Distributed DES Decryption

DeVonte' Applewhite, Ryan Wheeler, AJ Yeh

Objectives:

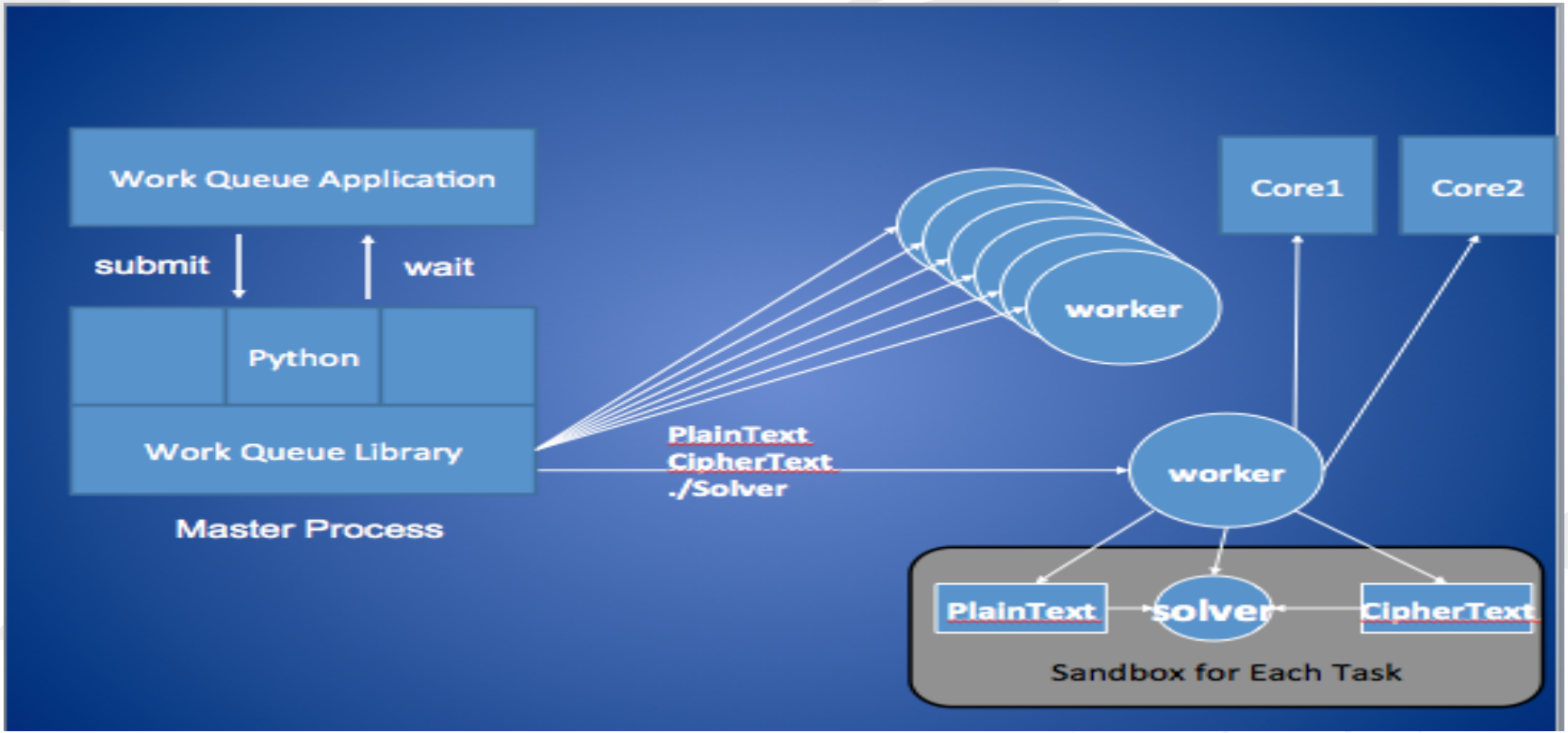
- Create a Brute Force Algorithm to find the DES Encryption Key for a File

- Distribute the Algorithm over the Cloud to maximize throughput

Background : DES

- Symmetric key encryption algorithm
- Key size: 56 bits
- Standardized in 1976
- Block cipher that is seeded by a key

Diagram of System

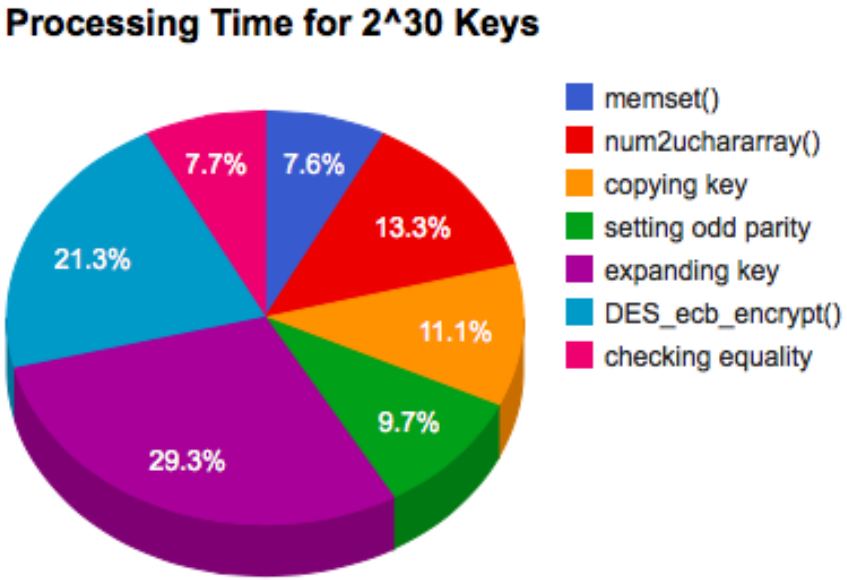


Problems with Size

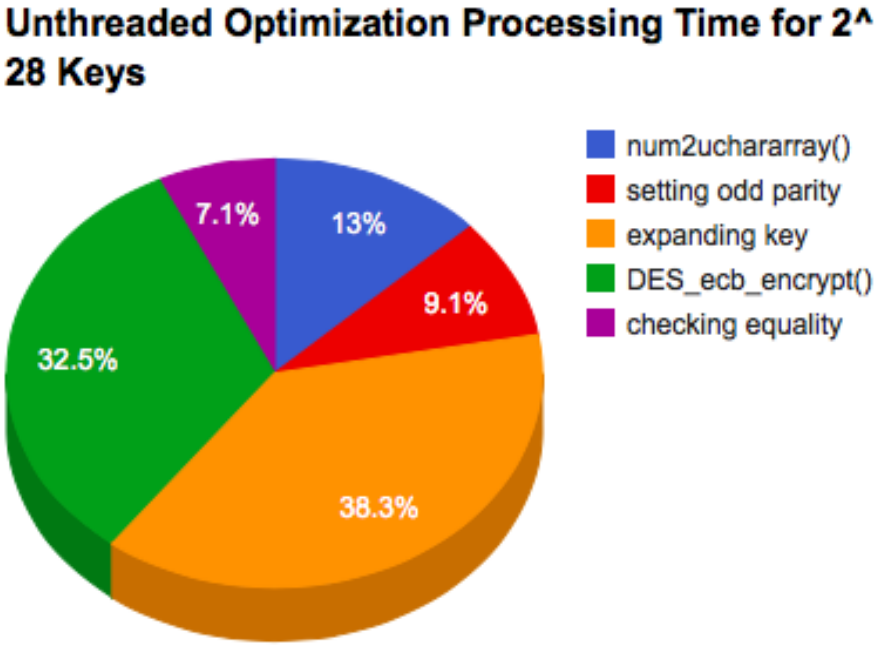
Problem: Our original program tested 3.3*10^6 keys per second. Testing the full key space would take 692 years!!!!!

Revision: Restrict the key size.

Local Optimizations



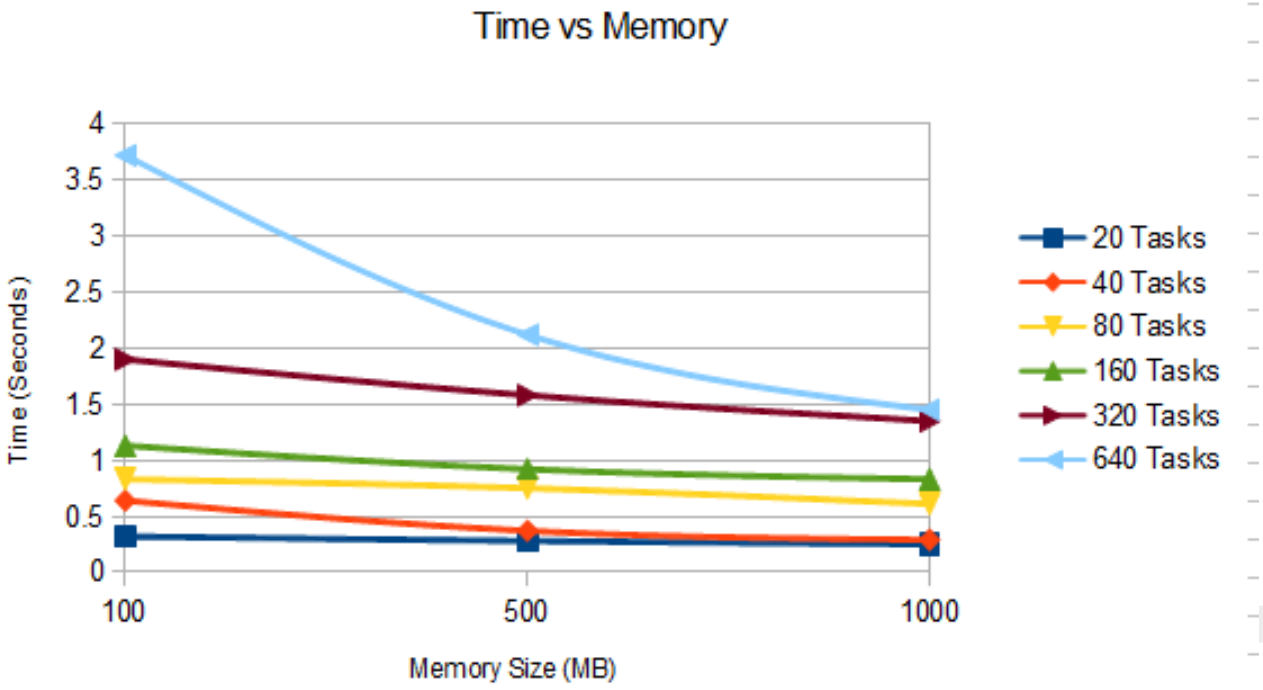
Local Optimizations



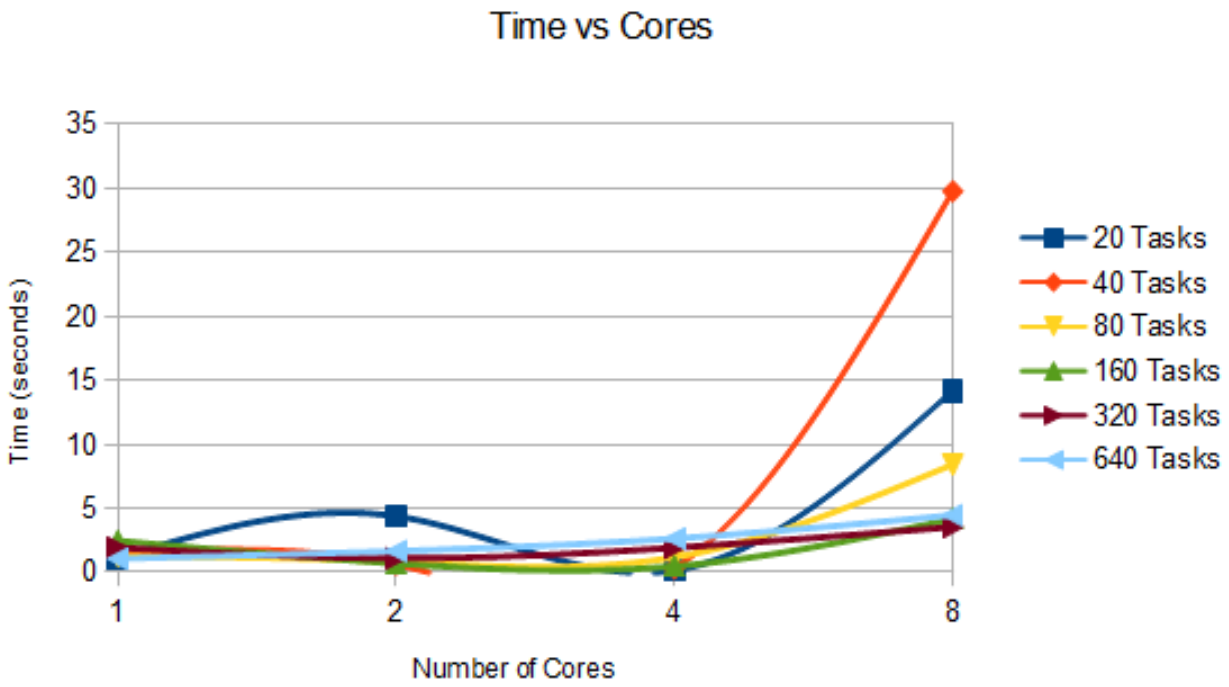
Distributed Optimizations

- Early Exit Optimization
  - This causes the program to exit early if the key is found
  - Whether it exits early is entirely luck based
- Amount of Memory
- Number of Cores
- Disk Space

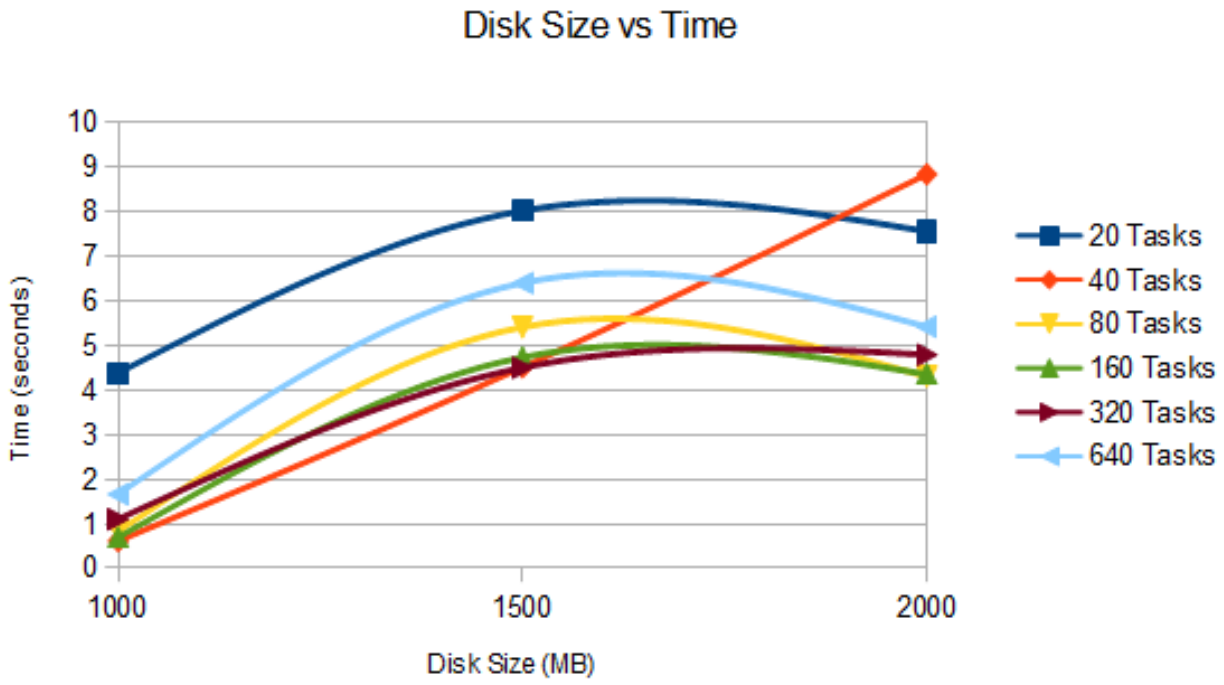
Distributed Optimizations



Distributed Optimizations



Distributed Optimizations



Comparisons and Results

- In 1998, a DES key was broken in 55 hours
- When distributed, a DES key was broken in 22 hours and 15 minutes
- Our Program cracks a 30 bit DES key in less than 1 second on average
  - ~2.13 years for 56 bit key
  - Initially, our program would have taken ~692 years

Thank You