Block Ciphers in Parallel

1. Introduction
   * If we use a block cipher method of encrypting and decrypting data will it be faster in parallel or sequential
   * Encryption is very important in many types computing especially when transferring data, and it can also be hefty on processing in some cases.
2. Design Considerations
   * Sizes of given data can be of any size and we will need to accomidate for that
   * Threads used were 4,8,16
3. We used up to 16 threads of the stampede cores
4. Visual studio, WinSCP, Putty, notepad++
5. icpc CipherParallel.cpp –o CipherParallel.exe -lpthread | sbatch CipherParallelScript

g++ CipherSerial.cpp -o CipherSerial.exe | sbatch CipherSerialScript

1. Depending on what method of timing the results change drastically. Local hardware produced that using threads could be nearly1.5x faster. Stampede says sequential even in large data cases is faster.
2. ALL TABLES/CURVES CAN BE FOUND IN INCLUDED FILES
3. Trying to figure out why time differences were so large depending on where I ran my code. I could never discover the reason why, but I lean more on my local hardware as it seemed to react to threads.
4. I believe my local hardware is correct and that my program shows that block ciphers in parallel can run faster than sequential even on smaller numbers of around 2000 characters