Faculty of Computers
& Artificial Intelligence

Benha University

High-Speed Encryption Algorithm Based on Polynomial Roots

A Senior Project Submitted In Partial Fulfillment Of The Requirements For The Degree Of Bachelor Of Computers And Artificial Intelligence.

Scientific Computing Department

Project Team

1. Mohamed Ahmed Elsayed Emary
2. Abdelfattah Zakaria Abdelfattah Morsy
3. Mohamed Abdelfattah Ahmed Abdelfattah
4. Sara Reda Abdallah Elsheikh
5. Dalia Abdallah Mohamed Mahmoud
6. Shrouk Elsayed Mohamed Abdelmoneim

Under Supervision of :

Dr.El-sayed Badr

Benha, June 2024

J U N E – 2 0 2 4

Acknowledgement

We would like to express our sincere gratitude to our project supervisor, Dr. Sayed Badr, for his invaluable guidance and support throughout the completion of our graduation project. His expertise and insightful feedback were instrumental in shaping our research and refining our approach. We are particularly grateful for his willingness to offer constructive criticism, which challenged us to think critically and improve the quality of our work.

Furthermore, Dr. Badr generously provided us with essential resources that facilitated our research. His encouragement and mentorship played a significant role in motivating us to persevere through challenges and achieve our goals. We are deeply indebted to Dr. Badr for his dedication and support, which have significantly contributed to the success of our graduation project.

Declaration

We hereby certify that this material, which we now submit for assessment on the program of study leading to the award of Bachelor of Computers and Artificial Intelligence in (High-Speed Encryption Algorithm Based on Polynomial Roots) is entirely our own work, that we have exercised reasonable care to ensure that the work is original, and does not to the best of our knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of our work.

Signed: _____

Signed: _____

Signed: _____

Signed: _____

Signed: _____

Signed: _____

June 24, 2024

Abstract

Cryptographic algorithms are pivotal to protecting sensitive data in the digital age, but traditional symmetric encryption methods often face challenges such as computational complexity and slowness. In response, our project presents a novel, pioneering polynomial interpolation-based encryption algorithm designed to boost encryption and decryption speeds. This innovative approach uses polynomials derived from secret keys, employing a secant root-finding method that has proven superior in terms of number of iterations, CPU time, and function value to find the root of the polynomial.

By encrypting messages to ciphertext roots and efficiently decrypting them back to plaintext, our algorithm shows significant performance gains over AES. Furthermore, we have implemented our algorithm in a secure messaging web application called InTouch. The InTouch system ensures end-to-end encryption, where only the sender can encrypt messages before sending them, and only the intended recipient can decrypt and view them using the shared key. This integration not only highlights the efficiency of the algorithm but also emphasizes its practicality in securing communications across different platforms. By leveraging polynomial interpolation and optimizing root-finding operations, our project provides a cryptographic solution that excels in both efficiency and security. This advance holds the potential to facilitate widespread adoption of strong encryption in communications networks