Lab 4 - Password Cracking

Frankie Fazlollahi

Task 2: Cracking a Set of Passwords

Q1:

```
C:\john\run>john -wordlist=C:\Users\frank\Desktop\HW4Files\dictionary.txt -format=raw-MD5 C:\Users\frank\Desktop\HW4Files\target.txt
```

Figure 1: Command for Wordlist mode

```
$dynamic_0$58b3994b2fc2536ee6d208039d3f8849:casper
$dynamic_0$6e7fbb71576d0ad7a80050881d24385f:badone
$dynamic_0$1719dca083320cac531f636e2d36dfa2:brookstone
$dynamic_0$a20c24703cc44153ac2d83fcc709a344:knockers
$dynamic_0$3cd509071d765eb67dd2a7798d0145c4:braindamage
$dynamic_0$8a54ae86df2d4a9f54a26e80554e806e:hashemi
$dynamic_0$22d7fe8c185003c98f97e5d6ced420c7:qwertyui
```

Figure 2: Passwords cracked using Wordlist mode

```
C:\john\run>john -wordlist=C:\Users\frank\Desktop\HW4Files\dictionary.txt -format=raw-MD5 C:\Users\frank\Desktop\HW4Files\target.txt -rules
```

Figure 3: Command for Wordlist mode with default rules

```
$dynamic_0$58b3994b2fc2536ee6d208039d3f8849:casper
$dynamic_0$6e7fbb71576d0ad7a80050881d24385f:badone
$dynamic_0$1719dca083320cac531f636e2d36dfa2:brookstone
$dynamic_0$a20c24703cc44153ac2d83fcc709a344:knockers
$dynamic_0$3cd509071d765eb67dd2a7798d0145c4:braindamage
$dynamic_0$8a54ae86df2d4a9f54a26e80554e806e:hashemi
$dynamic_0$22d7fe8c185003c98f97e5d6ced420c7:qwertyui
$dynamic_0$ec987ee686247d911ed7311adb2cd7b9:tacoma1
$dynamic_0$37e2182ede57c04db93559ddb03f8ac8:lebanon1
$dynamic_0$f28ef2b2839f1c1cb60259bb2e94bc7a:motorhead1
$dynamic_0$294eea1dda8b7ad51a65f1f6450c25b1:smoesmoe
$dynamic_0$08503486c361db6700e91ccaa2ceb98f:1orange
$dynamic_0$7fee45a45c3a8e547b3e3bc75ba1bcd4:butthead2
$dynamic_0$f768a04b896ebed667e0baec563ac3fc:riverside!
$dynamic_0$38a271d7e80f64a373af4ab471db78e8:homedepot5
$dynamic_0$e2c863f4f009a1e36a37b372cdfe6fb2:bubbles4
$dynamic_0$1882a24c2b2d4f90d819468095ebd13b:ruben6
$dynamic_0$3557ffcb9b6e22ffcb93c8ce24a1d1d5:8ferret
```

Figure 4: Passwords cracked using Wordlist mode with default rules

```
C:\john\run>john --single --format=rawMD5 C:\Users\frank\Desktop\HW4Files\target.txt
```

Figure 5: Command for Single Crack mode

```
$dynamic_0$58b3994b2fc2536ee6d208039d3f8849:casper
$dynamic_0$6e7fbb71576d0ad7a80050881d24385f:badone
$dynamic_0$1719dca083320cac531f636e2d36dfa2:brookstone
$dynamic_0$a20c24703cc44153ac2d83fcc709a344:knockers
$dynamic_0$3cd509071d765eb67dd2a7798d0145c4:braindamage
$dynamic_0$8a54ae86df2d4a9f54a26e80554e806e:hashemi
$dynamic_0$22d7fe8c185003c98f97e5d6ced420c7:qwertyui
$dynamic_0$ec987ee686247d911ed7311adb2cd7b9:tacoma1
$dynamic_0$37e2182ede57c04db93559ddb03f8ac8:lebanon1
$dynamic_0$f28ef2b2839f1c1cb60259bb2e94bc7a:motorhead1
$dynamic_0$294eea1dda8b7ad51a65f1f6450c25b1:smoesmoe
$dynamic_0$08503486c361db6700e91ccaa2ceb98f:1orange
$dynamic_0$7fee45a45c3a8e547b3e3bc75ba1bcd4:butthead2
$dynamic_0$f768a04b896ebed667e0baec563ac3fc:riverside!
$dynamic_0$38a271d7e80f64a373af4ab471db78e8:homedepot5
$dynamic_0$e2c863f4f009a1e36a37b372cdfe6fb2:bubbles4
$dynamic_0$1882a24c2b2d4f90d819468095ebd13b:ruben6
$dynamic_0$3557ffcb9b6e22ffcb93c8ce24a1d1d5:8ferret
```

Figure 6: Passwords cracked using Single Crack mode (nothing new)

```
C:\john\run>john --incremental=Lower --format=raw-MD5 C:\Users\frank\Desktop\HW4Files\target.txt
```

Figure 8: Command for Incremental:Lower mode

```
$dynamic_0$58b3994b2fc2536ee6d208039d3f8849:casper
$dynamic_0$6e7fbb71576d0ad7a80050881d24385f:badone
$dynamic_0$1719dca083320cac531f636e2d36dfa2:brookstone
$dynamic_0$a20c24703cc44153ac2d83fcc709a344:knockers
$dynamic_0$3cd509071d765eb67dd2a7798d0145c4:braindamage
$dynamic_0$8a54ae86df2d4a9f54a26e80554e806e:hashemi
$dynamic_0$22d7fe8c185003c98f97e5d6ced420c7:qwertyui
$dynamic_0$ec987ee686247d911ed7311adb2cd7b9:tacoma1
$dynamic_0$37e2182ede57c04db93559ddb03f8ac8:lebanon1
$dynamic_0$f28ef2b2839f1c1cb60259bb2e94bc7a:motorhead1
$dynamic_0$294eea1dda8b7ad51a65f1f6450c25b1:smoesmoe
$dynamic_0$08503486c361db6700e91ccaa2ceb98f:1orange
$dynamic_0$7fee45a45c3a8e547b3e3bc75ba1bcd4:butthead2
$dynamic_0$f768a04b896ebed667e0baec563ac3fc:riverside!
$dynamic_0$38a271d7e80f64a373af4ab471db78e8:homedepot5
$dynamic_0$e2c863f4f009a1e36a37b372cdfe6fb2:bubbles4
$dynamic_0$1882a24c2b2d4f90d819468095ebd13b:ruben6
$dynamic_0$3557ffcb9b6e22ffcb93c8ce24a1d1d5:8ferret
$dynamic_0$cd763fe469bf116ee5e35fd459196164:portinga
$dynamic_0$b64dbac9ad2efa88f07d3cd33778877d:iamadam
$dynamic_0$814ddf77ccb791db542d9f0656e4b875:fildaman
```

Figure 9: Passwords cracked using Incremental:Lower mode

```
C:\john\run>john --incremental=ASCII --format=raw-MD5 C:\Users\frank\Desktop\HW4Files\target.txt
```

Figure 10: Command for Incremental:ASCII mode

```
$dynamic_0$58b3994b2fc2536ee6d208039d3f8849:casper
$dynamic_0$6e7fbb71576d0ad7a80050881d24385f:badone
$dynamic_0$1719dca083320cac531f636e2d36dfa2:brookstone
$dynamic_0$a20c24703cc44153ac2d83fcc709a344:knockers
$dynamic_0$3cd509071d765eb67dd2a7798d0145c4:braindamage
$dynamic_0$8a54ae86df2d4a9f54a26e80554e806e:hashemi
$dynamic_0$22d7fe8c185003c98f97e5d6ced420c7:qwertyui
$dynamic_0$ec987ee686247d911ed7311adb2cd7b9:tacoma1
$dynamic_0$37e2182ede57c04db93559ddb03f8ac8:lebanon1
$dynamic_0$f28ef2b2839f1c1cb60259bb2e94bc7a:motorhead1
$dynamic_0$294eea1dda8b7ad51a65f1f6450c25b1:smoesmoe
$dynamic_0$08503486c361db6700e91ccaa2ceb98f:1orange
$dynamic_0$7fee45a45c3a8e547b3e3bc75ba1bcd4:butthead2
$dynamic_0$f768a04b896ebed667e0baec563ac3fc:riverside!
$dynamic_0$38a271d7e80f64a373af4ab471db78e8:homedepot5
$dynamic_0$e2c863f4f009a1e36a37b372cdfe6fb2:bubbles4
$dynamic_0$1882a24c2b2d4f90d819468095ebd13b:ruben6
$dynamic_0$3557ffcb9b6e22ffcb93c8ce24a1d1d5:8ferret
$dynamic_0$cd763fe469bf116ee5e35fd459196164:portinga
$dynamic_0$b64dbac9ad2efa88f07d3cd33778877d:iamadam
$dynamic_0$814ddf77ccb791db542d9f0656e4b875:fildaman
$dynamic_0$f953b3b46f77a401c7696e3c08f7ddaa:maxx13
$dynamic_0$a9799fbbe77e122598eede701fa86a92:sunset15
$dynamic_0$dea3504138eb2b47a164e42f131e0949:candy1992
$dynamic_0$fe7784f19dcb80ce0c2d83604cec226a:1memme
$dynamic_0$927a6b823e57598f4b955fe6b75df1d8:babigirl1
$dynamic_0$fa6eea2bcddac31cb1423b57296c561a:1susan2
$dynamic_0$13a29bed00f54bdebe58c6964ca93c30:20013694
$dynamic_0$630d744e04e0fb3f21409cd0f8f7e78c:2123546a
$dynamic_0$ba4618e21435b5165e62944042303a36:papone67
$dynamic_0$267f6c48301b826129a8b7f7227e1b79:1t18490
$dynamic_0$fb7c4f5c4e75aa0f08dd9b74179ffa07:1medical
$dynamic_0$831ee7ad177fc0e2907f1f662db339c0:goodday1
$dynamic_0$f7b0b76d6ac99a6b129a70c972b8edd7:dingding1
$dynamic_0$06a8398e54ae42c3654abfd6e6e274d1:f00tba11
$dynamic_0$71d59f7ce0de8b66dcafce78941546d3:teamdisco
$dynamic_0$5c3eaa3d54f364264c621dd61ab37979:criminal16
```

Figure 11: Passwords cracked using Incremental:ASCII mode

```
C:\john\run>john -wordlist=C:\Users\frank\Desktop\HW4Files\dictionary.txt -format=raw-MD5 C:\Users\frank\Desktop\HW4Files\target.txt --rules=Jumbo
```

Figure 12: Command line for Wordlist mode with Jumbo rules

```
$dynamic_0$58b3994b2fc2536ee6d208039d3f8849:casper
$dynamic_0$6e7fbb71576d0ad7a80050881d24385f:badone
$dynamic_0$1719dca083320cac531f636e2d36dfa2:brookstone
$dynamic_0$a20c24703cc44153ac2d83fcc709a344:knockers
$dynamic_0$3cd509071d765eb67dd2a7798d0145c4:braindamage
$dynamic_0$8a54ae86df2d4a9f54a26e80554e806e:hashemi
$dynamic_0$22d7fe8c185003c98f97e5d6ced420c7:qwertyui
$dynamic_0$ec987ee686247d911ed7311adb2cd7b9:tacoma1
$dynamic_0$37e2182ede57c04db93559ddb03f8ac8:lebanon1
$dynamic_0$f28ef2b2839f1c1cb60259bb2e94bc7a:motorhead1
$dynamic_0$294eea1dda8b7ad51a65f1f6450c25b1:smoesmoe
$dynamic_0$08503486c361db6700e91ccaa2ceb98f:1orange
$dynamic_0$7fee45a45c3a8e547b3e3bc75ba1bcd4:butthead2
$dynamic_0$f768a04b896ebed667e0baec563ac3fc:riverside!
$dynamic_0$38a271d7e80f64a373af4ab471db78e8:homedepot5
$dynamic_0$e2c863f4f009a1e36a37b372cdfe6fb2:bubbles4
$dynamic_0$1882a24c2b2d4f90d819468095ebd13b:ruben6
$dynamic_0$3557ffcb9b6e22ffcb93c8ce24a1d1d5:8ferret
$dynamic_0$cd763fe469bf116ee5e35fd459196164:portinga
$dynamic_0$b64dbac9ad2efa88f07d3cd33778877d:iamadam
$dynamic_0$814ddf77ccb791db542d9f0656e4b875:fildaman
$dynamic_0$f953b3b46f77a401c7696e3c08f7ddaa:maxx13
$dynamic_0$a9799fbbe77e122598eede701fa86a92:sunset15
$dynamic_0$dea3504138eb2b47a164e42f131e0949:candy1992
$dynamic_0$fe7784f19dcb80ce0c2d83604cec226a:1memme
$dynamic_0$927a6b823e57598f4b955fe6b75df1d8:babigirl1
$dynamic_0$fa6eea2bcddac31cb1423b57296c561a:1susan2
$dynamic_0$13a29bed00f54bdebe58c6964ca93c30:20013694
$dynamic_0$630d744e04e0fb3f21409cd0f8f7e78c:2123546a
$dynamic_0$ba4618e21435b5165e62944042303a36:papone67
$dynamic_0$267f6c48301b826129a8b7f7227e1b79:1t18490
$dynamic_0$fb7c4f5c4e75aa0f08dd9b74179ffa07:1medical
$dynamic_0$831ee7ad177fc0e2907f1f662db339c0:goodday1
$dynamic_0$f7b0b76d6ac99a6b129a70c972b8edd7:dingding1
$dynamic_0$06a8398e54ae42c3654abfd6e6e274d1:f00tba11
$dynamic_0$71d59f7ce0de8b66dcafce78941546d3:teamdisco
$dynamic_0$5c3eaa3d54f364264c621dd61ab37979:criminal16
$dynamic_0$5b858a9f7c6881e63cf39c70e1a6d11e:1nothing1
```

Figure 13: Passwords cracked using Wordlist mode with Jumbo rules

Task 3: Cracking your own password

Q2: I used Incremental:Alnum mode to try to crack my password because the password I chose for this task only consists of letters and numbers. My password was not able to be cracked in the 15 minutes using this mode, likely because incremental mode takes a long time since it is generating all possible character combinations.

```
C:\john\run>john --incremental=Alnum --format=raw-MD5 C:\Users\frank\Desktop\HW4Files\hash.txt
```

Figure 14: Command line for running Incremental:Alnum mode on my password

Task 4: Find the password with the provided information

Q3: I used a mask to try to find this password because we were given information about what the password looks like, which mask mode does well at since it produces fast password candidates when given what the word should look like. The mask I used was [Aa@][Ll][Gg][Ee3][Bb][Rr][Aa@][Ii1][Cc]?d?d?d because this would spell the word "algebraic" that was given with the possibility of some of the letters being uppercase, lowercase, or replaced with @, 1, or 3 for the letters a, e, and i, respectively. I added ?d?d?d at the end in case the 3 digits were appended at the end of the password. This attempt worked on my first try, but if this did not crack the password, then I would have put the ?d?d?d at the beginning instead.

```
C:\john\run>john --mask=[Aa@][Ll][Gg][Ee3][Bb][Rr][Aa@][Ii1][Cc]?d?d?d --format=raw-MD5 C:\Users\frank\Desktop\HW4Files\password.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
Alg3bR@ic406     (file)
1g 2120064p 0:00:00:00 DONE (2021-11-02 09:52) 15.87g/s 33651Kp/s 33651Kc/s 33651KC/s ALGEBR@ic406..@lgeBra1c406
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed
```

Figure 15: Command line and result of using mask on the password based on given information

```
$dynamic_0$cfe188bd21e5296f8f4c5cd4c7abe70f:Alg3bR@ic406
```

Figure 16: Password cracked