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