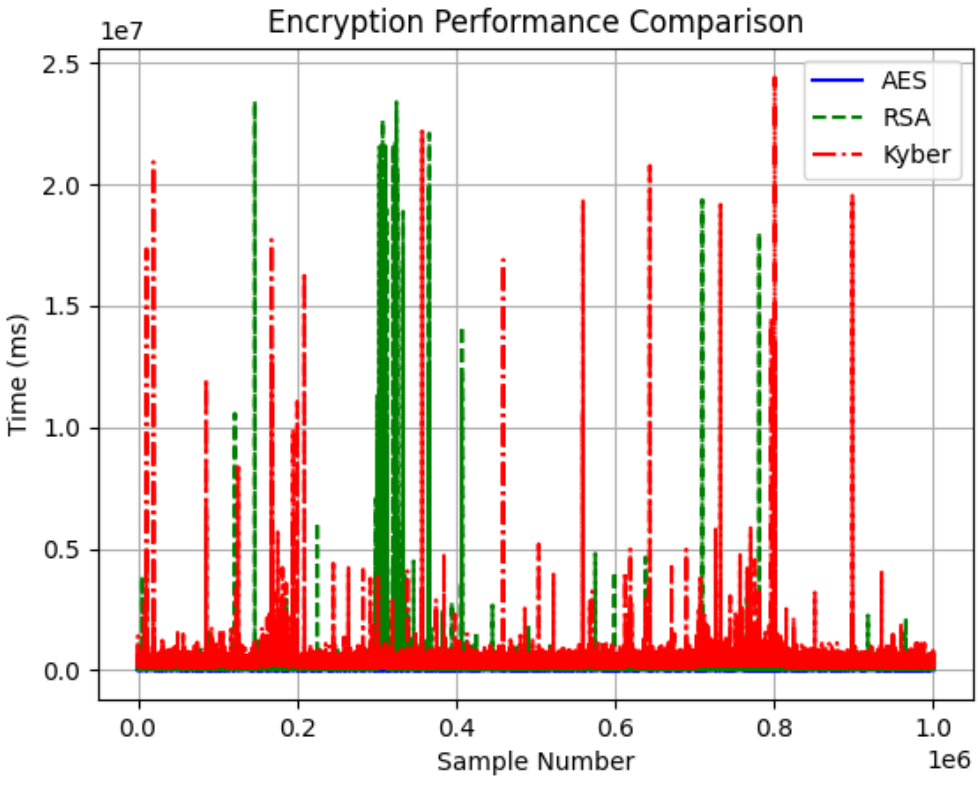
LAB 1 REPORT: Lab 1 - Basic Cryptography - AES, RSA, and Kyber

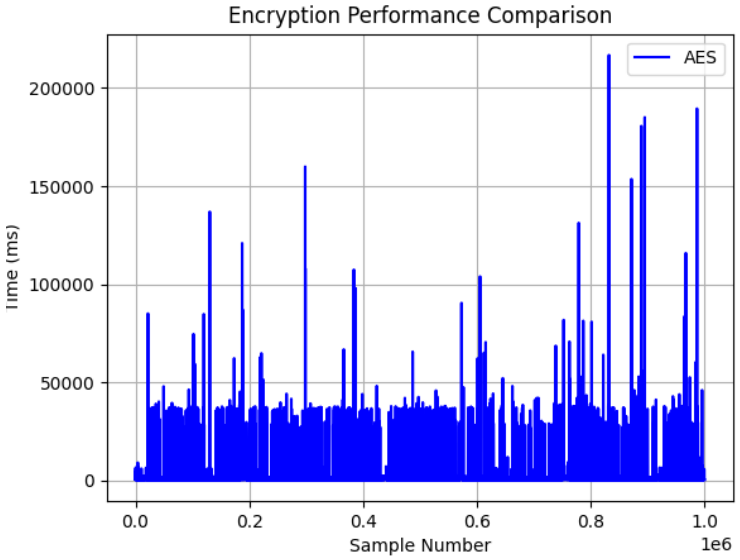
Name: Germain Mucyo, 002301781 (NUID)
Email: mucyo.g@northeastern.edu

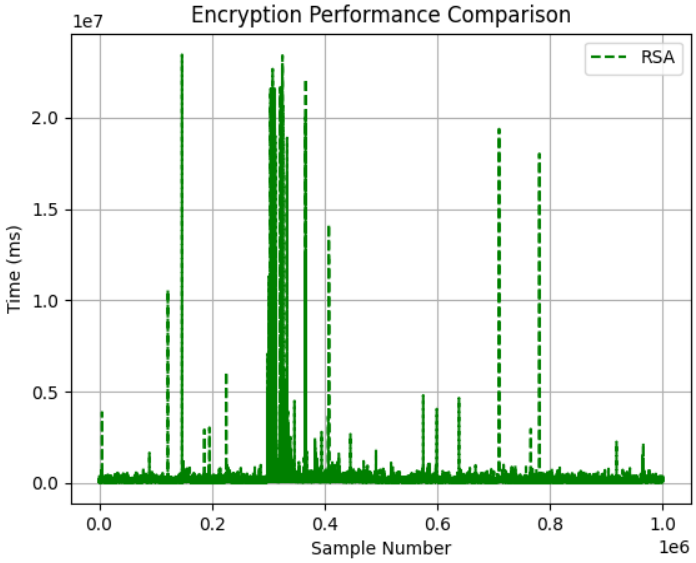
INTRODUCTION

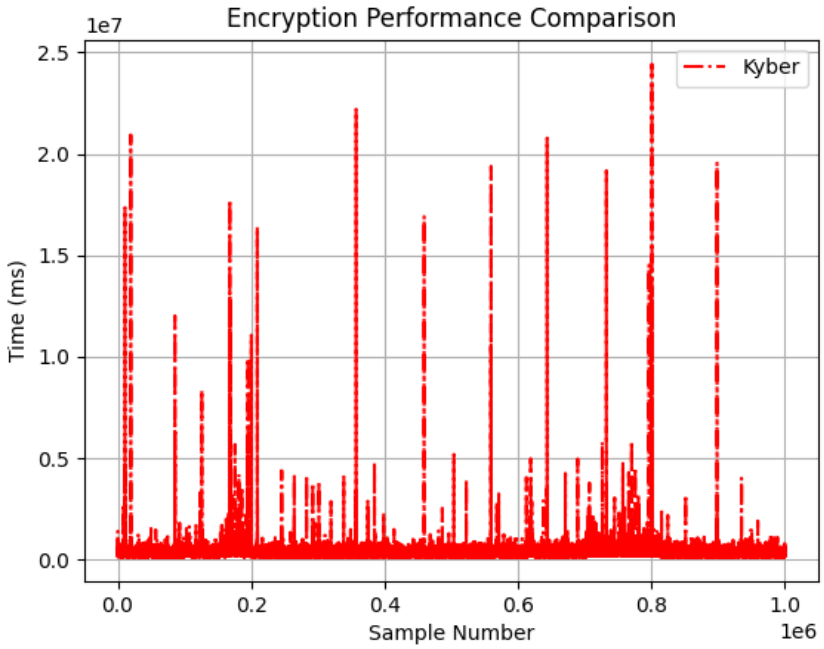
This document is organized into three main parts that reflect my experience and understanding of Modules 1, 2, and 3 of the lab. The first part focuses on Module 1, presenting plots that illustrate the timing distribution for AES, RSA, and Kyber functions, along with a comparative analysis of their performance. The second part provides answers to the questions related to Modules 1 and 2, showcasing my comprehension of the concepts explored. Finally, the third part I generated the secure message that emphasizes my understanding of secure communication between the client and server, with codes (Look in codes folder) detailing the implementation of RSA and AES encryption and decryption algorithms.

Timing distribution Plots for AES, RSA, and Kyber functions









Question 1.

How much slower is RSA/Kyber than AES?

AES plot presents a clearer picture of AES performance, specifying that most AES encryption times are below 100,000 CPU cycles, with many samples even below 50,000. In contrast, RSA demonstrates considerably slower performance, with encryption times frequently exceeding 10,000,000 CPU cycles. Considering that Kyber is faster than RSA as the picture shows.

Overall, in terms of performance, RSA is approximately 10 to 100 times slower than AES, while Kyber is around 10 times slower than AES but significantly faster than RSA.

Scenarios RSA, AES, and Kyber are mainly used for:

AES-128 excels in high-speed data encryption, such as in TLS for web communications, also in cloud storage and database encryption.

RSA is used mostly in digital signature and secure key exchange. Because of its asymmetric nature, RSA is particularly useful in scenarios where secure communication needs to be established between parties that do not share a common key.

Kyber512 is emerging as a crucial player in post-quantum cryptography, providing security against the potential risks posed by future quantum computing advancements. Kyber can be applied in secure key exchange protocols, like RSA, but offers the advantage of being more efficient against quantum threats.

Why would someone want to use Kyber rather than RSA

As the threat landscape evolves, especially with advancements in quantum computing, Kyber presents itself as a robust and forward-looking alternative to traditional cryptographic algorithms like RSA. In terms of speed, Kyber generally offers better performance than RSA in terms of encryption and decryption speed (Refer to Plots above). Also, most studies/papers I was reading states that choosing a post-quantum algorithm like Kyber positions organizations to better protect sensitive data in a rapidly changing technological landscape.

Question 2/ Module 2.

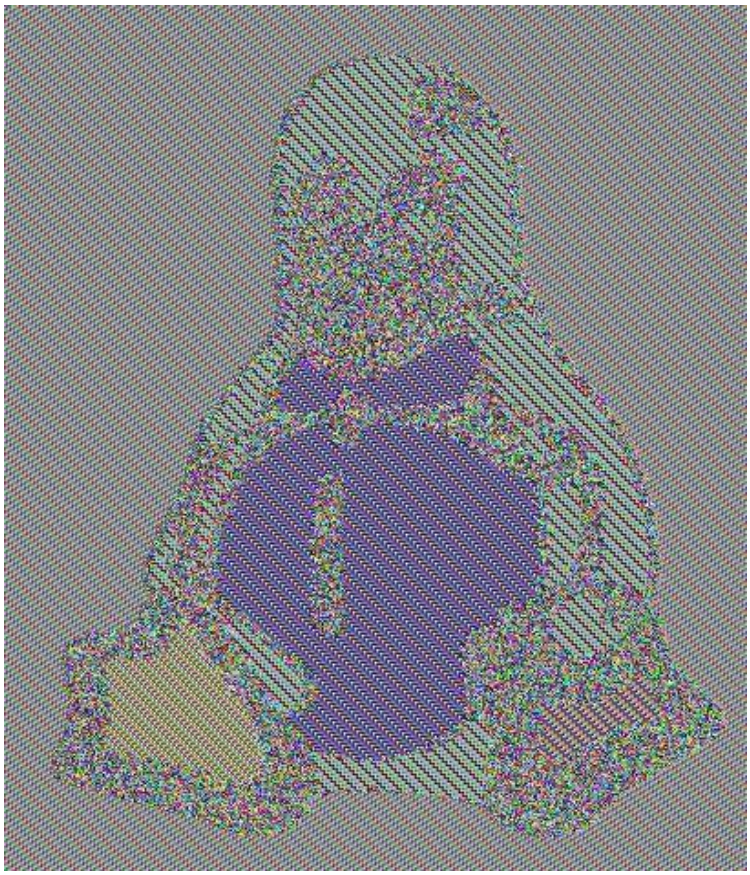


Figure 2 ECB Mode image

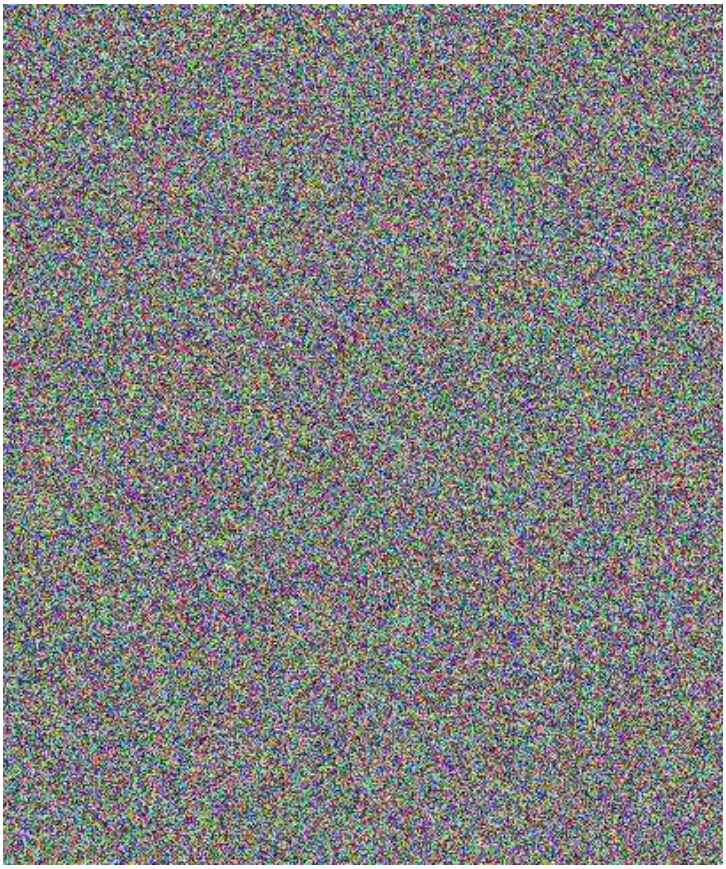


Figure 1 CBC mode image

Question 2:

ECB Mode: Visible Patterns: The structure of the original image is likely still visible. In terms of Security Implication This mode is not secure for images (or any data with repeating patterns) because it does not effectively hide the original content. Anyone looking at the it can easily infer the basic layout of the image, even though the data is encrypted.

CBC Mode: No Visible Patterns which gives it the Security Advantage. Hence it is much more secure than ECB for image encryption because it hides the structure of the image. This makes it much harder to infer the original content of the image from the encrypted version.

Module 3: Secret Message: 9a 54 e0 9b 2c 9f 94 8b ad 1a 97 d0 70 a8 da 14

Reference:

Stinson, D. R., & Vanstone, S. A. (2005). Cryptography: Theory and Practice (3rd ed.). CRC Press.

Katz, J., & Lindell, Y. (2014). Introduction to Modern Cryptography: Principles and Protocols (2nd ed.). Chapman and Hall/CRC.

Daemen, J., & Rijmen, V. (2002). AES: The Advanced Encryption Standard. In The Block Cipher Companion (pp. 77-105). Wiley.

Hoffstein, J., Pipher, J., & Silverman, J. (2017). An Introduction to Post-Quantum Cryptography. Advances in Cryptology – ASIACRYPT 2017. Springer. https://doi.org/10.1007/978-3-319-70600-2_9

Koblitz, N. (1987). Elliptic Curve Cryptosystems. Mathematics of Computation, 48(177), 203-209. https://doi.org/10.1090/S0025-5718-1987-08722-3