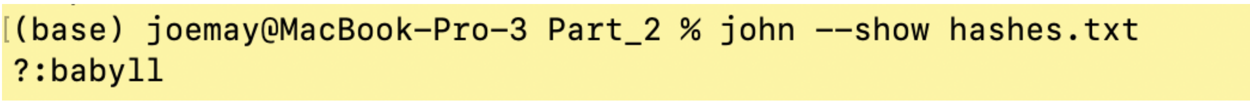
Assignment 2- Part 2 - Report

Joseph May

1. MD5Crypt:

PASSWORD: babyll

DESCRIPTION: In order to crack this password I used the John the Ripper software. Firstly I downloaded the Bee Movie txt file from the link provided. I then used the following command in order to move every word to a new line, uncapitalize each word and remove any extraneous characters that couldn't be contained in the password. I then stored the hash I was given in another txt file. I ran the command john --format=md5crypt --wordlist=wordlist.txt hashes.txt, this attempts to decrypt the words in the hashes.txt file, using wordlist, wordlist.txt in the format of md5crypt. This command found the password in the wordlist.

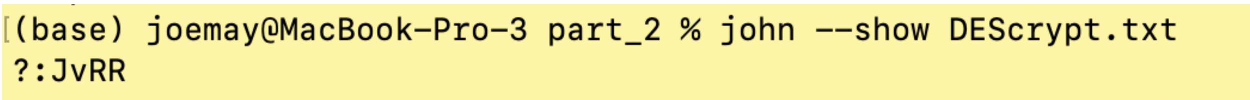


```
[(base) joemay@MacBook-Pro-3 Part_2 % john --show hashes.txt
?:babyll
```

2. DEScrypt:

PASSWORD: JvRR

DESCRIPTION: In order to decrypt this password, firstly the config file was changed in order to limit the max length that was attempted to be decrypted with the knowledge that we were provided. The part of the conf file that was changed was the [Incremental:ASCII] section. The following command was then run in order to decrypt the john --incremental=ASCII --format=descrypt DEScrypt.txt, where the hashed password was stored in the file DEScrypt.txt, and the format of the decryption was DEScrypt.



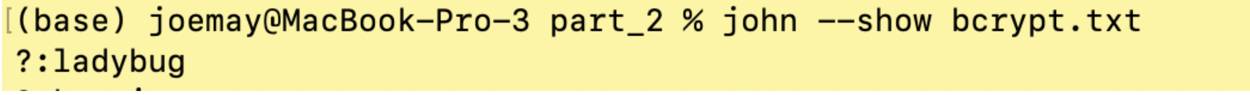
```
[(base) joemay@MacBook-Pro-3 part_2 % john --show DEScrypt.txt
?:JvRR
```

3. bcrypt:

PASSWORD: ladybug

DESCRIPTION: To crack this password firstly I downloaded the password leak file that was provided to use as a wordlist. I then created a txt file called bcrypt.txt that contained my hashed password. I then ran the command john --wordlist=rockyou-20.txt

--format=bcrypt bcrypt.txt, this attempts to crack the hashes in the bcrypt.txt file using the wordlist rockyou-20.txt in the format of bcrypt. This cracked the hashed password.



```
[(base) joemay@MacBook-Pro-3 part_2 % john --show bcrypt.txt
 ?:ladybug
```

4. Custom:

PASSWORD: oliver
DESCRIPTION: For this custom hashed password it was run through three different hash functions 100 times each. The way in which this hash was cracked was the wordlist, which was the same as the bcrypt leaked password wordlist, was used to iterate through each of the words. For each word it was encoded using utf-8 and then ran through md5 100 times, the result was ran through sha256 100 times and then the result was ran through sha512 100 times. The end result was then compared to the hash value that was given and if it matched then that was the password. The code to implement this created two functions, one for iterating through the hash functions and one for reading the wordlist file, calling the hashing function and then comparing to the desired hash. The hashlib library was used for each of the hashing functions, the re library was used in order to only consider 6 letter alphanumeric passwords from the wordlist. For the hashing function the input word is first encoded to utf-8 using .encode. Then a for loop is used for each of the specific hash functions. Then in the cracking function, the wordlist is imported, only the correct words are considered, they are passed through the hash algorithm and then compared to the original hash where it is then outputted. The python file is named customhash.py, the makefile is called Makefile which runs with make or make -B -f Makefile. The executable that is generated is called customhash. All of this code is run using Python 3.12.7.