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.