**Final Project Phase 2: Progress Report**

**Lucas Hall ID# 20474841**

**Francisco Gonzalez ID# 20388005**

**Ryan Luna ID# 20201083**

The selected paper has provided us with the framework we need to build upon the research into parallel implementations of cryptographic algorithms. The paper’s implementation is focused on the advantages of parallel execution on a GPU. Our concern is that some machines may not have a dedicated GPU available for handling the encryption process. We believe that we can provide further insight into the advantages of data-parallel execution of (AES) image encryption on a CPU, as opposed to a GPU.

At first, we focused our efforts on implementing an AES algorithm from scratch using various sources. We were able to encrypt/decrypt simple plaintext, however, there were unforeseen difficulties moving towards encrypting larger data (e.g. images) with our scratch AES implementation. Given the timeline, we decided to move towards using a python package that provides AES encryption/decryption quite conveniently. As the focus of our project is on parallel computing (not encryption), we felt that this is a safe move. We have successfully developed the code responsible for the sequential implementation of image encryption/decryption using AES. Proper testing of average encryption and decryption times have yet to be conducted but at first look we have that encryption takes around 0.16 seconds and decryption, around 0.18 seconds. The code was executed on a 2018 MacBook Pro using an Intel i7-8850H CPU. We have begun development on the data-parallel implementation of this code. Once completed, we will do batch encryption of images using both sequential and parallel approaches of our implementation. Furthermore, we will compare execution times of each method and report on that. Due to the timeline, we fear that we will be unable to replicate this work for the DES encryption algorithm as originally planned. Any shortcomings will be reported on and presented.

As of now, each of us have our delegated responsibilities for this project. We have begun work on the presentation and documentation of our work. Overlooking the aforementioned shortcomings, we are confident in our ability to provide viable results by the project deadline.