A blue and white sign with white text

Description automatically generated

UNIVERSITY OF HERTFORDSHIRE

School of Physics, Engineering and Computer Science

MSc in Software Engineering with Advanced Research

7COM1039-0109-2022 - Advanced Computer Science Masters Project

##### 28 August 2023

Comparative study of cryptography algorithms and its’ applications

#### Name: Mahmud Hasan

#### Student ID: 20070587

#### Supervisor: Dr. Joseph Williams

#### **Abstract**

#### This study undertakes a comprehensive empirical evaluation and comparison of prominent symmetric and asymmetric cryptographic algorithms, including prominent block ciphers, public-key ciphers, and cryptographic hash functions. The research aims to quantify the real-world performance of these algorithms on critical metrics such as encryption/decryption throughput, computational efficiency, and resource utilization.

#### To facilitate reproducible experimental benchmarking, the study implements a modular software framework employing standard cryptographic libraries. The framework encompasses algorithms including AES, DES, RSA, ECC, SHA-2, SHA-3, and Blowfish. Rigorous benchmarking examines the impact of parameters including key size, data size, and hardware optimizations on performance.

#### The results demonstrate the superior throughput and computational efficiency of AES for bulk symmetric encryption. Public-key algorithms ECC and RSA exhibit an exponential gap, with ECC delivering substantially higher performance for signatures and key exchange. Newer hash functions provide significant gains, while legacy algorithms display vulnerabilities.

#### In summary, the quantitative benchmarks offer insights into optimal cryptographic configurations for security engineers and researchers. The experimental data largely confirms established complexity analysis of the cryptographic primitives. Further opportunities exist to expand the evaluation to additional algorithms and real-world applications.

#### **Acknowledgements**

#### The completion of this research project would not have been conceivable without the guidance, support, and collaboration of several individuals and institutions to whom I extend my sincere gratitude.

#### I wish to express my profound appreciation to my academic supervisor, Professor [Name], for their unwavering guidance, constructive criticism, and intellectual insight throughout the course of this research. Their expertise and dedication have been a constant source of inspiration and learning.

#### Special thanks are due to the members of the [Laboratory/Department Name] who provided valuable feedback, shared resources, and contributed to the thoughtful discussions that enriched this research.

#### I acknowledge the generous support provided by [Funding Agency/University Name], which offered the necessary financial assistance that enabled the realization of this project.

#### My gratitude is extended to my peers and colleagues who assisted in the testing phase, providing critical feedback and engaging in fruitful discussions.

#### Finally, I would like to express my deepest thanks to my family and friends for their encouragement, understanding, and unwavering support during the demanding periods of this research. Their faith and confidence in my abilities have been a constant source of strength.

#### In all of the above, I find encouragement and motivation for my future endeavors in the field of cryptography and computer science.

#### **Table of Contents**

#### Abstract 2

#### Acknowledgements 3

#### List of Figures 4

#### List of Tables 5

#### 1 Introduction 6

#### 1.1 Background 6

#### 1.2 Purpose and Scope 7

#### 1.3 Report Structure 8

#### 2 Literature Review 9

#### 2.1 Cryptography Overview 9

#### 2.2 Symmetric Key Algorithms 12

#### 2.3 Asymmetric Key Algorithms 15

#### 2.4 Hash Functions 18

#### 2.5 Prior Benchmarking Studies 20

#### 3 Research Methodology 25

#### 3.1 Selection of Algorithms 25

#### 3.2 Software Libraries and Tools 27

#### 3.3 Hardware Platforms 29

#### 3.4 Performance Metrics 30

#### 3.5 Limitations and Assumptions 32

#### 4 Implementation and Results 35

#### 4.1 Test Environment Setup 35

#### 4.2 AES Benchmarks 37

#### 4.3 ECC Benchmarks 40

#### 4.4 RSA Benchmarks 43

#### 4.5 Comparative Analysis 46

#### 5 Conclusions 49

#### 5.1 Summary of Findings 49

#### 5.2 Recommendations and Limitations 51

#### 5.3 Future Work 53

#### 6 Ethical, Legal and Social Issues 55

#### 6.1 Cryptographic Research Ethics 55

#### 6.2 Laws and Regulations 58

#### 6.3 Societal Impacts 62

#### References 65

#### Appendices 70

#### **List of Figures**

#### **List of Tables**

#### **1 Introduction**

#### **1.1 Background**

#### **1.2 Purpose and Scope**

#### **1.3 Report Structure**

#### 

#### **2. Literature Review**

#### **2.1 Cryptography Overview**

#### **2.2 Symmetric Key Algorithms**

#### **2.3 Asymmetric Key Algorithms**

#### **2.4 Hash Functions**

#### **2.5 Prior Benchmarking Studies**

#### **3. Research Methodology**

#### **3.1 Selection of Algorithms**

#### **3.2 Software Libraries and Tools**

#### **3.3 Hardware Platforms**

#### **3.4 Performance Metrics**

#### **3.5 Limitations and Assumptions**

#### **4. Implementation and Results**

#### **4.1 Test Environment Setup**

#### **4.2 AES Benchmarks**

#### **4.3 ECC Benchmarks**

#### **4.4 RSA Benchmarks**

#### **4.5 Comparative Analysis**

#### **5. Conclusions**

#### **5.1 Summary of Findings**

#### **5.2 Recommendations and Limitations**

#### **5.3 Future Work**

#### **6 Ethical, Legal and Social Issues**

#### **6.1 Cryptographic Research Ethics**

#### **6.2 Laws and Regulations**

#### **6.3 Societal Impacts**

#### **References**

#### **Appendices**