DDM - Duftes Daten Mischen

Assignment 3

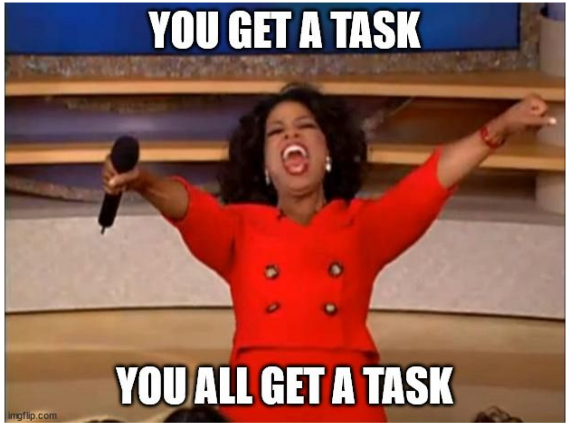
Work Packages

Hint Cracking Tasks

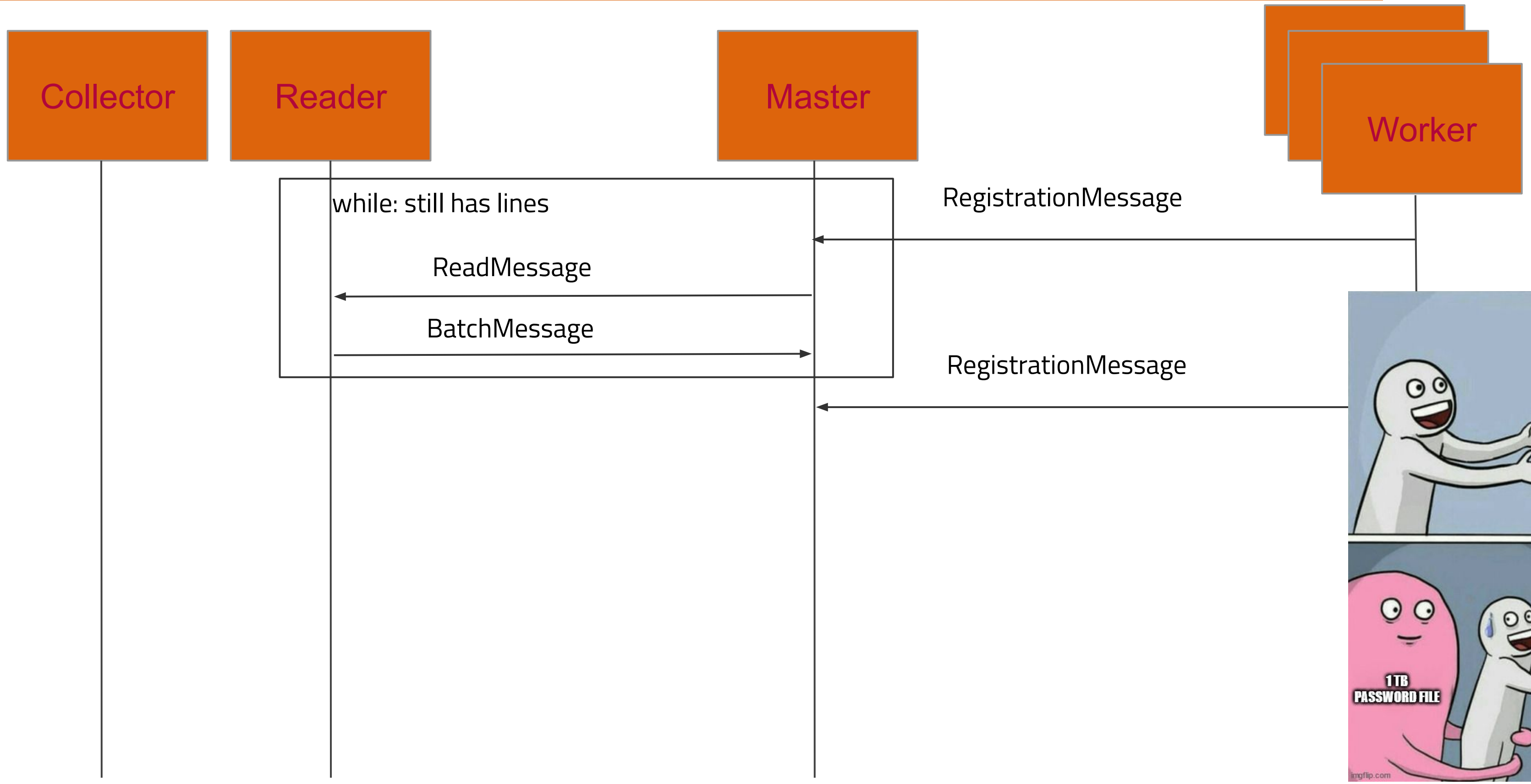
- Generated for one password
- 50 per Worker
- Solution triggers
  - Next passwords hints cracking tasks, if task queue empty
  - Password Cracking Task, if the cracked hint was the last one for the password

Password Cracking Tasks

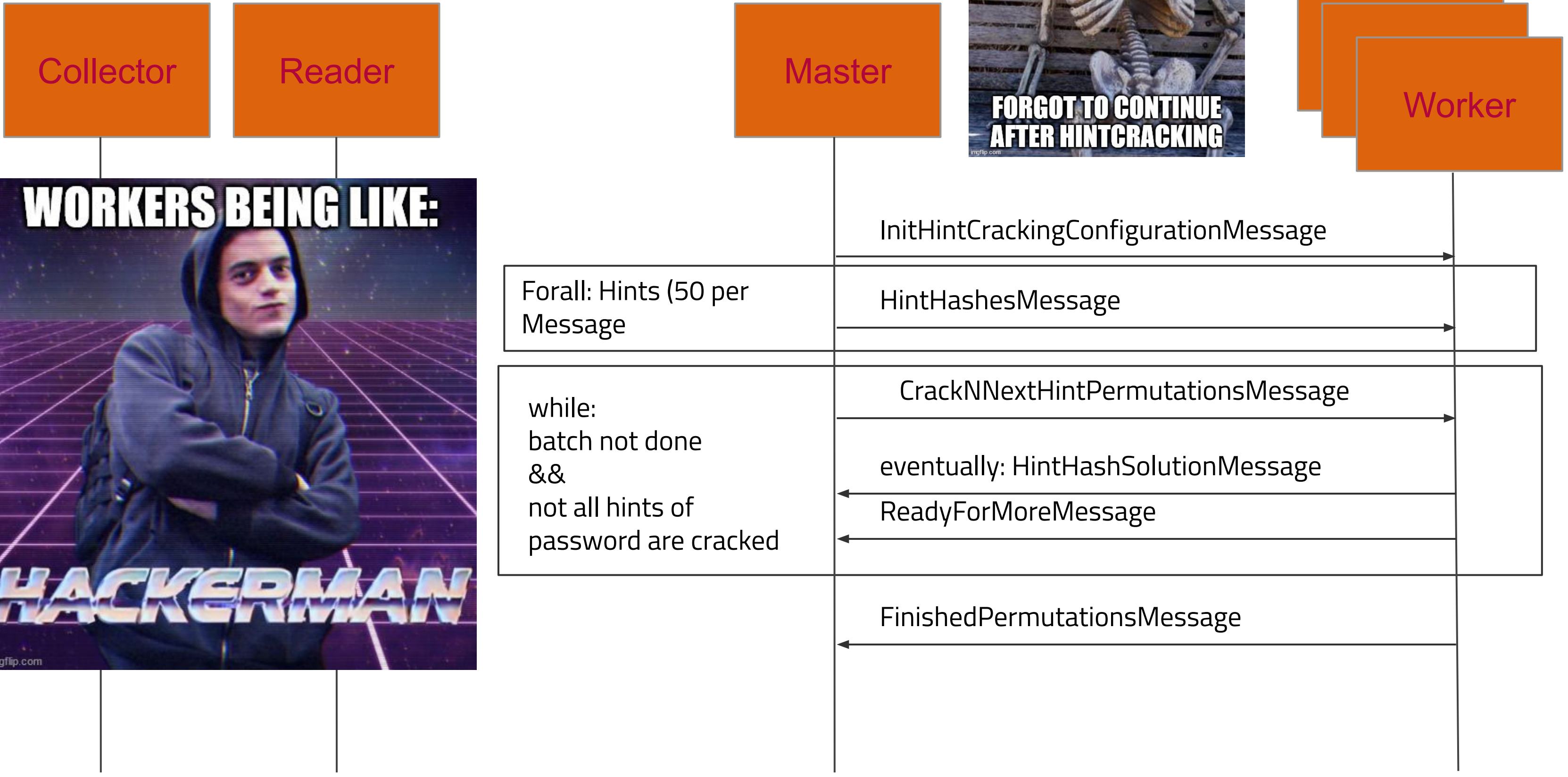
- Scheduled after all hints of the password are known
- Thrown in the same queue as the hint cracking tasks
- Terminates the system, if completed and all passwords are now known



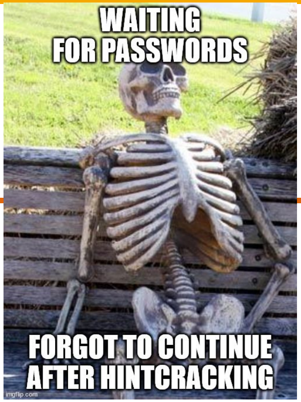
Program Flow 🌊 - Init

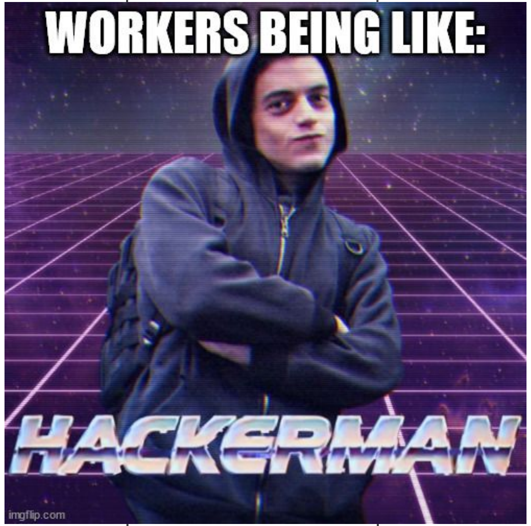


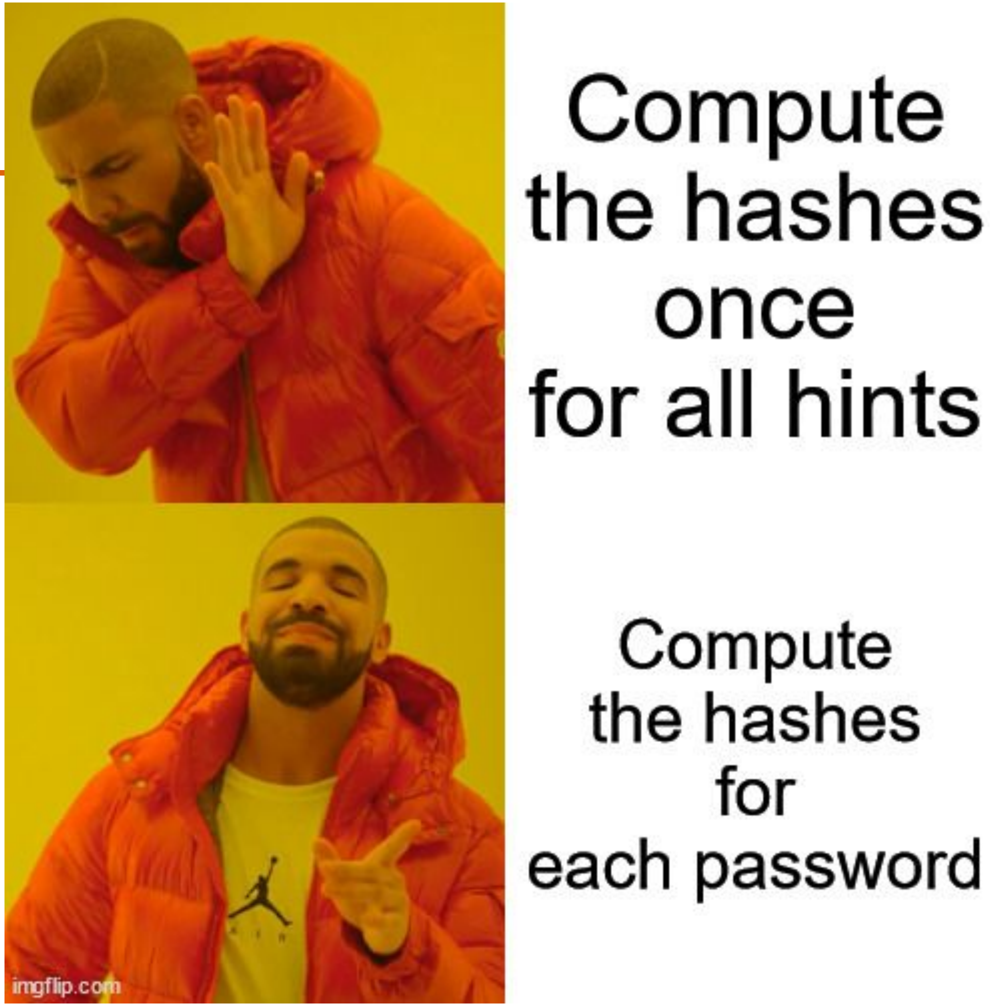
Program Flow 🌊 - Hint Cracking
For each password



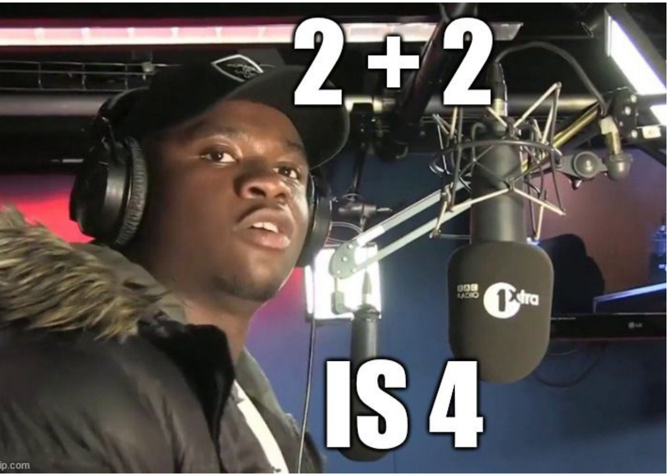
Collector
Reader
Master
Worker
InitHintCrackingConfigurationMessage
Forall: Hints (50 per Message
HintHashesMessage
while:
batch not done
&&
not all hints of
password are cracked
CrackNNextHintPermutationsMessage
eventually: HintHashSolutionMessage
ReadyForMoreMessage
FinishedPermutationsMessage





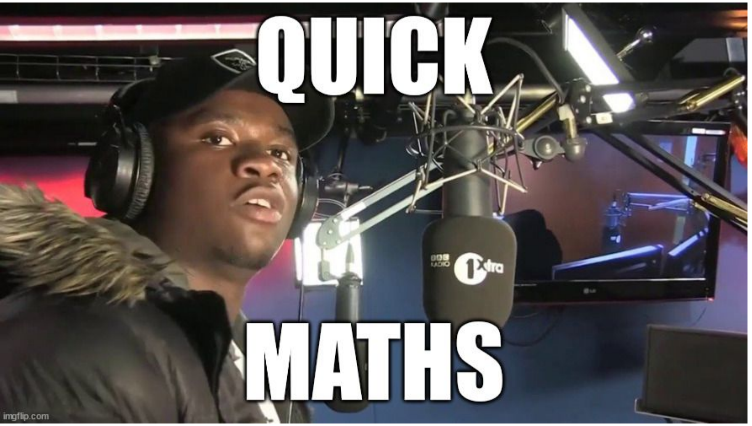

Compute the hashes once for all hints
Compute the hashes for each password
imgflip.com

Generating Password Cracking Jobs with fixed size - independent of alphabet length



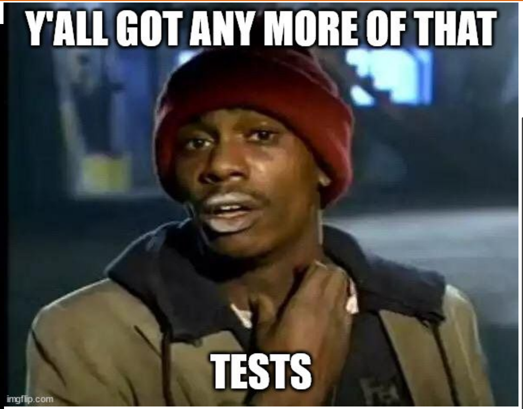
```
public static boolean shiftPwdPermutation(int[] alphabetIndices, int alphabetLength){
        int currentIndex = alphabetIndices.length - 1;
        boolean hasOverflow = true;
        while(hasOverflow && currentIndex >= 0){
                ++alphabetIndices[currentIndex];
                hasOverflow = alphabetIndices[currentIndex] >= alphabetLength;
                if(hasOverflow){
                        alphabetIndices[currentIndex] = 0;
                }
                --currentIndex;
        }
        return !hasOverflow;
  }

  public static boolean addPwdPermutation(int[] firstAlphabetIndices, int[] secondAlphabetIndices, int alphabetLength){
        /* would be nice but we do not want to write catch blocks
        if(firstAlphabetIndices.length != secondAlphabetIndices.length){
                throw new IllegalAccessException("The two provided arguments do not have the same length! First length " +
firstAlphabetIndices.length + "; second length " + secondAlphabetIndices.length);
        } */
        int overflow = 0;
        for(int i = firstAlphabetIndices.length - 1; i >= 0; --i){
                int sum = firstAlphabetIndices[i] + secondAlphabetIndices[i] + overflow;
                if(sum > alphabetLength - 1){
                        int remainder = sum % alphabetLength;
                        overflow = (int) Math.floor((float)sum / (float) alphabetLength);
                        firstAlphabetIndices[i] = remainder;
```

Generating Password Cracking Jobs with fixed size - independent of alphabet length



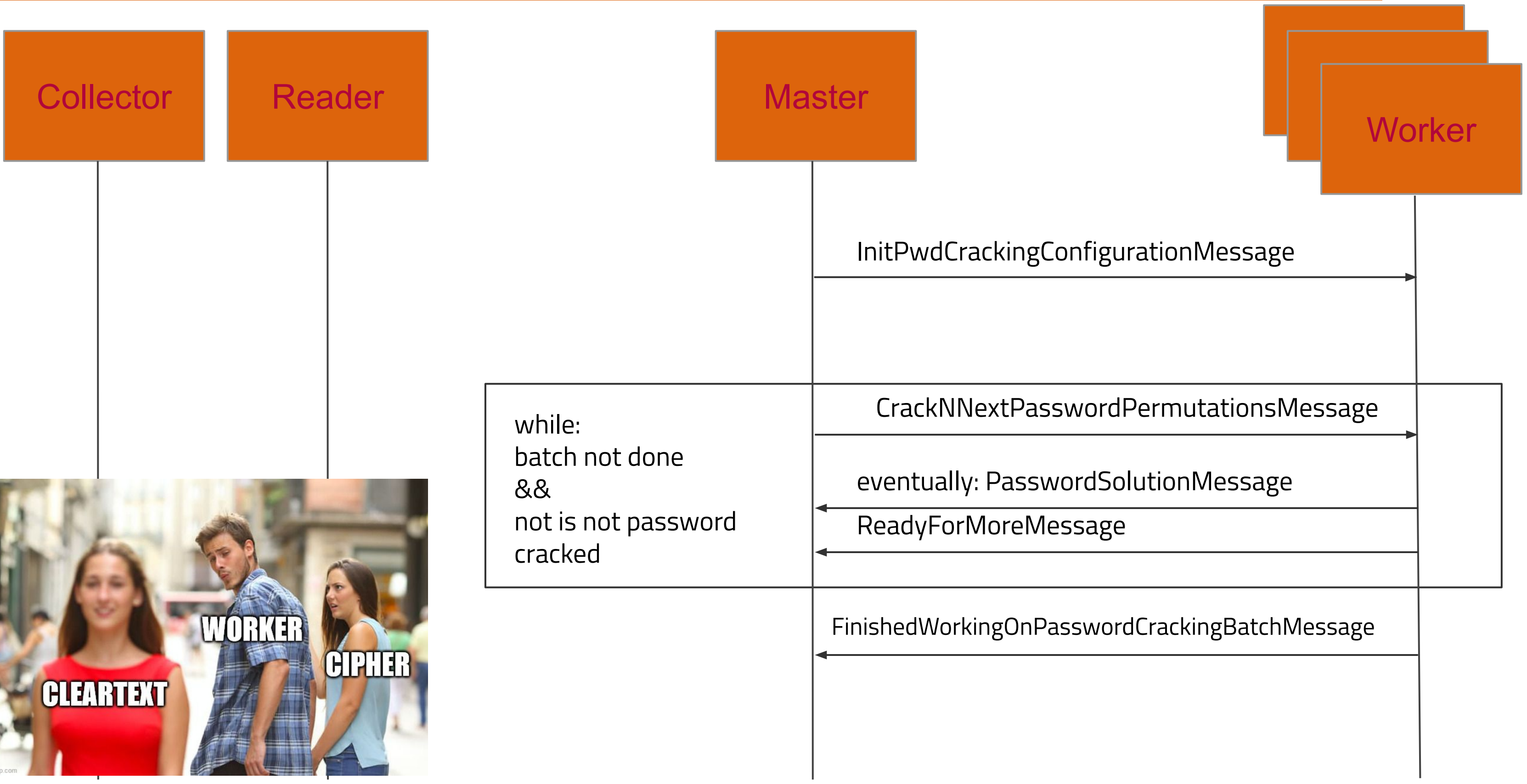
```
                int remainder = sum % alphabetLength;
                overflow = (int) Math.floor((float)sum / (float) alphabetLength);
                firstAlphabetIndices[i] = remainder;
            } else {
                firstAlphabetIndices[i] = sum;
                overflow=0;
            }
        }
        boolean didNotOverflow = overflow == 0;
        return didNotOverflow;
}

public static boolean numberToPermutation(int number, int alphabetLength, int passwordLength, int[] alphabetIndices){
        for(int i = 0; i < passwordLength; ++i){
            alphabetIndices[i] = 0;
        }
        int index = passwordLength - 1;
        while(index >= 0 && number > 0) {
            int remainder = number % alphabetLength;
            alphabetIndices[index] = remainder;
            number = (int) Math.floor((float) number / (float) alphabetLength);
            --index;
        }
        boolean didNotOverflow = number <= 0;
        return didNotOverflow;
}
```

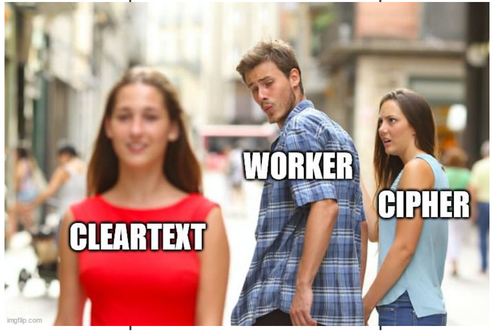
Generating Password Cracking Jobs with fixed size
- independent of alphabet length



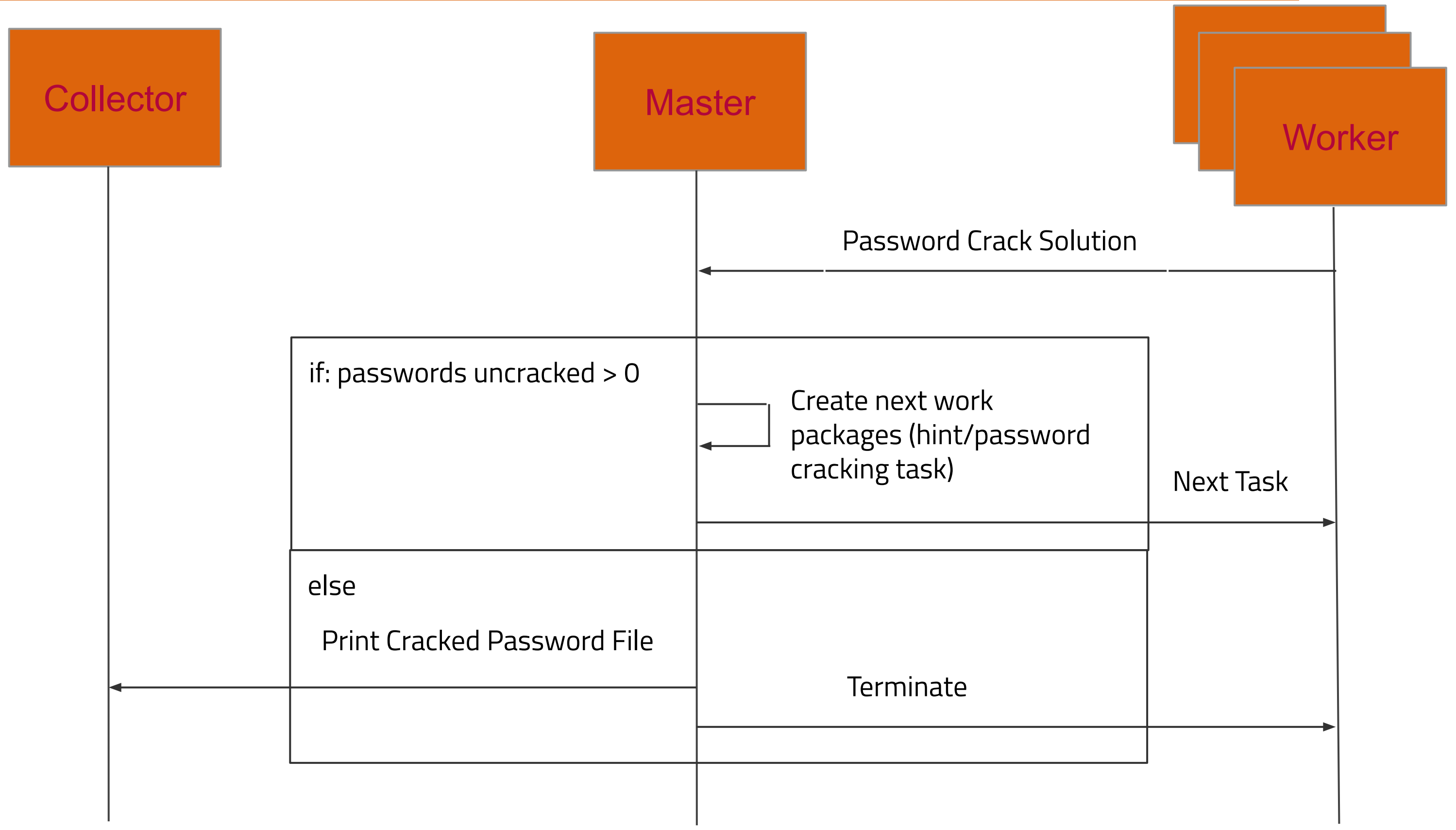
Other teams

Program Flow 🌊 - Password Cracking
For each password


Collector
Reader
Master
Worker
InitPwdCrackingConfigurationMessage
while:
batch not done
&&
not is not password
cracked
CrackNNextPasswordPermutationsMessage
eventually: PasswordSolutionMessage
ReadyForMoreMessage
FinishedWorkingOnPasswordCrackingBatchMessage



Program Flow 🌊 - Teardown


Collector
Master
Worker
Password Crack Solution
if: passwords uncracked > 0
Create next work packages (hint/password cracking task)
Next Task
else
Print Cracked Password File
Terminate

Possible Optimizations

- Sort hints to remove duplicates
- Do not repeat hint cracking packages for each password
- Reduce Worker idle time on task generation
    - Generate new tasks before queue is empty (eg. is reduced to two work packages)
- Send message content in batch (solutions, hints)