Project proposal CS290G

RSA implementation with speed comparison

Our project idea is to implement RSA encryption to run on the UDOO, using several different optimization methods. We will implement different arithmetic improvement algorithms presented in class, this includes, but are not limited to, the standard multiplication algorithm, binary method, and Montgomery multiplication algorithm. We will then compare the run time on the different versions to look at the speed improvement.

The motivation behind the project idea is to see and measure the effects of using improved arithmetic algorithms, and to find the optimal solution / fastest version.

The approach is to implement one version using standard arithmetic operators, and then, as mentioned, implement other versions using various improved arithmetic algorithms. We will then run the implementations side by side and time them. We expect to see that the versions with the improved arithmetic functions to be more efficient.

The biggest challenge for this project will be to implement the improved arithmetic operators correctly. If the operators contains errors, either the result of the operator or the timing it takes to execute will be wrong. This is especially important to address and test for, because none of the group members have very much experience with implementing alternative arithmetic operators in C. We will implement the project in C, because of the speed and flexibility of the language.