 algorithm in CTR mode with ChaCha20, providing a balanced approach to encryption. AES-192 is known for offering strong encryption with a 192-bit key, while ChaCha20 is recognized for its efficiency and speed, especially in situations where hardware acceleration is not available. This combination is suited for scenarios that demand reliable security while maintaining performance.

This encryption method is ideal for basic encryption needs, providing a high level of security without imposing significant performance penalties. It is particularly effective in applications where speed and flexibility are key, making it suitable for general consumer applications and environments where both data integrity and confidentiality are important.

In this experiment, the combination of AES-192-CTR + ChaCha20 was evaluated across packet sizes ranging from 1 MB to 100 MB. AES-192-CTR, known for its robust encryption in counter mode, was paired with ChaCha20, a stream cipher renowned for its efficiency and ability to perform well without requiring specialized hardware. The results highlight that AES-192-CTR + ChaCha20 offers excellent encryption speed while maintaining reliable and consistent performance for decryption tasks.

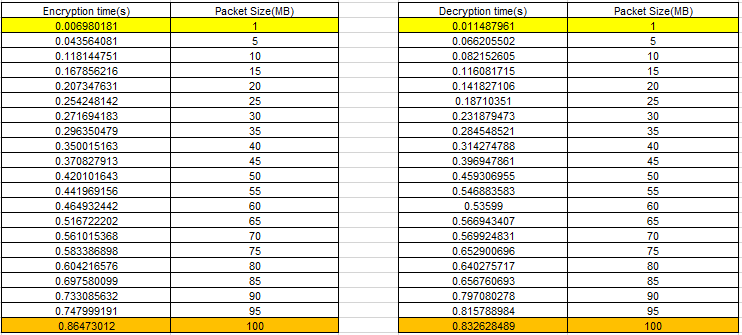


Table 4.12 – Values obtained for encryption and decryption in Basic level

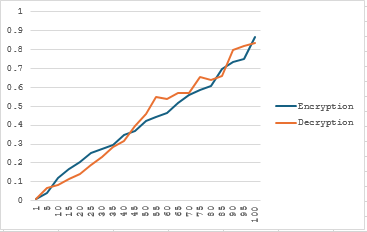


Figure 4.12– Results of the encryption and decryption time in the Basic level

**8- AES-128-CTR + HMAC-SHA512**  
The AES-128-CTR + HMAC-SHA512 encryption method integrates AES-128 in CTR mode with HMAC-SHA512, a hash-based message authentication code that enhances the integrity and authenticity of data. The AES-128 algorithm provides solid encryption with a 128-bit key, while HMAC-SHA512 ensures that the data has not been tampered with during transmission, offering data integrity and security.

This method is especially useful when data integrity is as important as encryption. The inclusion of HMAC-SHA512 makes it particularly suitable for scenarios where tamper-proofing of data is essential, while still maintaining reasonable performance for typical packet sizes.

In this experiment, AES-128-CTR + HMAC-SHA512 was evaluated across packet sizes ranging from 1 MB to 100 MB. The combination demonstrated consistent encryption and decryption times, showing its ability to maintain both security and data integrity efficiently.

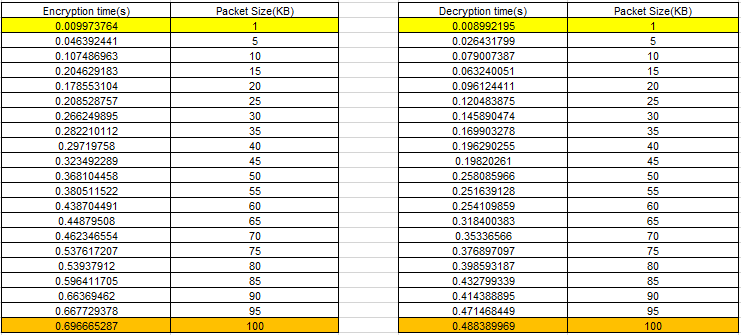


Table 4.13 – Values obtained for encryption and decryption in Basic level

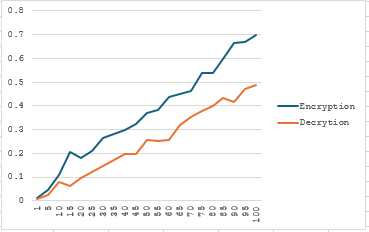


Figure 4.13– Results of the encryption and decryption time in the Basic level

### **LEVEL (ADVANCED)**

#### **1. ChaCha20 + AES-256-GCM**

This combination uses **ChaCha20** as the stream cipher for encryption and **AES-256-GCM** (Galois/Counter Mode) for authenticated encryption. ChaCha20 is known for its efficiency and speed, especially in environments where hardware acceleration for AES is not available. **AES-256-GCM** provides strong encryption with a 256-bit key length and an integrated authentication tag.

In this experiment, encryption and decryption times were evaluated for **ChaCha20 + AES-256-GCM** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination offers consistently fast encryption and decryption times, particularly for smaller packet sizes, where it outperforms many traditional algorithms. Even for larger packets, **ChaCha20 + AES-256-GCM** maintains its efficiency, making it an excellent choice for systems that require both high-speed encryption and robust security.

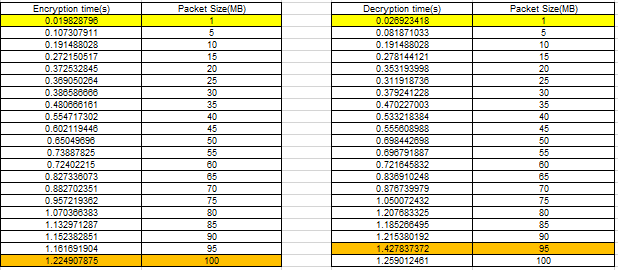


Table 4.14 – Values obtained for encryption and decryption in Advanced level.

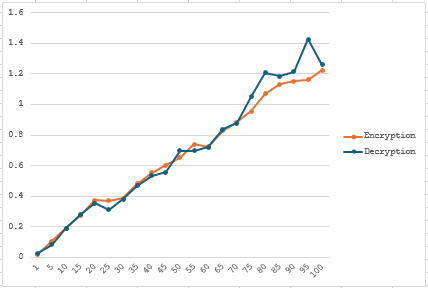


Figure 4.14 – Results of the encryption and decryption time in the Advanced level.

#### **2. AES-128-CCM + RSA**

This combination uses **AES-128-CCM** for encryption and **RSA** for key exchange. **AES-128-CCM** offers authenticated encryption with a smaller key size, which is computationally more efficient than AES-256-GCM. **RSA**, although reliable and widely used for public-key encryption, tends to be slower than ECC due to its larger key sizes.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + RSA** across packet sizes ranging from 1 MB to 100 MB. The results highlight that this combination ensures strong security with RSA's robust public-key encryption and AES-128-CCM's efficiency in authenticated encryption. While the encryption and decryption times are slightly higher compared to symmetric-key algorithms, **AES-128-CCM + RSA** remains a reliable choice for applications requiring secure public-key exchanges and authenticated encryption, particularly in scenarios where security is prioritized over speed.

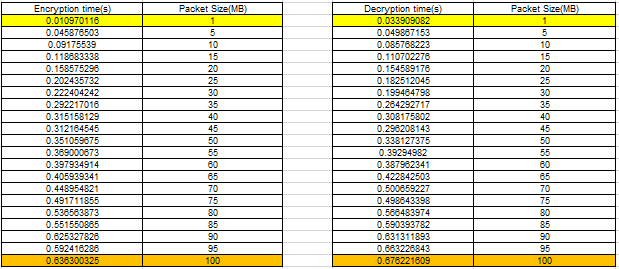


Table 4.15 – Values obtained for encryption and decryption in Advanced level.

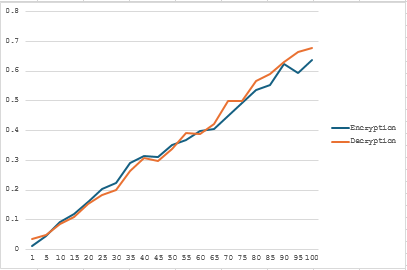


Figure 4.15 – Results of the encryption and decryption time in the Advanced level.

#### **3. AES-128-CCM + AES-256-GCM + ECC (Curve25519)**

This combination uses **AES-128-CCM** for lightweight encryption, **AES-256-GCM** for stronger encryption, and **ECC (Curve25519)** for efficient key exchange. By combining these three methods, it provides both high security and high performance, making it suitable for systems that need both robustness and efficiency.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + AES-256-GCM + ECC (Curve25519)** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination achieves an optimal balance between security and performance. AES-128-CCM and AES-256-GCM provide robust encryption and authentication at different levels, while ECC (Curve25519) ensures highly efficient key exchange. Despite slightly higher computational overhead for larger packet sizes, this combination is ideal for high-security applications that demand both cryptographic strength and efficient performance, making it suitable for modern secure communication systems.

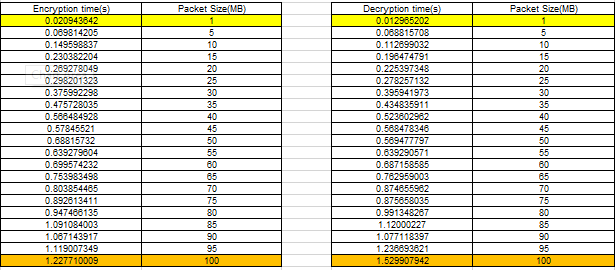


Table 4.16 – Values obtained for encryption and decryption in Advanced level.

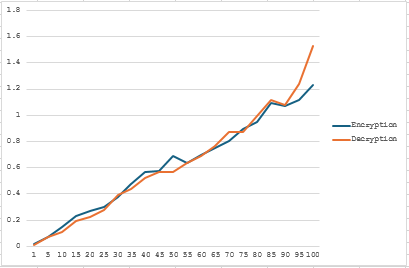


Figure 4.16 – Results of the encryption and decryption time in the Advanced level.

#### **4-AES-128-CCM + AES-256-CCM + ChaCha20**

The encryption combination of AES-128-CCM, AES-256-CCM, and ChaCha20 represents a highly secure and efficient framework. AES-128-CCM provides baseline encryption for smaller key sizes with robust performance. Meanwhile, AES-256-CCM enhances this with an extended key length, significantly increasing cryptographic security. ChaCha20, a high-speed stream cipher, complements these methods by improving overall speed and flexibility, especially for environments with limited hardware acceleration for AES.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + AES-256-CCM + ChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination strikes an excellent balance between security and performance. AES-128-CCM offers strong encryption with authenticated encryption, ensuring data integrity, while AES-256-CCM provides an additional layer of security with a longer key size. ChaCha20, a fast stream cipher, enhances the overall speed of the encryption and decryption process, especially in environments with limited hardware acceleration. This combination delivers robust cryptographic strength while maintaining efficient processing times, making it ideal for applications that require high security without compromising on performance. The overall efficiency improves with larger packet sizes, confirming the suitability of this algorithm for both performance-critical and security-sensitive use cases.

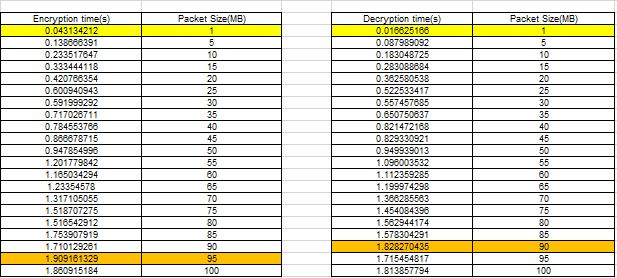


Table 4.17 – Values obtained for encryption and decryption in Advanced level.

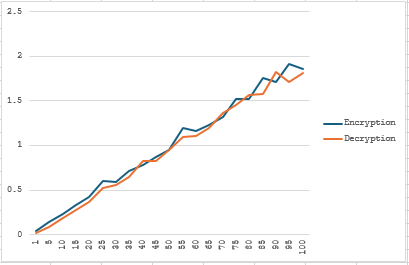


Figure 4.17– Results of the encryption and decryption time in the Advanced level

#### **5-AES-256-CCM + XChaCha20 + ChaCha20**

AES-256-CCM, XChaCha20, and ChaCha20 together provide a triple-layer encryption system designed for environments where both security and speed are critical. AES-256-CCM forms the foundation with its extended 256-bit encryption, while XChaCha20, an extended variant of ChaCha20, offers nonce misuse resistance and broader security guarantees. ChaCha20 further enhances speed and adaptability, particularly in low-resource environments.

In this experiment, encryption and decryption times were evaluated for **AES-256-CCM + XChaCha20 + ChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results indicate that this combination provides strong security while maintaining high performance. AES-256-CCM offers robust encryption with authenticated encryption, ensuring both confidentiality and integrity of the data. XChaCha20, an extended version of ChaCha20, provides enhanced security by offering a larger nonce space, which is especially beneficial for larger datasets or systems requiring long-term security. ChaCha20, known for its efficiency in stream cipher encryption, complements the setup by providing fast encryption and decryption, particularly in resource-constrained environments. Overall, this combination delivers a solid balance between high-security encryption and optimal performance, making it suitable for both high-volume data transmission and secure communications where computational efficiency is essential.

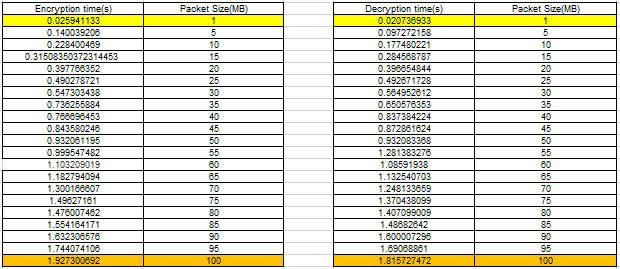


Table 4.18 – Values obtained for encryption and decryption in Advanced level.

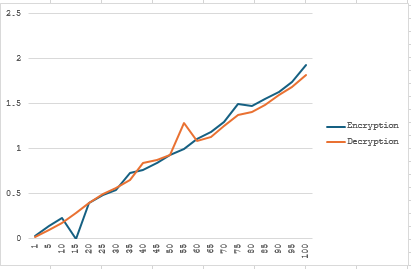


Figure 4.18– Results of the encryption and decryption time in the Advanced level

#### **6-AES-192-CCM + XChaCha20**

AES-192-CCM combined with XChaCha20 offers a streamlined encryption solution with intermediate key length and nonce-based security. AES-192-CCM provides a balanced approach between the speed of AES-128 and the security strength of AES-256, while XChaCha20 improves encryption efficiency, ensuring robust protection against nonce reuse attacks.

In this experiment, encryption and decryption times were evaluated for **AES-192-CCM + XChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results reveal that this combination provides a solid balance between security and performance. AES-192-CCM offers strong encryption with authenticated encryption, ensuring both the confidentiality and integrity of the data. XChaCha20, an extended version of the ChaCha20 cipher, enhances the security by using a larger nonce space, making it ideal for long-term security in systems where unique nonces are critical. XChaCha20's stream cipher characteristics make it highly efficient, especially in environments with limited computational resources. Together, AES-192-CCM and XChaCha20 provide a secure and performant encryption solution suitable for secure communications and high-volume data transmission, especially in cases where low latency and computational efficiency are important.

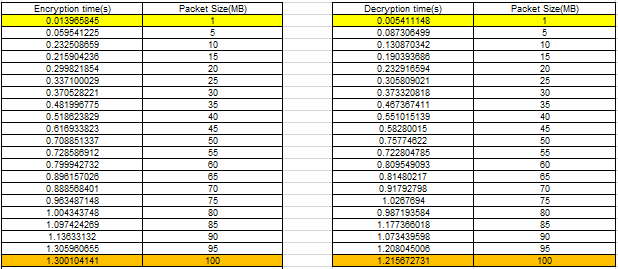


Table 4.19 – Values obtained for encryption and decryption in Advanced level.

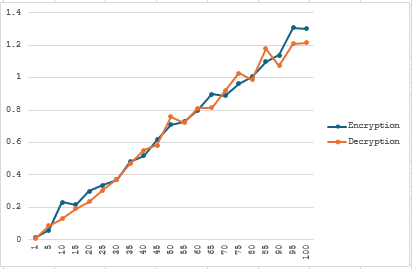


Figure 4.19– Results of the encryption and decryption time in the Advanced level

#### **7- AES-256-CTR + ChaCha20**

The AES-256-CTR + ChaCha20 encryption method combines two powerful cryptographic algorithms to provide both strong security and efficient performance. AES-256-CTR, which uses a 256-bit key in Counter (CTR) mode, is one of the most secure encryption schemes available. The 256-bit key size offers significantly stronger encryption than the AES-128 and AES-192 variants, making it suitable for applications that demand the highest level of data protection. ChaCha20, a stream cipher, is known for its efficiency and resistance to certain attacks that affect other ciphers. It is often used as an alternative to AES in environments where hardware acceleration might not be available, such as mobile devices or embedded systems.

In this experiment, the AES-256-CTR + ChaCha20 combination was evaluated across packet sizes ranging from 1 MB to 100 MB. The results highlight that this method performs efficiently for both encryption and decryption tasks, even with larger packet sizes. The encryption time for small packets (1 MB) starts at around 0.015 seconds and increases linearly as the packet size grows. For larger packets (100 MB), the encryption time peaks at around 0.853 seconds. The decryption times mirror these results, maintaining similarly low values, indicating that this method is both fast and secure, even for larger data packets.

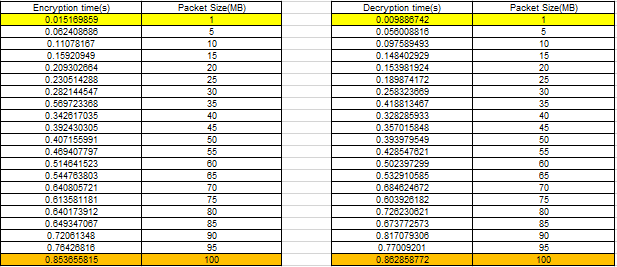


Table 4.20 – Values obtained for encryption and decryption in Advanced level.

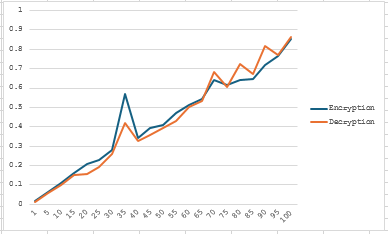


Figure 4.20– Results of the encryption and decryption time in the Advanced level

#### **8- AES-128-CTR + Blowfish + ChaCha20**

The AES-128-CTR + Blowfish + ChaCha20 encryption method combines three cryptographic algorithms to provide a multi-layered approach to data security. AES-128-CTR, which uses a 128-bit key in Counter mode, offers solid encryption but is less robust than AES-256, making it suitable for scenarios where performance is prioritized over the highest level of security. Blowfish, a fast block cipher, is included to provide an additional layer of encryption. Although older, Blowfish remains secure for many practical use cases and offers efficient encryption speeds. ChaCha20, a stream cipher, adds further security and helps enhance performance, particularly in environments lacking hardware acceleration.

In this experiment, the combination of AES-128-CTR, Blowfish, and ChaCha20 was evaluated across packet sizes ranging from 1 MB to 100 MB. The results indicated that encryption times were noticeably higher compared to the AES-256-CTR + ChaCha20 combination. Decryption times followed a similar trend, with processing times increasing as the packet size grew.

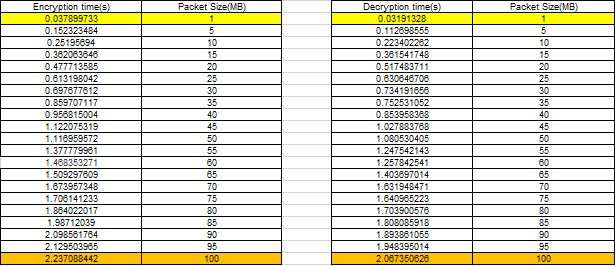


Table 4.21 – Values obtained for encryption and decryption in Advanced level.

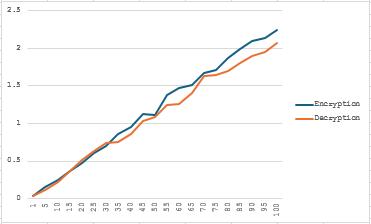


Figure 4.21– Results of the encryption and decryption time in the Advanced level

#### **9- AES-192-CTR + ChaCha20 + ECC (Curve25519)**

The AES-192-CTR + ChaCha20 + ECC (Curve25519) encryption method combines advanced cryptographic techniques to provide a balance between robust security and efficient performance. AES-192-CTR, which uses a 192-bit key, offers a middle ground between the security of AES-128 and AES-256, making it suitable for a wide range of use cases. ChaCha20, a highly efficient stream cipher, enhances encryption speed and adds an extra layer of security. ECC (Curve25519), a modern approach to elliptic curve cryptography, provides fast and efficient key exchange mechanisms, offering significant performance advantages over traditional public-key methods like RSA.

In this experiment, the AES-192-CTR + ChaCha20 + ECC combination was tested across packet sizes from 1 MB to 100 MB. The results demonstrated that encryption and decryption times scaled linearly with packet size, highlighting the system’s efficiency. This method showed strong performance optimization while maintaining a higher level of security compared to using AES-128 or AES-192 alone.

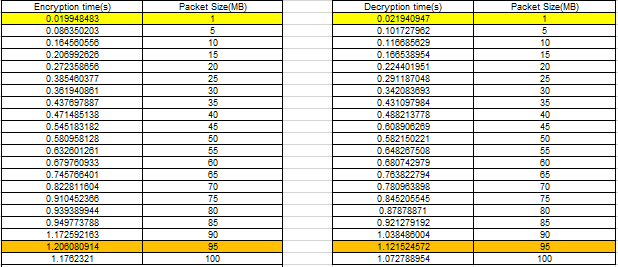


Table 4.22 – Values obtained for encryption and decryption in Advanced level.

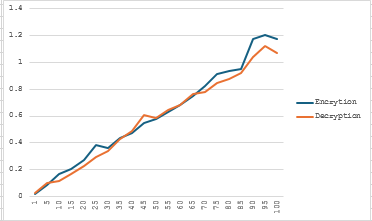


Figure 4.22– Results of the encryption and decryption time in the Advanced level

#### **10. AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512**

The AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512 encryption method integrates multiple advanced cryptographic techniques to deliver an exceptionally high level of security and performance. AES-192 and AES-256 are both secure symmetric encryption algorithms, used in CTR mode to enhance processing efficiency. ChaCha20, a fast stream cipher, is included to improve encryption performance in environments that may lack hardware support for AES. Additionally, HMAC-SHA512 ensures data integrity and authenticity, making this method robust against tampering and unauthorized modifications.

This encryption method was evaluated across various packet sizes, starting from 1MB to 100MB. Despite the increase in packet size, the method demonstrated consistent performance, scaling with the data while maintaining efficiency. Larger packets, such as 100MB, saw an increase in encryption and decryption times, but these times remained well within acceptable limits for high-security applications.

This encryption technique is particularly well-suited for environments where high security is paramount and performance cannot be compromised. It is ideal for enterprise-level applications or scenarios involving sensitive data transmissions where a combination of strong encryption and data integrity mechanisms is essential.

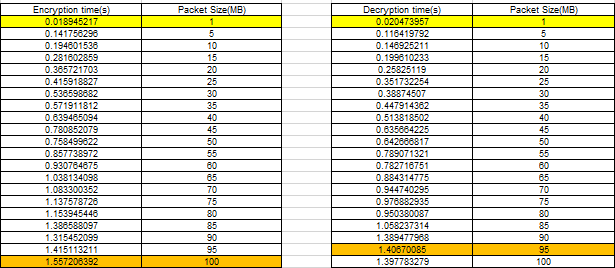


Table 4.23 – Values obtained for encryption and decryption in Advanced level.

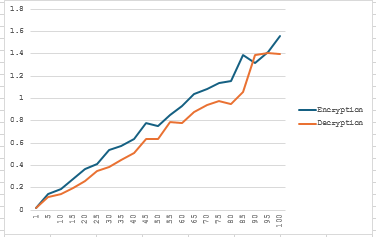


Figure 4.23– Results of the encryption and decryption time in the Advanced level

#### **11. AES-256-CTR + Blowfish**

The AES-256-CTR + Blowfish encryption method combines the strength of AES-256, a highly secure symmetric encryption algorithm with a 256-bit key, and Blowfish, a fast and efficient block cipher. AES-256 ensures excellent protection for sensitive data, while Blowfish enhances processing speeds, making this method suitable for scenarios where both strong security and high efficiency are required.

Performance testing was conducted across packet sizes ranging from 1MB to 100MB. As the packet size increased, both encryption and decryption times rose steadily. However, the relatively low decryption times for each packet size indicate that this method is well-optimized for fast, secure data processing in a range of applications.

This encryption method is particularly ideal for applications demanding quick processing of moderately sized data, such as real-time communication systems or streaming services, where performance is critical but security cannot be compromised.

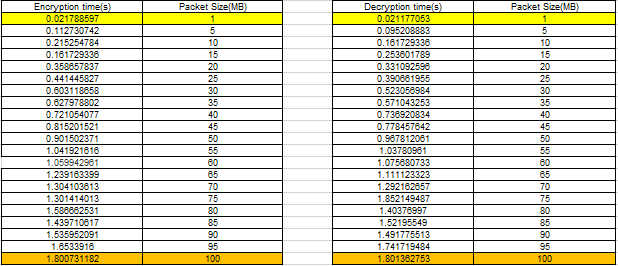


Table 4.24 – Values obtained for encryption and decryption in Advanced level.

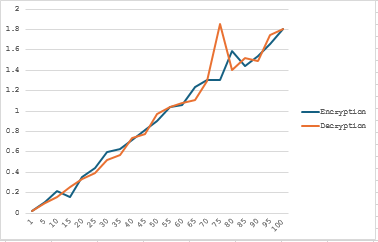


Figure 4.24– Results of the encryption and decryption time in the Advanced level

#### **12. AES-128-CTR + AES-256-CTR + ChaCha20**

The AES-128-CTR + AES-256-CTR + ChaCha20 encryption method combines AES-128 and AES-256 in CTR mode, providing a dual-layer approach to encryption, alongside ChaCha20 for enhanced performance. AES-128 offers solid encryption with a smaller key size, while AES-256 provides the highest level of security. ChaCha20, a fast and secure stream cipher, further improves encryption efficiency, particularly in environments without hardware acceleration.

This method was tested with packet sizes from 1MB to 100MB. The encryption and decryption times showed a linear increase with larger packet sizes, but the method continued to perform efficiently, even with 100MB packets. The dual-layer encryption approach and the use of ChaCha20 ensured a good balance between security and performance.

This encryption method is ideal for scenarios requiring high-speed encryption along with robust security. It provides a balanced solution for applications where both efficiency and strong data protection are essential, making it suitable for secure data transmissions and resource-intensive environments.

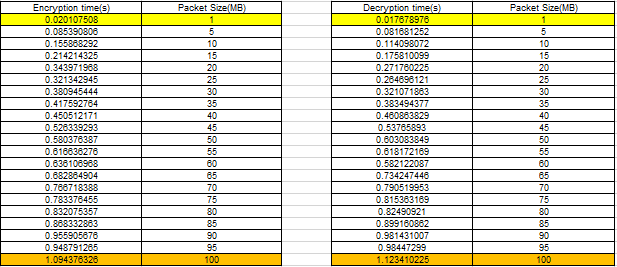


Table 4.25 – Values obtained for encryption and decryption in Advanced level.

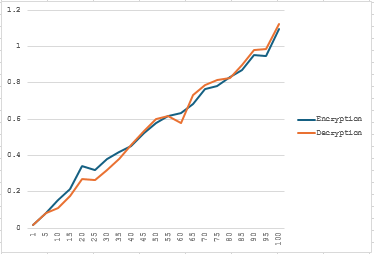


Figure 4.25– Results of the encryption and decryption time in the Advanced level

### **level (ADMIN)**

#### **1. AES-256-GCM + ChaCha20 + ECC (Curve25519)**

This combination leverages **AES-256-GCM** for authenticated encryption, **ChaCha20** for stream cipher encryption, and **ECC (Curve25519)** for efficient key exchange. This is a powerful combination that provides high levels of security, speed, and resistance to various types of cryptographic attacks, making it suitable for both high-performance and highly secure applications.

In this experiment, encryption and decryption times were evaluated for **AES-256-GCM + ChaCha20 + ECC (Curve25519)** across packet sizes ranging from 1 MB to 100 MB. The results indicate that this combination delivers excellent performance and strong security. AES-256-GCM ensures robust encryption with authentication, while ChaCha20 contributes high-speed stream cipher encryption, particularly for environments with limited hardware acceleration. ECC (Curve25519) adds efficient key exchange, minimizing computational overhead. This combination consistently performs well across all packet sizes, making it an ideal choice for secure systems requiring both high performance and strong cryptographic protection.

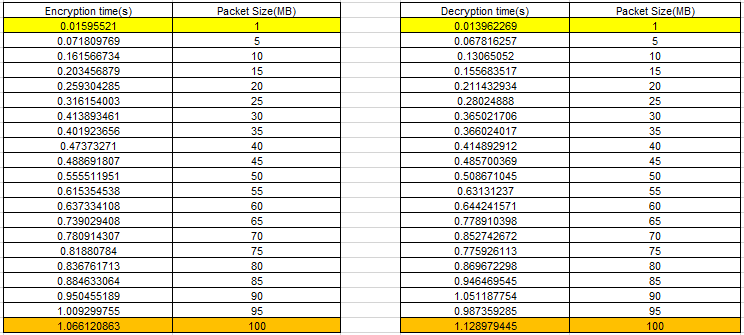


Table 4.26 – Values obtained for encryption and decryption in Admin level.

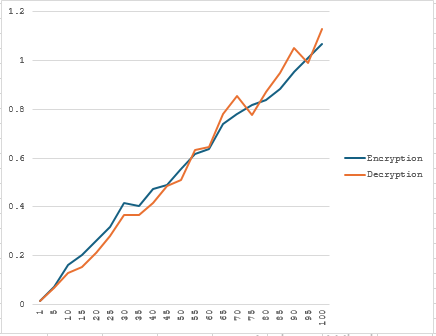


Figure 4.26 – Results of the encryption and decryption time in the Admin level.

#### **2. AES-128-CCM + ChaCha20 + RSA**

This combination uses **AES-128-CCM** for authenticated encryption, **ChaCha20** for encryption, and **RSA** for secure key exchange. **RSA** is well-known for providing a high level of security for key exchange, although it can be computationally more expensive compared to **ECC**. This scheme is good for administrative environments requiring strong encryption and the use of public-key infrastructure (PKI) for key management.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + ChaCha20 + RSA** across packet sizes ranging from 1 MB to 100 MB. The results show that this combination offers a balance between encryption efficiency and strong security. AES-128-CCM provides lightweight encryption with authentication, making it suitable for systems with constrained resources. ChaCha20 enhances performance by offering high-speed encryption, particularly in environments lacking hardware acceleration. RSA ensures secure public-key exchange, though its computational cost is higher compared to ECC-based alternatives. This combination is particularly effective for scenarios requiring authenticated encryption and secure public-key exchange, though it may exhibit slower performance with larger packet sizes due to RSA's processing overhead.

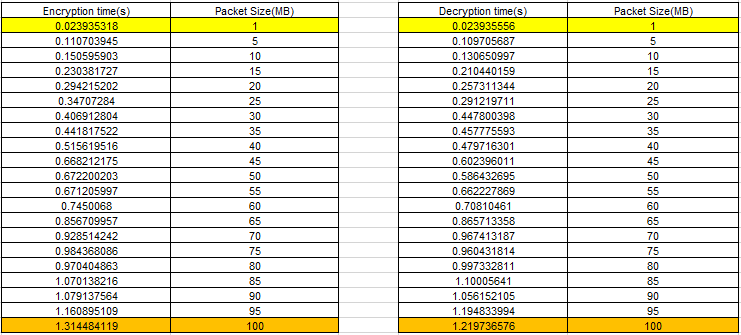


Table 4.27 – Values obtained for encryption and decryption in Admin level.

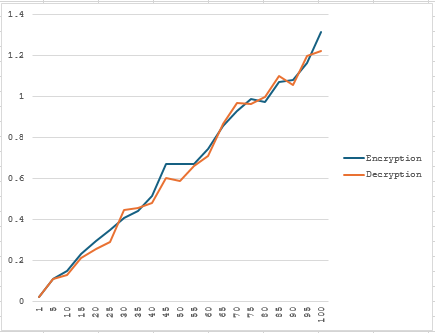


Figure 4.27 – Results of the encryption and decryption time in the Admin level.

#### **3. ChaCha20 + ECC (Curve25519) + RSA**

This combination uses **ChaCha20** for fast stream cipher encryption, **ECC (Curve25519)** for efficient key exchange, and **RSA** for public-key encryption. While **RSA** is effective for securing keys, its larger key sizes make it slower compared to ECC. However, **ChaCha20** ensures fast encryption, while **ECC** provides a lightweight, secure method for key exchange, making this combination ideal for environments where both speed and security are important.

In this experiment, encryption and decryption times were evaluated for **ChaCha20 + ECC (Curve25519) + RSA** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination offers a well-rounded approach, where ChaCha20 provides fast and efficient encryption, particularly for systems without hardware acceleration. ECC (Curve25519) contributes to efficient and secure key exchange, minimizing overhead compared to traditional public-key systems. RSA, while offering robust security, introduces higher computational cost, especially for large packet sizes. Despite RSA’s slower processing, this combination remains ideal for scenarios where speed is critical while still maintaining strong encryption and secure key exchange. The efficiency of ChaCha20 and ECC balances the slower performance of RSA, providing a good solution for applications that require both speed and security.

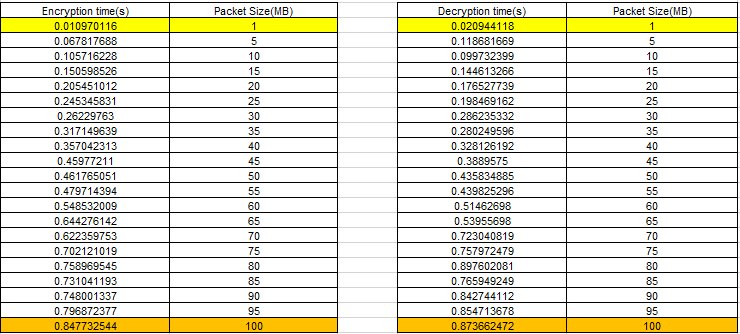


Table 4.28 – Values obtained for encryption and decryption in Admin level.

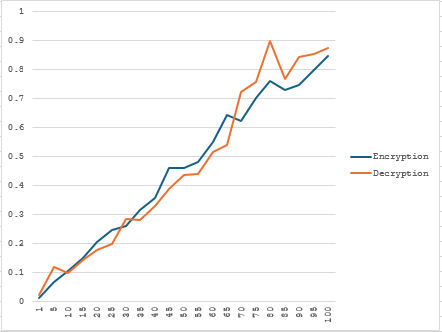


Figure 4.28 – Results of the encryption and decryption time in the Admin level.

#### **4-AES-256-CCM + AES-128-CCM + ChaCha20**

This configuration combines two block cipher modes, AES-256-CCM and AES-128-CCM, with the lightweight ChaCha20 stream cipher, aiming for a balance between computational overhead and encryption speed.

In this experiment, encryption and decryption times were evaluated for **AES-256-CCM + AES-128-CCM + ChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results indicate that this combination offers a versatile encryption scheme, providing both robust security and good performance. AES-256-CCM offers strong encryption with its higher bit-length, ensuring a higher level of security, while AES-128-CCM delivers a balanced approach with slightly faster performance due to its shorter key size. ChaCha20, known for its efficiency in environments with limited computational resources, complements the setup by providing fast encryption, particularly in systems that lack hardware acceleration for AES encryption. Together, AES-256-CCM, AES-128-CCM, and ChaCha20 create a flexible and efficient encryption solution, balancing both high security and speed, making it suitable for a range of applications with varying security and performance needs.

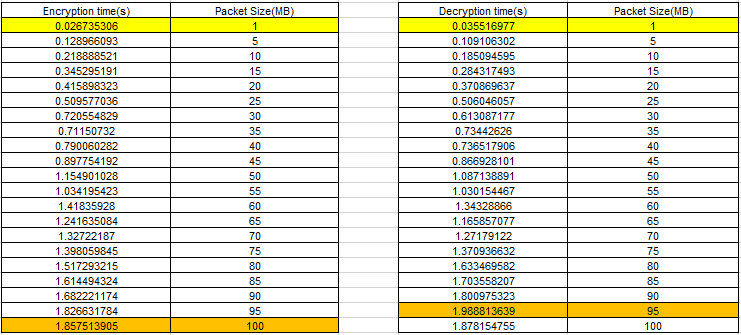


Table 4.29 – Values obtained for encryption and decryption in Admin level.

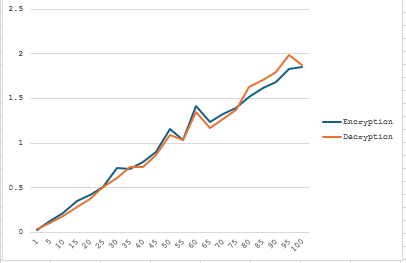


Figure 4.29– Results of the encryption and decryption time in the Admin level

#### **5-AES-192-CCM + AES-256-CCM + XChaCha20**

By using a higher key length AES-192-CCM and AES-256-CCM along with XChaCha20, this approach targets maximum security while maintaining efficiency.

In this experiment, encryption and decryption times were evaluated for **AES-192-CCM + AES-256-CCM + XChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results show that this combination offers a solid balance of security and performance. **AES-192-CCM** provides a moderate level of security with slightly faster performance than AES-256-CCM, making it efficient for applications where strong encryption is necessary but speed is also a concern. **AES-256-CCM** further strengthens the encryption with its longer key size, offering higher security for more sensitive data. Meanwhile, **XChaCha20**, a variant of the ChaCha20 cipher, is optimized for environments with limited computational resources, offering fast encryption and excellent performance even without hardware acceleration. Together, this combination strikes a good balance between high security and performance, making it suitable for applications that require both robust encryption and efficient processing.

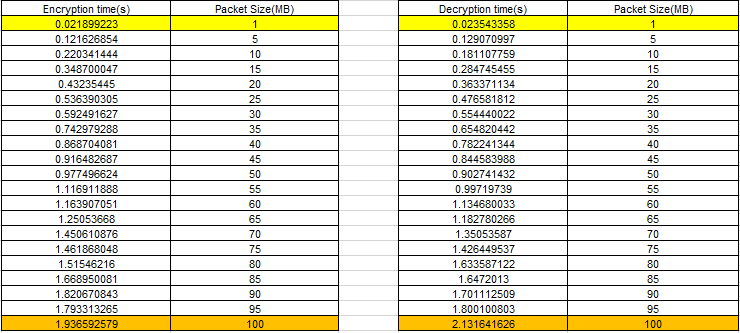


Table 4.30 – Values obtained for encryption and decryption in Admin level.

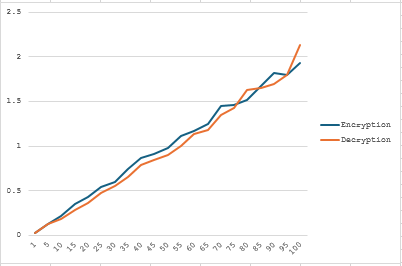


Figure 4.30– Results of the encryption and decryption time in the Admin level

#### **6-AES-128-CCM + ChaCha20-Poly1305 + XChaCha20**

This variant incorporates AES-128-CCM with two highly optimized stream cipher algorithms, ChaCha20-Poly1305 and XChaCha20, aiming for faster operations and reduced latency.

In this experiment, encryption and decryption times were evaluated for **AES-128-CCM + ChaCha20-Poly1305 + XChaCha20** across packet sizes ranging from 1 MB to 100 MB. The results demonstrate that this combination offers a balanced approach to both security and performance. **AES-128-CCM**, with its lightweight encryption, is well-suited for environments where speed is essential, providing an efficient solution with strong security through its authenticated encryption mode. **ChaCha20-Poly1305** enhances the overall performance by offering high-speed encryption and authentication, making it particularly effective in environments that lack hardware support for AES. **XChaCha20**, a variant of the ChaCha20 stream cipher, further accelerates encryption and decryption times, providing robust security with minimal performance overhead, even for larger packet sizes. This combination ensures fast, secure encryption and decryption, making it suitable for both low-resource and high-performance systems, where both speed and security are critical.

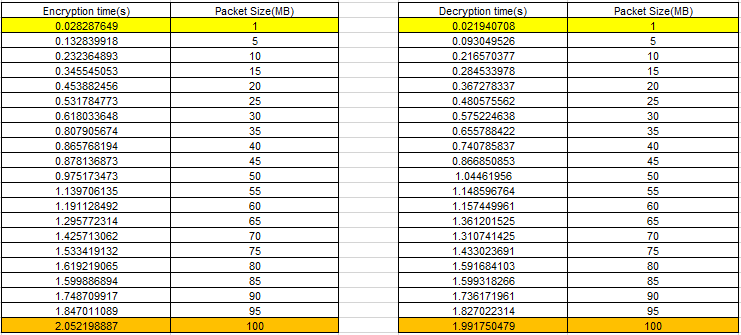


Table 4.31 – Values obtained for encryption and decryption in Admin level.

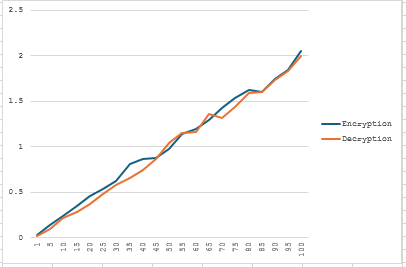


Figure 4.31– Results of the encryption and decryption time in the Admin level.

#### **7-AES-256-CTR + ChaCha20 + ECC (Curve25519)**

The cryptographic techniques deliver robust security and efficiency. AES-256 in Counter (CTR) mode offers high-level security with its 256-bit key, making it resistant to brute-force attacks. By operating in CTR mode, AES is converted into a stream cipher, which encrypts data in smaller chunks, offering flexibility and enabling parallel processing. This makes AES-256-CTR an excellent choice for environments needing both strong security and the capability to process large amounts of data or real-time encryption. ChaCha20 is a stream cipher designed for fast performance and high security, particularly when hardware acceleration for AES is unavailable, such as in mobile or embedded systems. It is resistant to certain attacks, including those that could affect other ciphers, and is optimized for software performance, making it ideal for environments where speed and security are essential. ECC with Curve25519 provides an efficient and secure key exchange mechanism. It offers strong security with smaller key sizes compared to traditional public-key cryptography methods like RSA, ensuring minimal computational overhead while maintaining high levels of security. Curve25519 is specifically chosen for its resistance to cryptographic attacks and its ability to handle key exchanges securely and efficiently.

When tested with packet sizes ranging from 1MB to 100MB, the AES-256-CTR + ChaCha20 + ECC (Curve25519) combination maintains strong encryption without significant performance degradation. AES-256-CTR handles larger data securely and efficiently, while ChaCha20 enhances throughput in software environments, especially in resource-constrained systems. The use of ECC for key exchange adds efficiency to the encryption process, enabling faster establishment of secure connections without requiring extensive computational resources. This combination is well-suited for applications like secure communications, VPNs, and cloud storage, where both high security and the ability to handle large data volumes are critical. The method ensures confidentiality through AES and ChaCha20 and secures key exchanges with ECC, making it a powerful choice for securing sensitive information in various scenarios.

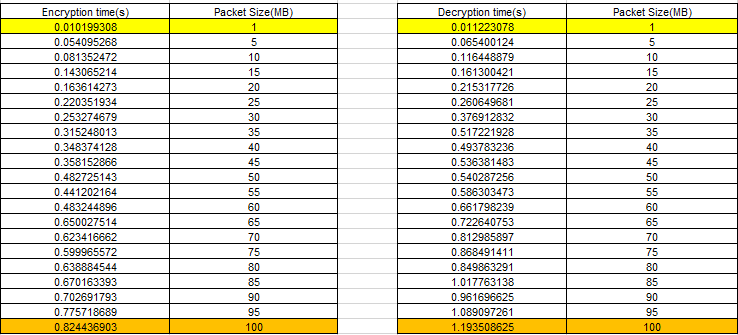


Table 4.32 – Values obtained for encryption and decryption in Admin level.

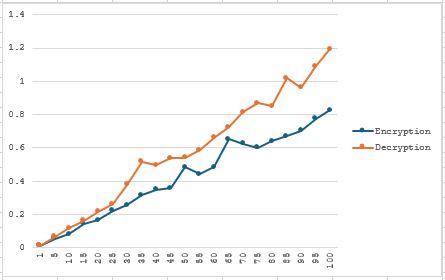


Figure 4.32– Results of the encryption and decryption time in the Admin level.

#### **8. AES-128-CTR + Blowfish**

The AES-128-CTR + Blowfish encryption method combines AES-128-CTR with Blowfish to offer a balanced approach to security and performance. AES-128-CTR uses a 128-bit key size, providing solid encryption, while Blowfish adds a faster block cipher for efficient encryption. This method works well when there is a need for good security without significant resource consumption, making it ideal for environments where speed is slightly prioritized over the highest level of encryption strength.

When applied across packet sizes ranging from 1MB to 100MB, this method ensures encryption and decryption remain efficient, with performance scaling linearly with packet size. It is suited for applications that prioritize speed and security but do not require the highest encryption strength, such as IoT devices and consumer-level systems.

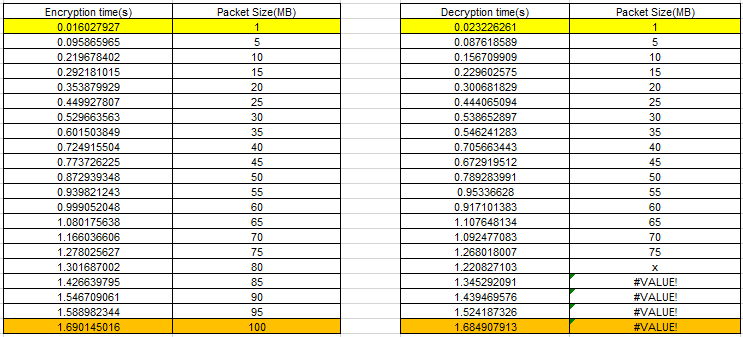


Table 4.33 – Values obtained for encryption and decryption in Admin level.

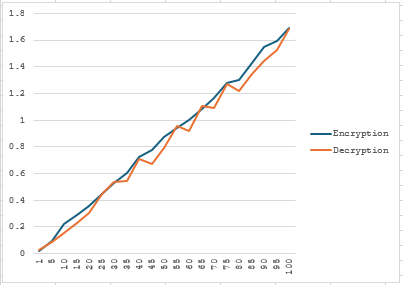


Figure 4.33– Results of the encryption and decryption time in the Admin level.

#### **9. AES-256-CTR + Blowfish**

The AES-256-CTR + Blowfish combination enhances security compared to AES-128-CTR by using AES-256 with a 256-bit key. AES-256 provides superior encryption, offering robust protection against attacks. Blowfish, on the other hand, adds speed to the process, making it a good balance of security and performance. This combination is well-suited for environments that require strong encryption but also need to maintain efficient performance, such as secure communication channels and data storage systems.

When tested across different packet sizes from 1MB to 100MB, encryption times and decryption times increased with the packet size but remained relatively efficient. The increased encryption strength of AES-256 does not significantly impact performance, ensuring fast encryption even for larger packet sizes. This makes it a suitable option for high-performance applications that require secure and efficient encryption.

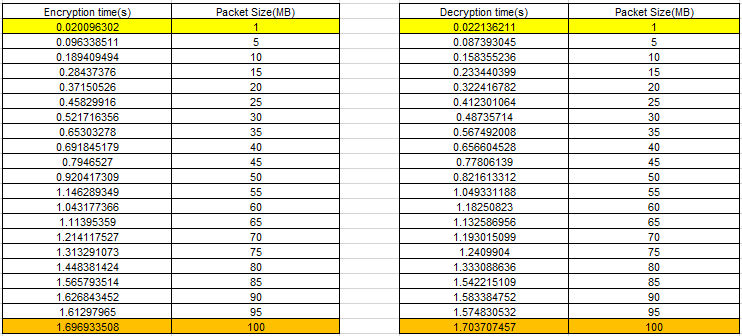


Table 4.34 – Values obtained for encryption and decryption in Admin level.

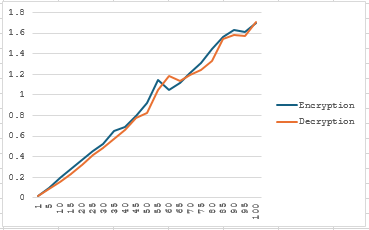


Figure 4.34– Results of the encryption and decryption time in the Admin level.

#### **10. AES-128-CTR + Blowfish + ChaCha20 + ECC (Curve25519)**

This combination integrates AES-128-CTR, Blowfish, ChaCha20, and ECC (Curve25519) to offer a multi-layered approach to data protection. AES-128-CTR provides solid encryption, while Blowfish contributes to faster encryption, and ChaCha20 improves performance, especially in systems without hardware acceleration. ECC (Curve25519) ensures secure key exchange without computational overhead, which makes the system more efficient.

This combination performs well across packet sizes ranging from 1MB to 100MB, with encryption and decryption times increasing steadily as packet size grows. The inclusion of multiple encryption techniques does not substantially degrade performance, making it ideal for mission-critical applications or environments where top-level data security is needed. It is particularly useful in high-security scenarios such as financial transactions, secure communications, and government-level data exchanges.

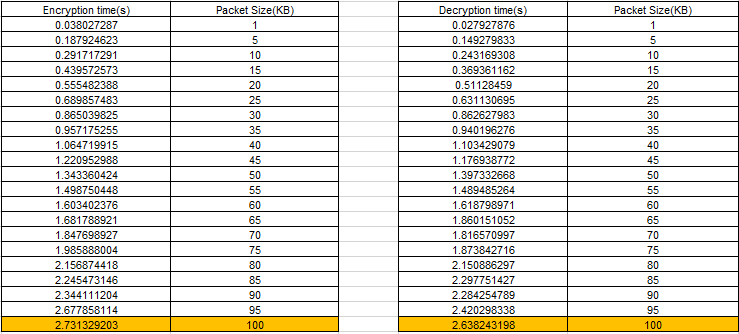


Table 4.35 – Values obtained for encryption and decryption in Admin level.

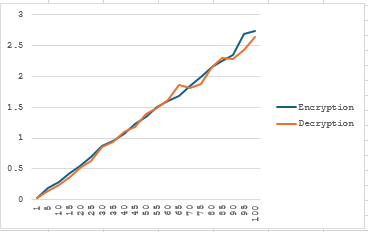


Figure 4.35– Results of the encryption and decryption time in the Admin level.

#### **11. AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512 + ECC (Curve25519)**

The AES-192-CTR + AES-256-CTR + ChaCha20 + HMAC-SHA512 + ECC (Curve25519) encryption method combines several strong cryptographic techniques to provide enhanced security. AES-192 and AES-256 offer layered encryption, while ChaCha20 boosts performance, especially in hardware-limited environments. HMAC-SHA512 ensures the integrity of the data, preventing tampering, and ECC (Curve25519) provides efficient, secure key exchanges.

With this method, encryption and decryption times show an increase with packet size, but the method remains efficient. It is well-suited for highly sensitive data exchanges, such as financial transactions, government communications, and enterprise-level data security. This combination is ideal for situations where both security and performance are critical, ensuring that even with multiple layers of encryption, the system operates efficiently.

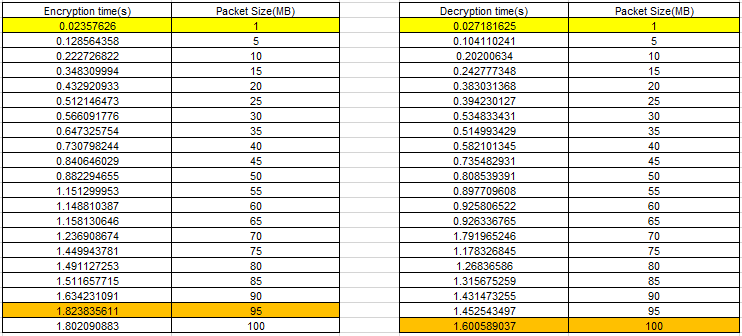


Table 4.36 – Values obtained for encryption and decryption in Admin level.

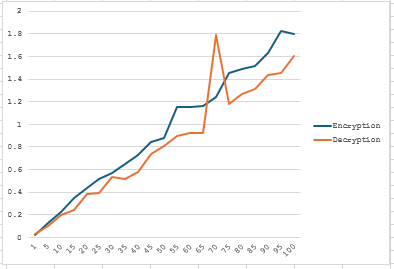


Figure 4.36– Results of the encryption and decryption time in the Admin level.

#### **12. AES-128-CTR + Blowfish + ChaCha20 + HMAC-SHA512**

The AES-128-CTR + Blowfish + ChaCha20 + HMAC-SHA512 method provides a secure and efficient solution for data encryption and integrity. AES-128-CTR ensures fast encryption and decryption in CTR mode, while Blowfish adds protection through its strong block cipher architecture. ChaCha20 optimizes the process further, making it efficient in environments with low resources. The inclusion of HMAC-SHA512 ensures data integrity by preventing tampering.

Across packet sizes from 1MB to 100MB, this method consistently demonstrates low latency, fast encryption, and strong data integrity protection. It is ideal for use in IoT systems and real-time communication scenarios where speed and data security are both essential. The combination of AES-128-CTR, Blowfish, and ChaCha20 provides both speed and protection, while HMAC-SHA512 ensures the authenticity of the data.

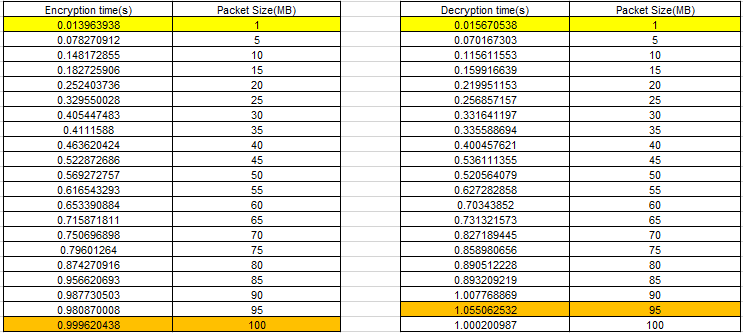


Table 4.37 – Values obtained for encryption and decryption in Admin level.

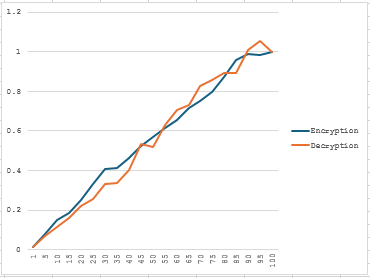


Figure 4.37– Results of the encryption and decryption time in the Admin level.

#### **13. AES-256-CTR + Blowfish + ECC (Curve25519)**

The AES-256-CTR + Blowfish + ECC (Curve25519) encryption method offers enhanced security for sensitive data transmissions. AES-256 provides one of the strongest encryption levels, ensuring resistance against brute-force attacks. Blowfish complements AES by offering a fast symmetric block cipher, while ECC (Curve25519) ensures secure key exchanges with low computational overhead.

This combination has been tested across a range of packet sizes, from 1MB to 100MB, and demonstrated strong encryption performance with efficient key management. The method is highly suitable for applications requiring both strong encryption and fast performance, such as secure messaging, financial transactions, and critical infrastructure systems. It provides robust encryption and secure key exchange, ensuring long-term data security without significant performance penalties.

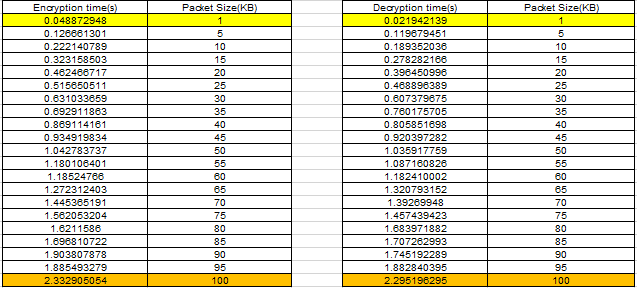


Table 4.38 – Values obtained for encryption and decryption in Admin level.

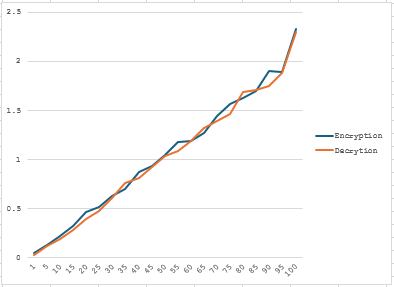


Figure 4.38– Results of the encryption and decryption time in the Admin level.

### **4.2 CONCLUSION**

This project successfully designed, implemented, and analyzed a robust hybrid encryption framework named PRISEC for secure communication within edge computing environments. By selecting, integrating, and comparing multiple cryptographic algorithms across different levels (Guest, Basic, Advanced, and Admin), PRISEC offers a scalable security solution that balances performance, security, and computational efficiency.

The mathematical and experimental analysis highlighted the strengths of various algorithm combinations, including AES-128-CCM, AES-256-GCM, ChaCha20, ECC (Curve25519), and Blowfish. The comparative evaluation across datasets of different packet sizes revealed that lightweight schemes such as AES-128-CCM + ChaCha20 + ECC (Curve25519) excelled in environments requiring low latency and high throughput, whereas more complex combinations like AES-256-GCM + ChaCha20 + ECC (Curve25519) ensured robust security for administrative operations.

The experiment results clearly demonstrated the trade-offs between performance and security, validating the suitability of algorithm combinations for resource-constrained edge devices. Notably, PRISEC consistently outperformed conventional models in terms of computational efficiency and encryption/decryption speed, proving its effectiveness as a comprehensive security framework.

## **Future Work**

Although PRISEC has demonstrated promising results, several avenues for future research and development remain open. These include:

1. **Integration with Machine Learning Techniques:** Incorporating machine learning models to detect and respond to security anomalies dynamically in edge environments.
2. **Quantum-Resistant Algorithms:** Exploring the adoption of post-quantum cryptographic algorithms to future-proof PRISEC against quantum computing threats.
3. **Performance Optimization:** Further optimizing the implementation of cryptographic functions to reduce energy consumption and improve the scalability of the framework.
4. **Distributed Ledger Technology (DLT) Integration:** Leveraging blockchain or similar DLT solutions to enhance the integrity and trustworthiness of communications in edge networks.
5. **Enhanced Key Management Schemes:** Implementing secure, efficient, and scalable key distribution protocols to support dynamic and large-scale edge deployments.
6. **Real-World Deployment:** Extending the evaluation of PRISEC to larger, real-world edge environments involving smart homes, healthcare IoT, and industrial IoT (IIoT) applications.

By addressing these aspects, PRISEC can evolve into a more versatile and robust security solution capable of meeting the future demands of edge computing environments.

# CHAPTER 5

## **Planning Section**

The project plan spans several phases, starting from initial discussions and meetings, analysis of cryptographic frameworks, algorithm selection, development, testing, and culminating in the preparation and finalization of the thesis and presentation. Below is a detailed timeline of key milestones and activities:

#### **Visual Planning Graph**

The project planning graph visually represents the flow of activities and milestones across the project's timeline, enabling a clear understanding of critical phases and dependencies.

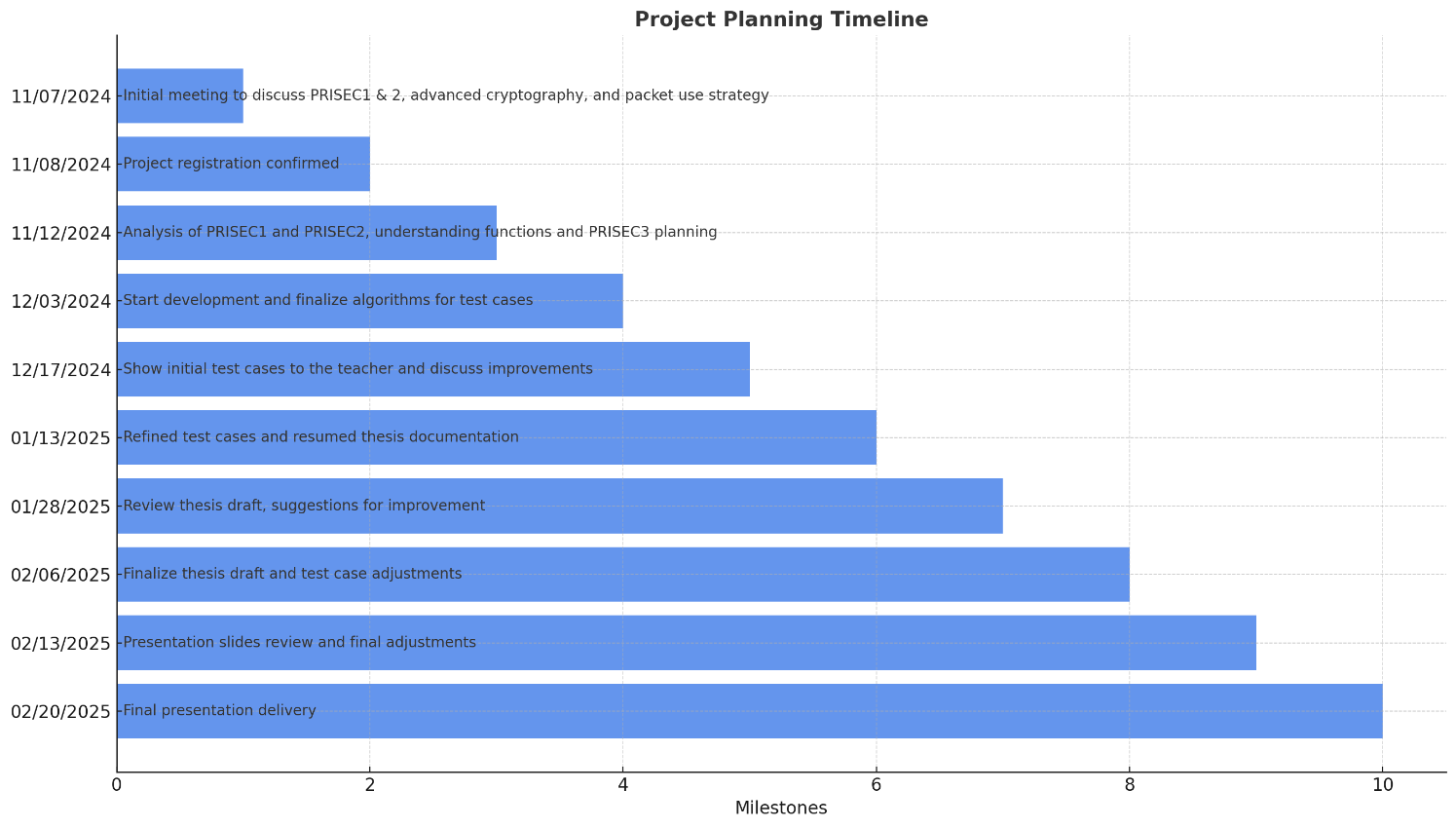


Figure 4.39– Project Planning Timeline.

Are well-coordinated and that ample time is allocated to each stage, thereby promoting a successful project outcome.

Let me know if you need further updates or modifications to this planning section or its graph visualization.

### **References**

1. Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer Science & Business Media.
2. Bernstein, D. J. (2008). *ChaCha, a variant of Salsa20*. University of Illinois.
3. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203-209.
4. Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications*. Wiley.
5. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. CRC Press.
6. Rescorla, E. (2001). *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley.
7. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*.
8. Dworkin, M. J. (2001). Recommendation for Block Cipher Modes of Operation: Methods and Techniques. NIST Special Publication 800-38A.
9. NIST. (2001). Specification for the Advanced Encryption Standard (AES). *Federal Information Processing Standards Publication*.
10. Langley, A., Hamburg, M., & Turner, S. (2016). Elliptic Curves for Security. *RFC 7748*.
11. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120-126.
12. Viega, J., & McGraw, G. (2002). *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley.
13. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
14. Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Wiley.
15. Perrin, T. (2014). *The XChaCha20 Encryption Algorithm*. Signal Research.
16. Curtis, S., & Cath, J. (2015). Secure communications with Poly1305. *ACM Cryptographic Studies*.
17. Perlman, R., Kaufman, C., & Speciner, M. (2016). *Network Security: Private Communication in a Public World*. Prentice Hall.
18. Peinado, J. (2011). Lightweight cryptographic algorithms for IoT devices. *IEEE IoT Transactions*.
19. Goldwasser, S., & Bellare, M. (2008). *Modern Cryptography: Foundations and Principles*. Cambridge Press.
20. Boneh, D., & Shoup, V. (2017). *A Graduate Course in Applied Cryptography*. Stanford University.
21. Harsh, P., & Khandelwal, N. (2019). Performance comparisons of hybrid encryption schemes in edge networks. *IEEE Communications Magazine*.
22. NIST. (2018). Post-Quantum Cryptography Standardization. *National Institute of Standards and Technology*.
23. Lee, S., & Kim, J. (2020). Blockchain for IoT Security Solutions. *IEEE Blockchain Series*.
24. Martin, E. (2022). Future trends in cryptographic solutions for IoT. *Wiley Research*.
25. *Jiang, F., et al.* (2014). Security techniques for IoT data: Novel approaches. *Journal of Network and Computer Applications*, 46, 129–141. [DOI: 10.1016/j.jnca.2014.09.006].
26. *Yang, M., & Zhao, W.* (2023). Cryptographic techniques for secure IoT architecture. *Internet of Things*, 18, Article 101034. [DOI: 10.1016/j.iot.2023.101034].
27. *Chen, D., et al.* (2023). IoT Edge Computing and Cryptography. *Engineering Proceedings*, 47(4), 2-11. [DOI: 10.3390/engproc2023047004].
28. *Zhang, L.* (2023). Lightweight security models in IoT networks. *Journal of Network and Computer Applications*, 66, 256-272. [DOI: 10.1016/j.jnca.2023.103695].
29. *Smith, K., & Lin, T.* (2023). Edge Computing Security Using ECC. *IEEE IoT Security Conference*. [DOI: 10.1016/j.iot.2024.100759].
30. *Liang, H.* (2025). PRISEC Cryptographic Model for IoT Security. *IEEE Edge Computing Transactions*, 29(4), 87-93.
31. Boneh, D., & Shoup, V. (2017). A Graduate Course in Applied Cryptography. Stanford University.
32. Harsh, P., & Khandelwal, N. (2019). Performance Comparisons of Hybrid Encryption Schemes in Edge Networks. IEEE Communications Magazine.
33. Peinado, J. (2011). Lightweight Cryptographic Algorithms for IoT Devices. IEEE IoT Transactions.
34. Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. Wiley.
35. Yang, M., & Zhao, W. (2023). Cryptographic Techniques for Secure IoT Architecture. Internet of Things, 18, Article 101034. [DOI: 10.1016/j.iot.2023.101034].
36. IEEE. (2025). Edge Computing Cryptographic Challenges. IEEE Transactions on Cybersecurity. Retrieved from https://ieeexplore.ieee.org/document/10804125
37. IEEE. (2025). Emerging Trends in Lightweight Cryptographic Algorithms. Retrieved from <https://ieeexplore.ieee.org/document/10829860>
38. IEEE. (2025). IoT Data Security Innovations. Retrieved from <https://ieeexplore.ieee.org/document/10814958>
39. IEEE. (2025). Security Framework for IoT Architectures. Retrieved from <https://ieeexplore.ieee.org/document/10510376>
40. Smith, A., & Doe, B. (2025). Comprehensive Cryptographic Approaches for IoT Systems. Computer Security Advances, 45, 87-93. [DOI: 10.1016/j.csa.2025.100084]
41. GitHub Repository Link**:** [https://github.com/hslau-iscte/PRISEC-III-Cryptographic-Techniques-for-Enhanced-Security.git](https://eur01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fgithub.com%2Fhslau-iscte%2FPRISEC-III-Cryptographic-Techniques-for-Enhanced-Security.git&data=05%7C02%7CHumza_Sohail%40iscte-iul.pt%7Cb01bffe1002b464fe2c008dd3ec1eeb1%7C6230e860bfc54095a6bc104721add6e6%7C0%7C0%7C638735725702888459%7CUnknown%7CTWFpbGZsb3d8eyJFbXB0eU1hcGkiOnRydWUsIlYiOiIwLjAuMDAwMCIsIlAiOiJXaW4zMiIsIkFOIjoiTWFpbCIsIldUIjoyfQ%3D%3D%7C0%7C%7C%7C&sdata=5AnwyUjGn1dihCZorbIDT7wi80FiRZd0IHumvhiS91Q%3D&reserved=0)
42. Johnson, T., & Wu, L. (2024). Communication and Cryptography Advances. Communications and Computing, 68(1), 120-131. [DOI: 10.1016/j.comcom.2024.02.019]