Tyler Lorella

Maxfield England

Cryptography Project Part 1

Thus far we have built most of the SHA-3 algorithm in java using the C implementation as described by Markku-Juhani Saarinen (https://github.com/mjosaarinen/tiny_sha3/blob/master/sha3.c). We have more work todo with converting the code, mostly the "update state with more data", "finalize hash output", "compute SHA-3 hash", and the "xof function". We've encountered mostly conceptual level issues with having difficulty understanding what is going on in the functions and thus being difficult to implement into Java. In order to catch up on our project progress we will be visiting office hours more frequently to ensure we conceptually understand the algorithms, the C implementation, and how it will work in our java program. By the end of the week we're optimistic of completing the Project part 1 progress.