DannyLangfordHW05

danny14@vt.edu

April 2018

1 Question 3.2

I ran the decryption method locally from 20 bits to 24 bits on one thread each time. Once I hit 24 bits it took roughly 100 seconds to run. I wanted to forecast how long it would take to run 31 bits locally on one thread. I put the data I gathered into Minitab and constructed a time series plot of the data. From there, since it was easy to tell that the data showed exponential growth from 20 to 24 bits, I conducted an exponential forecast of the data up to 31 bits producing the following graph:

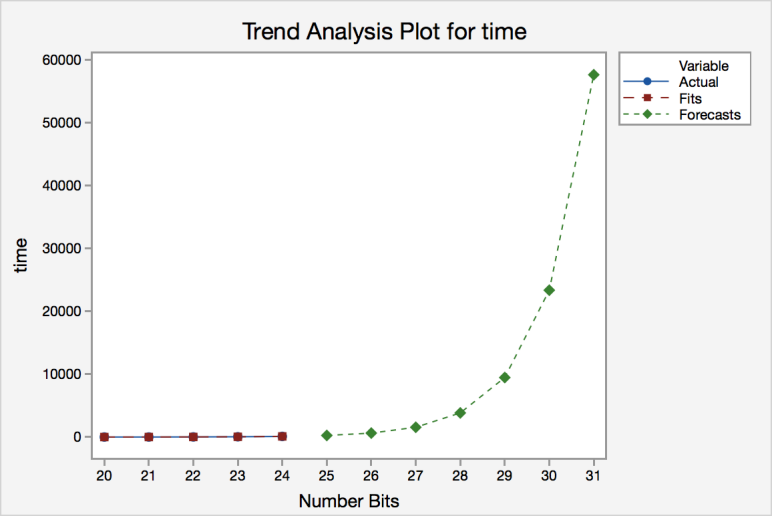

Figure 1: 31 Bits Forecast

We can see at 31 bits it took roughly 57,000 seconds which is the equivalent of 16 hours. I believe this is a good estimate of the time it takes to run the decryption process because adding more bits is an exponentially time consuming process.

2 Question 4.3

When testing different n-bit encryptions, the GPU accelerated version of the decryption program was exponentially faster. As bits increased the time difference between the GPU accelerated version of the decryption program and the normal decryption program grew. In order to achieve the same performance as one of the P100 GPUs on the New River cluster we would have to use 4 to 6 GPU cores to achieve this.