

# Assignment 3

- Main idea: Each workers calculates hashes for a range of possible hints. Then, for a given hash, the worker tries all of our encrypted hints to see if one encrypted hint matches.
  - Why? Hashing is expensive(99% runtime) and we want to avoid duplicate hash calculations.
  - -> The larger the batch, the greater the performance of the algorithm  
Runtime  $\sim$  #batches
- We have one master and  $n$  workers
  - Master: Distributes the hint candidates to the workers. Sends all encrypted hints to every worker.
  - Worker: Calculates the hashes for all of its hint candidates and compares the encrypted hints to them.
  - Similar procedure for password decryption
- Pull Propagation: Worker sends message to master in order to request a new task.
- Tasks can either be hint or password decryption
- When all tasks for a batch are distributed, we request a new batch so that workers that finish their task can get a new task (without waiting for the others to finish)
- Once all hints for a batch are received, we add password encryption tasks for the batch. Once all passwords are encrypted, the batch is deleted from master main mem.