Zachary Anderson

Daniel Yoon

CS 4600-1

A Python Implementation of the Cramer-Shoup Algorithm for Cryptographically Secure Messaging

Abstract: The Diffie-Hellman key exchange, while effective, is vulnerable to different attacks that rely on how unfeasible it is to determine the private key of a key exchange. The Cramer-Shoup algorithm is cryptographically secure, practical to compute, and is not vulnerable to the issues that the Diffie-Hellman algorithm has. In this report, we demonstrate an implementation of the Cramer-Shoup algorithm in Python and compare it to the Diffie-Hellman algorithm.

Introduction: