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**

#### Figure 1: Cryptographic Algorithm Families - Overview..........................9

#### Figure 2: Symmetric Key Algorithm - Block and Stream Ciphers.................13

#### Figure 3: Asymmetric Key Algorithms - RSA Key Generation Process..........16

#### Figure 4: Hash Functions - SHA-256 Operation..................................19

#### Figure 5: AES Benchmarks - Performance on Different Key Sizes...............38

#### Figure 6: ECC Benchmarks - Curve Comparisons.................................41

#### Figure 7: RSA Benchmarks - Performance with Various Key Lengths............44

#### Figure 8: Comparative Analysis - Speed, Security, and Efficiency..............47

#### Figure 24: Software Libraries and Tools - UML Diagram..........................28

#### Figure 25: Implementation Flowchart.............................................34

#### **List of Tables**

#### Table 1: Overview of Cryptographic Algorithms..........................10

#### Table 2: Symmetric Key Algorithms – Features and Uses.................14

#### Table 3: Asymmetric Key Algorithms – Key Lengths and Security......17

#### Table 4: Hash Functions – Characteristics and Applications.............20

#### Table 5: AES Benchmarks – Performance Metrics.........................39

#### Table 6: ECC Benchmarks – Curve Parameters and Security............42

#### Table 7: RSA Benchmarks – Key Lengths and Performance...............45

#### Table 8: Comparative Analysis – Algorithm Efficiency.....................49

#### Table 9: Ethical Considerations in Cryptographic Research.............58

#### Table 10: Societal Impacts of Cryptography – Case Studies............64

#### Table 11: Performance Metrics – Methods and Measurements...........32

#### Table 12: Hardware Platform – Desktop Specifications..................30

#### Table 13: Mobile Device – Technical Specifications......................31

#### Table 14: Limitations and Assumptions – List..............................34

#### Table 15: Test Environment Setup – Software and Tools.................37

#### Table 16: Comparative Analysis – Throughput vs. Latency..............48

#### Table 17: Legal Framework – International Regulations..................60

#### Table 18: Societal Impacts – Privacy and Security Considerations....63

#### Table 19: Future Work – Proposed Research Areas.......................55

#### Table 20: Summary of Findings – Conclusions.............................51

#### Table 21: Recommendations – Proposed Approaches.....................53

#### Table 22: Cryptographic Research Ethics – Guidelines...................57

#### Table 23: Laws and Regulations – Summary...............................61

#### Table 24: Software Libraries and Tools – List..............................29

#### Table 25: Implementation Steps – Workflow...............................35

#### **1 Introduction**

#### **1.1 Background**

#### As modern computing and communication systems have become inextricably linked to critical infrastructure, commerce, and personal data, the role of cryptography in enabling secure and trusted digital ecosystems continues growing rapidly (Abobar et al., 2022). Cryptography provides the technical mechanisms to realize the fundamental goals of information security - confidentiality, integrity, authentication, and non-repudiation (Menezes et al., 1996). By leveraging mathematical techniques to obscure meaning and establish identities, cryptographic algorithms facilitate activities ranging from encrypted networking to digital payments and signatures (Paar & Pelzl, 2009).

#### However, the proliferation of sensitive data online has been accompanied by increasingly sophisticated attacks and vulnerabilities targeting real-world cryptographic implementations. High-profile encryption failures like RC4 in WEP WiFi networks (Fluhrer et al., 2001), OpenSSL Heartbleed (Durumeric et al., 2014), and DROWN TLS attacks (Aviram et al., 2016) highlight the need to continuously reevaluate the robustness of widespread cryptographic primitives and protocols. As computational capabilities and cryptanalysis improve, acceptable standards of security and performance must evolve correspondingly.

#### Modern Cryptography:

#### Symmetric Key Algorithms: DES, replaced later by AES due to vulnerabilities, represents a widely-adopted symmetric encryption standard (NIST, 2001; Schneier, 1996).

#### Asymmetric Key Algorithms: Algorithms like RSA and ECC form the backbone of digital signatures and secure communication (Diffie & Hellman, 1976; Elliptic Curve Cryptography, 2004).

#### Hash Functions: SHA family of hash functions, including SHA-256, are crucial in data integrity verification (NIST, 2015).

#### Quantum Threat: Quantum computing's advancement has raised serious questions about existing cryptographic algorithms' security, leading to a search for quantum-resistant methods (Shor, 1999; Grover, 1996; Bernhard et al., 2020).

#### Legal and Ethical Landscape: Cryptography is entangled with legal and ethical considerations such as encryption export laws, user privacy, and the balance between national security and individual rights (Denning, 2000; Koops, 2010).

#### Cryptography in Specific Domains:

#### Financial Services: Cryptographic algorithms secure online transactions and protect sensitive financial data (Sullivan, 2000).

#### Healthcare: In healthcare, encryption and hashing ensure patient privacy and data integrity (Anderson, 1996).

#### Cryptocurrencies: Blockchain technology leverages cryptographic principles, most notably in Bitcoin (Nakamoto, 2008).

#### IoT: The Internet of Things (IoT) employs cryptographic methods for device authentication and data protection (Sicari et al., 2015).

#### Challenges and Research Gaps: The complexity of real-world applications demands ongoing research to evaluate cryptographic algorithms' resilience, performance, usability, and impact (Liu & Wang, 2012; Rogaway, 2015).

#### This research aims to empirically assess the effectiveness of both well-established and emerging symmetric and asymmetric cryptographic algorithms through extensive benchmarking and analysis. By developing optimized software frameworks leveraging industry-standard libraries like OpenSSL and BouncyCastle, reproducible experiments can quantify performance metrics including throughput, efficiency, latency and resistance under diverse real-world conditions (Bernstein et al., 2019). Comparing these empirical results against prevailing theoretical security estimates provides greater insight into optimal cryptographic configurations for contemporary applications.

#### As distributed systems and information security needs grow more complex, guidelines for judiciously selecting and tuning cryptographic controls become critical for both confidentiality and efficiency (Barker, 2016). This research intends to inform the design and adoption of cryptosystems that apply rigorous protections in a performant manner by thoroughly examining the most prevalent algorithms available today.

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

#### Purpose:

#### The principal objective of this research report is to provide an exhaustive analysis of various cryptographic algorithms, assessing their features, performance metrics, and applicability in different domains. Given the increasing emphasis on data security in the digital era and the varied cryptographic choices available, there is an imperative need to discern the strengths and vulnerabilities of each algorithm, which can aid both researchers and industry professionals in making informed decisions.

#### Scope:

#### Algorithm Analysis: The study encompasses a wide array of cryptographic algorithms, including both symmetric and asymmetric encryption techniques, as well as hashing functions. This comprehensive approach ensures that readers get a holistic understanding of the cryptographic landscape.

#### Performance Evaluation: Apart from theoretical underpinnings, the research emphasizes empirical assessments. By leveraging a modular software framework, the report benchmarks each algorithm against a set of predefined metrics, gauging their real-world efficiency.

#### Domain-Specific Insights: Recognizing that the efficacy of cryptographic methods can vary based on the application, the report delves into their performance across diverse domains such as finance, healthcare, and IoT. These insights offer a granular view of how different algorithms fare in specific contexts.

#### Ethical and Legal Implications: Beyond the technical facets, the research also touches upon the ethical, legal, and societal ramifications of cryptographic implementations, especially in the face of evolving global norms and regulations concerning data privacy and surveillance.

#### Future-Readiness: With quantum computing on the horizon, the research offers a perspective on the quantum resistance of current cryptographic algorithms and the ongoing efforts in the field to develop post-quantum cryptography.

#### The aim is to quantify the practical performance of algorithms on metrics meaningful to security engineers and researchers, such as:

#### Encryption/decryption throughput

#### Computational efficiency (CPU usage)

#### Memory requirements

#### Latency impacts

#### Key, signature, and hash generation speed

#### By implementing optimized software libraries integrated with hardware accelerators where applicable, the benchmarks reflect realistic usage scenarios and configurations.

#### The extensive tests use representative data sizes ranging from 512 bits to 1GB to analyze how performance scales. Statistical techniques are applied to ensure rigorous benchmarking.

#### The scope is limited to the cryptographic algorithms themselves rather than full protocols. However, benchmarks do account for factors like cipher modes. Analysis aims to determine optimal algorithms and configurations to securely apply cryptography at scale.

#### In essence, this report aims to be a comprehensive reference for both academia and industry, elucidating the intricate tapestry of cryptography in modern times, its challenges, and the road ahead.

#### **1.3 Report Structure**

#### This report is methodically structured to provide readers with a systematic understanding of cryptographic algorithms and their varied dimensions. The following summarizes each section:

#### Introduction (Section 1): Provides the background, purpose, and scope of the research, laying the groundwork for the subsequent discussion.

#### Literature Review (Section 2): Offers a critical review of the existing scholarly work in the field, encompassing an overview of cryptography, symmetric and asymmetric key algorithms, hash functions, and prior benchmarking studies.

#### Research Methodology (Section 3): Details the research design, including the selection of algorithms, software libraries and tools, hardware platforms, performance metrics, and the limitations and assumptions underlying the study.

#### Implementation and Results (Section 4): Presents the experimental setup, detailing the benchmarks for algorithms such as AES, ECC, and RSA, and a comparative analysis of the results.

#### Conclusions (Section 5): Summarizes the findings, provides recommendations and outlines the limitations of the research, and discusses avenues for future work.

#### Ethical, Legal, and Social Issues (Section 6): Examines the broader implications of cryptographic research and practice, with an emphasis on ethical considerations, relevant laws and regulations, and societal impacts.

#### References: A comprehensive list of all the academic sources, standards, and documents referenced throughout the report.

#### Appendices: Additional supporting material, including detailed code listings, supplementary data tables, and extended analysis, if applicable.

#### The structure is designed to guide the reader seamlessly from the fundamental concepts to the nuanced aspects of cryptographic algorithms, ensuring both depth and accessibility for a wide audience, ranging from scholars and practitioners to policymakers.

#### 

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

#### This literature review provides technical background on cryptographic algorithms and summarizes existing research comparing and analyzing the real-world performance of prominent techniques. It aims to contextualize the current study within prior academic work in this field.

#### **2.1 Cryptography Overview**

#### Cryptography underpins systems for secure communication and data protection by transforming information into a secure, encrypted format. Katz and Lindell (2007) define the fundamental goals of cryptography as confidentiality, integrity, authentication and non-repudiation. Cryptographic algorithms employ mathematical techniques to provide these properties.

#### Fundamental Concepts

#### Symmetric vs. Asymmetric Cryptography: Symmetric systems (like DES or AES) utilize a singular key for encryption and decryption, while asymmetric systems (like RSA) use distinct keys for each process (Diffie & Hellman, 1976).

#### Cryptography Algorithms: Over the years, various cryptographic algorithms have been introduced, designed to meet different security needs. Notable ones include RSA, DES, AES, and ECC (Stallings, 2014).

#### Hash Functions: These are algorithms that take an input and return a fixed-size string of bytes. They play a crucial role in ensuring data integrity (Menezes et al., 1996).

#### The two main classes of cryptographic algorithms are symmetric key and asymmetric key. In symmetric algorithms, the same secret key is used to encrypt and decrypt data. This includes ciphers like AES, DES, Blowfish, RC4 and ChaCha20. Asymmetric or public key algorithms use key pairs for encryption and decryption. RSA, ECC, Diffie-Hellman and DSA are prominent public key algorithms. Additionally, cryptographic hash functions like MD5, SHA-1 and SHA-2 generate fixed length message digests (Paar and Pelzl, 2009).

#### Early ciphers used simple Monoalphabetic substitution which was easy to cryptanalyze. The polyalphabetic Vigenère cipher improved security by encrypting with multiple alphabets. The 20th century saw the emergence of mechanical and electromechanical rotor machines like the German Enigma, providing the first practical applications of cryptography (Kahn, 1967).

#### Modern Relevance

#### Today, cryptography underpins many facets of our digital world. From securing financial transactions and preserving user privacy online (Schneier, 2015) to serving as the backbone of blockchain technology and cryptocurrencies, its influence is both broad and profound. Moreover, in an era characterized by data breaches and cybersecurity threats, cryptographic principles are more pertinent than ever (Goldberg, 1997).

#### Evolution of Major Cryptographic Algorithms

#### Symmetric Key Algorithms

#### One of the earliest symmetric ciphers was the Playfair cipher invented in 1854. It was the first to use digraph substitution instead of single letters. Later electromechanical rotor machines like Enigma (1918) allowed more complex polyalphabetic substitution and key changes. The Data Encryption Standard (DES) published in 1977 by IBM under NIST was the first publicly accessible cipher. It uses a Feistel structure on 64-bit blocks with 56-bit keys. DES was eventually broken and obsolete by the 1990s. The Advanced Encryption Standard (AES) was published in 2001 by Daemen and Rijmen as a replacement. It uses substitution-permutation with 128-bit blocks and 128/192/256 bit keys (Daemen and Rijmen, 2013).

#### Asymmetric Key Algorithms

#### Asymmetric cryptography was proposed in the 1970s to enable confidentiality and authentication in public environments. Ralph Merkle patented public key distribution in 1974. The RSA algorithm published in 1977 by Rivest, Shamir and Adleman introduced the first implementation based on factorization difficulty. ECC emerged in 1985 and offered stronger security per bit versus RSA due to using discrete logarithms. NIST standardized elliptic curves for government use by 2000 (Barker and Roginsky, 2015).

#### Hash Functions

#### Early non-cryptographic hashes like Fletcher's checksum (1982) just summed input bits. MD4 invented by Rivest in 1990 was one of the first cryptographic hashes. It evolved into MD5 but was found vulnerable to collisions. SHA-1 was developed in 1995 by the NSA as a strengthened alternative. After attacks emerged on SHA-1, the SHA-2 family was released in 2001 which remains secure (Schneier, 2004).

#### Evolution of Specific Cryptographic Algorithms

#### Symmetric Key Algorithms

#### Data Encryption Standard (DES): Introduced by the National Institute of Standards and Technology (NIST) in 1977, DES was among the first symmetric key algorithms widely adopted. It operated on 64-bit blocks and used a 56-bit key, which later proved to be insecure against brute-force attacks (Biham & Shamir, 1993).

#### Advanced Encryption Standard (AES): As DES's insecurity became apparent, NIST initiated a process to find its replacement, resulting in the selection of AES in 2001. AES offered significant improvements, with key sizes of 128, 192, or 256 bits and block sizes of 128 bits (Daemen & Rijmen, 2002).

#### Asymmetric Key Algorithms

#### RSA Algorithm: Named after its creators Rivest, Shamir, and Adleman, RSA was introduced in 1978 and became one of the first practical public-key cryptosystems. The security of RSA is based on the difficulty of factoring large composite numbers (Rivest et al., 1978).

#### Elliptic Curve Cryptography (ECC): Introduced in the mid-1980s, ECC represents a more efficient approach to public-key cryptography. It relies on the algebraic structure of elliptic curves over finite fields, providing the same level of security as RSA with significantly smaller key sizes (Koblitz, 1987; Miller, 1985).

#### Hash Functions

#### MD5: Developed in 1991, the MD5 hash function became widely used but was later found to have vulnerabilities that could allow collision attacks (Wang et al., 2004).

#### SHA-1 and SHA-2: The Secure Hash Algorithms were developed by the National Security Agency (NSA). While SHA-1 faced similar collision weaknesses as MD5, SHA-2 (introduced in 2001) remains secure and is an integral part of modern security protocols (NIST, 2015).

#### The evolution of cryptographic algorithms reflects a constant race between developing robust security measures and overcoming their inherent vulnerabilities. Each new generation of algorithms attempts to rectify the shortcomings of its predecessors, adapting to the rapidly changing landscape of computational capabilities and emerging threats.

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

#### Symmetric algorithms, also known as secret key algorithms, use the same cryptographic key for encrypting and decrypting data. Prominent examples of symmetric ciphers include AES, DES, 3DES, Blowfish, RC4, and ChaCha20 (Katz & Lindell, 2007). These algorithms are known for high speed and low computational complexity, making them suitable for bulk data encryption and applications like storage, networking, and embedded systems security (Singh & Supriya, 2020).

#### DES was developed in the 1970s by IBM and standardized by NIST until it was deprecated due to a small 56-bit key. It uses a Feistel cipher structure on 64-bit blocks. Weaknesses in DES against brute force attacks prompted replacement by 3DES and eventually the AES standard (Biham & Shamir, 1991). AES was selected through a 5 year NIST competition and uses an SPN structure on 128-bit blocks with 128, 192 or 256 bit keys. It provides strong resistance against linear and differential cryptanalysis attacks (Daemen & Rijmen, 2013).

#### Stream ciphers like RC4 and ChaCha20 generate a pseudorandom keystream to XOR with the plaintext instead of operating on fixed blocks. RC4 designed in 1987 by Rivest was widely used in protocols like WEP and TLS but shown to have biases enabling related-key attacks (Mantin & Shamir, 2001). ChaCha20 created in 2008 improves on RC4 and Salsa20 with better diffusion, a 64-bit nonce, and supports parallelization (Bernstein, 2008).

#### The Genesis: Data Encryption Standard (DES)

#### The Data Encryption Standard (DES) became the pioneering standard in the realm of symmetric cryptography. Adopted by the U.S. National Institute of Standards and Technology (NIST) in 1977, DES operated on 64-bit blocks with a 56-bit key (FIPS, 1977). Despite its wide acceptance, the algorithm's vulnerability to brute-force attacks due to its limited key length became evident (Biham & Shamir, 1993).

#### The Advent of Advanced Encryption Standard (AES)

#### With growing concerns over DES's susceptibility, NIST initiated a competition for its successor. This culminated in the selection of the Rijndael cipher, subsequently termed the Advanced Encryption Standard (AES). The AES architecture operates on block sizes of 128 bits and offers flexible key lengths of 128, 192, or 256 bits (Daemen & Rijmen, 2002). Given its robustness against known cryptographic attack vectors, AES has become the de facto standard for diverse security needs.

#### Triple DES: An Intermediate Measure

#### As a transitional response to DES's weakening security, Triple DES (3DES) emerged. This algorithm applied the DES encryption process thrice, thus amplifying its security. However, it also brought along increased computational overhead (Schneier, 1996). While considered more secure than its predecessor, 3DES eventually paved the way for algorithms with intrinsically higher security designs, such as AES.

#### Blowfish and Twofish: Alternatives to the Standards

#### Designed by Bruce Schneier in 1993, Blowfish became popular owing to its speed, simplicity, and openness (Schneier, 1993). Operating on 64-bit blocks and key lengths ranging up to 448 bits, Blowfish found its use in numerous applications. Its successor, Twofish, further extended the block size to 128 bits and maintained flexibility in key lengths (Schneier et al., 1998). Though not as ubiquitously adopted as AES, both algorithms have earned respect in cryptographic circles.

#### In the wake of evolving computational capabilities, particularly the advent of quantum computing, there's a renewed focus on ensuring the long-term viability of symmetric key algorithms. Nevertheless, as of the present day, AES dominates the landscape, underpinned by its consistent performance and resilience against cryptanalytic attacks (Bernstein, 2005).

#### While the journey of symmetric key algorithms reveals a tale of consistent evolution and adaptation, the essence remains: ensuring secure, confidential, and integral communication in an ever-digitizing world.

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

#### Asymmetric or public key algorithms use key pairs consisting of a public key for encryption/verification and private key for decryption/signing. This allows secure communication without prior key exchange. Prominent public key algorithms include RSA, ECC, ElGamal and DSA (Paar & Pelzl, 2009).

#### RSA was the first practical public-key cryptosystem, published in 1977 by Rivest, Shamir, and Adleman. It relies on the integer factorization hard problem. Key generation involves selecting two large primes and computing their product. Encryption and signatures use modular exponentiation with the public key, while the private key is needed to decrypt (Rivest et al., 1978). Its security stems from the difficulty of factoring large prime numbers. Key generation involves selecting two large random primes p and q, computing their product n, and finding exponents e and d such that ed ≡ 1 (mod φ(n)). The public key is (n, e) and private key is (n, d). Encryption and signature verification use modular exponentiation with the public key, while the private key is needed for decryption and signing (Rivest et al., 1978).

#### RSA key sizes have grown over time to maintain security against advances in factorization algorithms and computing power. Key lengths started at 512 bits in the 1970s, increasing to 1024 bits in the 1990s and 2048+ bits today. Longer keys substantially increase computational costs. Various padding schemes like OAEP and PSS help improve security. RSA is useful for encryption, authentication, and secure communication but inefficient for large data.

#### ECC (Elliptic Curve Cryptography) was proposed in 1985 and utilizes the discrete logarithm problem over elliptic curves. It offers equivalent security to RSA at much smaller key sizes. Computations use point addition and doubling on the curve based on modular arithmetic. ECC provides an efficient alternative to RSA for encryption, signatures and key exchange (Koblitz, 1987). It provides equivalent security to RSA at much smaller key sizes due to the discrete logarithm problem over elliptic curves. A 256-bit ECC key offers approximately the same security as a 3072-bit RSA key. Computations use point addition and doubling on the curve based on modular arithmetic operations. ECC is well-suited for constrained environments and provides an efficient alternative to RSA for encryption, signatures, and key exchange (Hankerson et al., 2004).

#### NIST has standardized elliptic curves over finite fields for government applications. SECP256r1 is a common 256-bit curve used in Bitcoin and other cryptosystems. ECC algorithms include ECDSA for digital signatures and ECDH for key agreement. Implementations must ensure secure parameter selection and avoid side-channel leaks that could enable attacks on certain curves.

#### RSA: Setting the Benchmark

#### The RSA algorithm, proposed by Rivest, Shamir, and Adleman in 1978, is arguably the most recognized and widely used asymmetric encryption method (Rivest et al., 1978). It relies on the mathematical complexity of factoring large prime numbers, which provides the security foundation. Over the decades, RSA's dominance has been evident, but it's not without criticisms, notably due to its computational intensity, especially with key lengths deemed safe against modern computing capabilities.

#### Elliptic Curve Cryptography (ECC): A Leap Forward

#### While RSA remained dominant, the search for more computationally efficient algorithms led to Elliptic Curve Cryptography (ECC). Proposed in the mid-1980s, ECC provides similar cryptographic strength as RSA but with much shorter key lengths, making it more efficient, especially for devices with constrained resources (Koblitz, 1987; Miller, 1986). Today, ECC is seeing broader adoption, particularly in mobile and IoT devices.

#### Diffie-Hellman (DH) and Its Variants

#### The Diffie-Hellman key exchange, pioneered by Whitfield Diffie and Martin Hellman in 1976, predates RSA by a short span and introduced a novel method for securely exchanging cryptographic keys over a public channel (Diffie & Hellman, 1976). Though not an encryption algorithm per se, DH's concept of key agreement laid the groundwork for subsequent public-key systems. Its Elliptic Curve variant (ECDH) combines the strengths of ECC and DH, providing secure key exchanges with reduced computational overhead.

#### Post-Quantum Cryptography: The Next Frontier

#### With quantum computing on the horizon, concerns over the potential vulnerabilities of existing public-key algorithms have emerged. Quantum computers could compromise the hard mathematical problems underpinning these algorithms. Thus, the cryptographic community has been exploring new public-key methods, or post-quantum algorithms, that remain secure even in a quantum-computational world (Bernstein & Lange, 2017).

#### Asymmetric key algorithms have experienced a dynamic evolution since their inception. From the groundbreaking ideas of Diffie-Hellman and RSA to the efficiency-focused innovations of ECC and the forward-looking designs of post-quantum cryptography, this field has been a testament to the relentless pursuit of security in an ever-evolving technological landscape.

#### **2.4 Hash Functions**

#### Cryptographic hash functions take an input message of arbitrary length and generate a fixed length digest by compressing the data. Hash functions should exhibit computational efficiency, preimage resistance, second preimage resistance and collision resistance (Rogaway & Shrimpton, 2004).

#### Hash functions play an essential role in cryptography by converting an arbitrary length of data into a fixed-size hash value, which can be used for various purposes, such as data integrity verification, digital signatures, and more. This literature review discusses the prominent hash functions, their applications, and the challenges faced in this critical area of cryptography.

#### Prominent cryptographic hash functions include MD5, SHA-1, SHA-2, SHA-3 and BLAKE2. MD5 was developed by Rivest in 1991 to improve upon MD4, increasing the digest size to 128 bits. However, security flaws including collision attacks emerged, prompting deprecation. SHA-1 was introduced in 1995 by the NSA as an alternative to MD5. It produces a 160-bit hash but has also shown vulnerabilities to analytic attacks (Schneier, 2004).

#### The SHA-2 family released in 2001 comprises hashes with digest sizes of 256, 384 and 512 bits. SHA-256 remains common for applications like digital signatures and blockchains due to its security and efficiency. SHA-3, based on the Keccak algorithm, won the NIST hash competition in 2012 after weaknesses in SHA-2. BLAKE2 (2012) improves on SHA-3 for speed on modern platforms (Aumasson et al., 2013).

#### Hash functions are the foundation for digital signatures, message authentication codes (MACs), key derivation and random number generation. Their security and performance is vital to overall cryptosystem strength.

#### Prominent hash functions include:

#### MD5 - Produces 128-bit digests using a 64-element compression function. Designed for speed but Collision attacks emerged by 2005, prompting deprecation. Still used for error checking but not security (Klima, 2005).

#### SHA-1 - Developed by the NSA in 1995 as an improvement over MD5, outputs 160-bit digest. Uses 80-step compression function. Vulnerable to theoretical attacks but no practical breaks yet. Deprecated by NIST but still common (Schneier, 2004).

#### SHA-256 - SHA-2 family hash with 256-bit output. Uses a Davies–Meyer compression function and processes 512-bit message blocks. No successful attacks better than brute force. Widely used for signatures and commitments (Rogaway & Shrimpton, 2004).

#### SHA-3 - Published in 2012 after NIST hash competition. Built on sponge construction and utilizes permutation Keccak-f. Targets security against attacks on prior SHA versions. Not yet widely deployed (Bertoni et al., 2013).

#### BLAKE2 - Improves on SHA-3 with optimizations for speed and parallelism on modern platforms. Uses tree mode for multi-threaded hashing. Popular for blockchains and cryptocurrencies (Aumasson et al., 2013).

#### Early Developments: MD5 and SHA-1

#### Among the early cryptographic hash functions, MD5 (Message Digest Algorithm 5) and SHA-1 (Secure Hash Algorithm 1) were widely adopted. Rivest designed MD5 in 1991 as an improvement over earlier versions (Rivest, 1992). Though widely used for years, vulnerabilities in collision resistance eventually tarnished its reputation.

#### SHA-1, published by the National Institute of Standards and Technology (NIST) in 1993, soon replaced MD5 in many applications. However, by the mid-2000s, researchers had identified weaknesses in SHA-1 as well, leading to a gradual decline in its usage (Wang et al., 2005).

#### SHA-2: Addressing the Weaknesses

#### To overcome the shortcomings of SHA-1, NIST introduced the SHA-2 family in 2001. Comprising different hash lengths (SHA-224, SHA-256, SHA-384, SHA-512), SHA-2 addressed previous weaknesses, and for a considerable period, it has remained a standard in the industry (Dworkin, 2015).

#### Keccak and SHA-3

#### The vulnerabilities in SHA-1 and other hash functions led NIST to launch a public competition for the next-generation hashing standard. The winning algorithm, Keccak, became the foundation for SHA-3, officially released in 2015 (Bertoni et al., 2011). Its unique sponge construction marked a departure from previous design principles, adding to the robustness of cryptographic hashing.

#### Cryptographic Hash Functions in Blockchain

#### Hash functions have found profound applications in blockchain technology, where they are used to maintain integrity and structure. SHA-256, for example, is central to the Bitcoin blockchain's operation (Nakamoto, 2008).

#### Challenges and the Quantum Threat

#### Despite substantial progress, cryptographic hash functions face challenges in ensuring long-term security. The advent of quantum computing might pose risks to existing hash functions, spurring research into post-quantum hash functions (Bernstein et al., 2017).

#### Cryptographic hash functions have evolved from the earlier days of MD5 and SHA-1 to the more resilient SHA-2 and SHA-3. Yet, with technology's perpetual advance, the cryptographic community must continue to innovate and prepare for potential future challenges, such as the quantum threat. The strength of hash functions underlies digital signature schemes and MACs for authentication. Keyed algorithms like HMAC extend hashes by hashing a key with the input. Random oracle models are important for proving hash security.

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

#### Benchmarking studies form a crucial aspect of cryptographic research, offering a pragmatic approach to understanding the efficacy of cryptographic algorithms in real-world scenarios. This literature review encapsulates the seminal works and emerging trends in the benchmarking of cryptographic algorithms, setting the stage for the evaluation of cryptographic systems' performance, security, and efficiency. Numerous research studies have aimed to benchmark and analyze the performance of cryptographic algorithms. This section summarizes key findings from relevant literature.

#### Gupta et al. (2018) benchmarked AES, DES, and Triple DES across varying key sizes, data sizes, and modes of operation. They found throughput increased proportionally with data size, and AES significantly outperformed DES and 3DES in encryption speed. Güneysu et al. (2008) specifically analyzed ultra-low latency implementations of AES, implementing the cipher in hardware and optimizing critical paths.

#### For public key cryptography, Bernstein et al. (2013) systematically compared RSA and ECC performance. Their results showed ECC operations completed 2-5x faster than RSA at equivalent security levels. Jawurek et al. (2012) found RSA decryption time scales superlinearly with key size, with PKCS#1 padding slowing performance. Several analyses have optimized and accelerated RSA on multi-core CPUs and GPGPUs (Harrison et al., 2010).

#### Hash function benchmarks by Khandaker et al. (2018) demonstrated SHA-256 throughput around 2x faster than SHA-3 and SHA-512 on short messages. BLAKE2 outperformed MD5 and SHA-1 as older hashes lack acceleration. Gan et al. (2018) profiled HMAC on varied hash functions, showing tuning of parameters like block size optimizes MAC performance.

#### Early Benchmarking Studies

#### During the late 1980s and early 1990s, as computers began to play a more integrated role in everyday tasks, the efficiency of cryptographic algorithms took center stage. Lenstra and Verheul (2000) offered one of the first systematic studies, assessing the relative efficiency of both symmetric and asymmetric algorithms in various computing environments. They emphasized the need for benchmarking as the foundation for making informed choices about cryptographic algorithms.

#### Comparisons Between Symmetric Algorithms

#### A series of studies led by Schneier and others during the late 1990s focused on symmetric algorithms like Blowfish, DES, and later AES. Their studies predominantly utilized the then-popular crypto libraries, aiming to demonstrate the superiority of some algorithms over others in specific use cases (Schneier, 1996).

#### Asymmetric Algorithms: Efficiency and Key Lengths

#### Menezes and Van Oorschot (1997) published a landmark study benchmarking RSA, ElGamal, and ECC, highlighting their relative merits in terms of computational efficiency. One of the significant findings from this period was the assertion that longer key lengths in asymmetric algorithms did not necessarily translate into better security, sparking subsequent research into optimal key lengths.

#### Benchmarking Post-Quantum Algorithms

#### With the onset of the 21st century and the looming potential of quantum computers, there's been a distinct shift towards benchmarking post-quantum algorithms. Bernstein et al. (2017) provided a comprehensive assessment of lattice-based, hash-based, and multivariate polynomial algorithms, showcasing their resilience against quantum adversaries.

#### Comparative Analysis Using Real-World Systems

#### The advent of cloud computing and IoT has led to an upsurge in studies that benchmark cryptographic algorithms on non-traditional platforms. Aumasson and Bernstein (2012) conducted a study evaluating cryptographic operations on ARM processors, typical of many smart devices.

#### The Role of Open-Source Benchmarking Suites

#### To facilitate consistent and reproducible benchmarking studies, several open-source suites have emerged, such as SUPERCOP (Bernstein, 2005). These suites offer standardized tests for a variety of algorithms, enhancing the comparability of results across different studies.

#### Benchmarking studies have consistently played a pivotal role in shaping the understanding and adoption of cryptographic algorithms. They offer a bridge between theoretical security and practical efficacy, ensuring that cryptographic practices evolve in tandem with technological advances and emergent threats.

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

#### This section describes the experimental framework, tools, metrics, and procedures used for benchmarking cryptographic algorithms in this study.

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

#### Algorithms are selected to cover a diverse and representative set of symmetric ciphers, asymmetric ciphers, hash functions, and other cryptographic primitives. Both established standards and emerging algorithms are included based on prevalence in literature, software, and real-world cryptosystems.

#### The symmetric ciphers selected are AES, DES, 3DES, Blowfish, RC4, and ChaCha20. These include historical ciphers like DES still in use today as well as modern standards like AES and promising candidates like ChaCha20.

#### Asymmetric ciphers include RSA, ECC, ECDH, and ElGamal. RSA remains the most widely used asymmetric algorithm while ECC offers performance advantages. ECDH is included for key exchange.

#### Hash functions consist of MD5, SHA-1, SHA-2, SHA-3, and BLAKE2. These span decades of hash research and standards.

#### Additionally, HMAC and CBC-MAC are included as message authentication algorithms along with Generators for pseudo-random number generation.

#### For each algorithm, standard parameters are configured such as 128/256 bit keys for AES, 2048/4096 bit keys for RSA, and common elliptic curves. Different block modes are evaluated where applicable.

#### The selection of cryptographic algorithms for this research is a critical step, determining the breadth and depth of the analysis. It involves a careful examination of various algorithms available, considering their relevance, importance, and applicability in different domains. Below is the detailed methodology for the selection of algorithms.

#### 3.1.1 Criteria for Selection

#### The criteria for selecting algorithms are based on the following key considerations:

#### Relevance: The algorithm must be relevant to current cryptographic practices and applications.

#### Popularity: Preference is given to widely-used algorithms in industry and academia.

#### Security Level: Algorithms with varying degrees of security are considered to analyze a broad spectrum of cryptographic needs.

#### Algorithm Type: Includes symmetric key, asymmetric key, and hash functions, to offer a comprehensive view of the cryptographic landscape.

#### Availability: Algorithms with accessible libraries and implementations are preferred for practical evaluation.

#### 3.1.2 Categories of Algorithms

#### The selected algorithms are categorized into three main classes:

#### Symmetric Key Algorithms: These are algorithms where the same key is used for both encryption and decryption.

#### Examples: Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), Blowfish.

#### Asymmetric Key Algorithms: These utilize two separate keys, one public and one private, for encryption and decryption.

#### Examples: Rivest–Shamir–Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie–Hellman key exchange.

#### Hash Functions: These are mathematical functions that convert an input into a fixed-length string of bytes, typically a hash value.

#### Examples: Secure Hash Algorithm (SHA-256), Message Digest Algorithm 5 (MD5), SHA-3.

#### 3.1.3 Justification of Selection

#### For each algorithm selected, a justification is provided, explaining the rationale behind the choice. For example:

#### AES: Selected for its status as a global standard, robust security features, and widespread adoption in various industries.

#### ECC: Chosen for its efficiency in providing the same level of security as RSA but with shorter key lengths, making it valuable for constrained devices.

#### 3.1.4 Exclusion Criteria

#### Any algorithms that do not meet the predefined criteria are explicitly excluded, with reasons provided. This may include outdated algorithms, algorithms with known vulnerabilities, or those lacking practical relevance.

#### 3.1.5 Summary

#### The selection of algorithms is carried out meticulously, keeping in mind the study's objectives and the broader cryptographic context. The inclusion of diverse algorithm types, carefully justified based on clearly defined criteria, ensures a well-rounded and comprehensive analysis.

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

#### The implementation and testing of cryptographic algorithms require the use of specific software libraries and tools. These provide the necessary functionalities to carry out the cryptographic operations and measure performance metrics accurately. Below is a detailed description of the software libraries and tools used in this research.

#### 3.2.1 Programming Languages

#### Python: Widely used for its simplicity and vast libraries. It's suitable for scripting and creating prototypes.

#### C++: Chosen for performance testing due to its efficiency and close-to-hardware characteristics.

#### 3.2.2 Cryptographic Libraries

#### OpenSSL: A robust, full-featured open-source toolkit that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. It provides cryptographic libraries for various algorithms.

#### Crypto++: A free C++ class library of cryptographic schemes.

#### PyCrypto: A collection of cryptographic algorithms and protocols for Python.

#### 3.2.3 Performance Analysis Tools

#### Valgrind: Used to profile the algorithms and to detect memory leaks, bottlenecks.

#### gprof: GNU profiler used for performance analysis in C++.

#### matplotlib: A Python plotting library used to visualize the performance results.

#### 3.2.4 Development and Testing Environments

#### Visual Studio Code: An open-source code editor used for development.

#### Jupyter Notebooks: An open-source web application that allows the creation and sharing of documents containing live code, equations, and visualizations.

#### 3.2.5 Version Control

#### Git: Used to manage code versions and collaborate efficiently with other researchers or team members.

#### 3.2.6 Justification for Tools Selection

#### The selection of these tools and libraries is based on their relevance, efficiency, support community, and compatibility with the research requirements. For example:

#### OpenSSL: Chosen for its extensive set of cryptographic functions and widely-accepted industry standards.

#### C++: Preferred for performance testing due to its ability to execute code faster, which is essential for benchmarking studies.

#### 3.2.7 Summary

#### The combination of the aforementioned software libraries and tools enables comprehensive analysis and evaluation of cryptographic algorithms. The use of open-source tools and libraries ensures transparency and replicability of the study. The selected tools align with the research's need for performance, ease of use, and flexibility in implementation and analysis.

#### **3.3 Hardware Platforms**

#### In the research study, different hardware platforms were used to evaluate and benchmark the performance of cryptographic algorithms. The platforms include both personal computing devices and modern mobile devices to ensure a diverse range of real-world applications and scenarios.

#### 3.3.1 Personal Computers (Desktop or Laptop)

#### For personal computing platforms, the following configuration was used:

#### - \*\*Processor\*\*: 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz, 2.42 GHz.

#### - \*\*Memory\*\*: 8.00 GB RAM (7.79 GB usable).

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

#### - \*\*Other Specifications\*\*: Specifics on storage, GPU, etc., could be included based on the requirements of the cryptographic evaluations.

#### #### 3.3.2 Mobile Devices

#### The mobile platform was included to represent scenarios where cryptographic algorithms are employed in handheld devices. Specifications are as follows:

#### - \*\*Model\*\*: [Specify Model Name].

#### - \*\*Operating System\*\*: Android 12, upgradable to Android 13.

#### - \*\*Processor\*\*: Google Tensor (5 nm) Octa-core CPU.

#### - \*\*Memory\*\*: Options of 128GB 8GB RAM, 256GB 8GB RAM; UFS 3.1.

#### - \*\*Display\*\*: AMOLED, 90Hz, HDR10+; 6.4 inches.

#### - \*\*Camera\*\*: Dual 50 MP and 12 MP rear; 8 MP front.

#### - \*\*Battery\*\*: Li-Ion 4614 mAh, non-removable, 50% in 30 min charging.

#### - \*\*Additional Features\*\*: IP68 dust/water-resistant, fingerprint sensor, Wi-Fi 802.11 a/b/g/n/ac/6e, Bluetooth 5.2, USB Type-C 3.1, etc.

#### This combination of platforms allows for a broad analysis of cryptographic algorithms across various hardware settings and is consistent with contemporary usage in both personal and professional domains.

#### **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**

#### Appendix A: Additional Data on Cryptographic Algorithms

#### A.1 Raw Data for AES Benchmarks

#### A.2 Raw Data for ECC Benchmarks

#### A.3 Raw Data for RSA Benchmarks

#### Appendix B: Code Snippets

#### B.1 Python Code for AES Encryption and Decryption

#### B.2 Python Code for ECC Key Generation and Encryption

#### B.3 Python Code for RSA Key Generation and Encryption

#### Appendix C: Supplemental Tables and Figures

#### C.1 Table: Detailed Results of AES Benchmarks

#### C.2 Figure: Histogram of ECC Benchmark Results

#### C.3 Table: Extended Comparative Analysis of Cryptographic Algorithms

#### Appendix D: Additional Analysis

#### D.1 Security Considerations for Different Key Lengths

#### D.2 Performance Impact of Algorithm Implementation Choices

#### D.3 Detailed Analysis of Hash Functions Performance

#### Appendix E: Additional Methodology Details

#### E.1 Details on Hardware Platform Setup

#### E.2 Explanation of Software Libraries and Tools Used

#### E.3 Further Discussion on Performance Metrics