Using C++ to Code the Baby-Step Giant-Step Decryption Algorithm for RSA and Elliptic Curve Cryptography

Flynn, Sofia (School: Georgetown Visitation Preparatory School)

The primary purpose of this project was to create a C++ program complete with a graphical user interface capable of calculating private information in both the RSA cryptosystem and the Elliptic Curve Cryptography scheme using the meet-in-the-middle Baby-Step Giant Step decryption algorithm. In RSA encryption, the private value to be computed by the BSGS algorithm was the decryption key, “D”, while in Elliptic Curve Cryptography, the private values to be computed were the secret alpha and beta. The secondary purpose of this project was to calculate the amount of iterations required to compute the aforementioned private information in RSA and ECC using the BSGS decryption scheme. The tertiary purpose of this project was to help users of the program learn more about cryptography, specifically about the RSA and elliptic curve cryptosystems by viewing educational videos incorporated into the program’s interface created with the particular intention of guiding users through the algorithms’ complexities in a more intuitive manner. The above purposes were accomplished by writing original code using C++ that could execute the steps required to calculate the desired private information in the studied algorithms and calculate how many iterations were required to compute the information in either algorithm. Qt was used to construct the program’s graphical user interface and Boost Multiprecision software was used to give the program the capacity to be able to handle the extremely large integers involved in this project. The coding in this project could potentially be used to compare the strength of the RSA cryptosystem to the Elliptic Curve Cryptography scheme when using the Baby-Step Giant-Step decryption algorithm to compute the systems’ private information.

Awards Won: