Project 3: Password and Key

CS4371 - Spring 2019

Due 4/30

ISSUED BY

Qijun Gu

GROUP 3 MEMBERS

Alexander Muyshondt

Anna Cowsar

Cynthia Cordova

Dylan Olgin

Saud Altwayan

Section I (Introduction):

Summarize what you have done in the project and clearly state the responsibility of each group member, e.g. who did which task, who wrote which part of the report, how your group was coordinated, etc.

Alexander Muyshondt: I worked with my group on Task I to set up the network and the firewall. I worked with Saud and Dylan on Task II to turn on the wireless card and establish the static IP for the network. Following the aircrack tutorial, I worked with my group to find the WEP key of the wireless network and set up the wireless card of Computer A.B to access the wireless network of Network B. I wrote the outline for the report and typed portions for Section III.

Anna Cowsar: I helped with trying to ssh into the other computer also some with changing the program in a way that works for the tasks. I helped with calculating the total keys in the last section in the report.

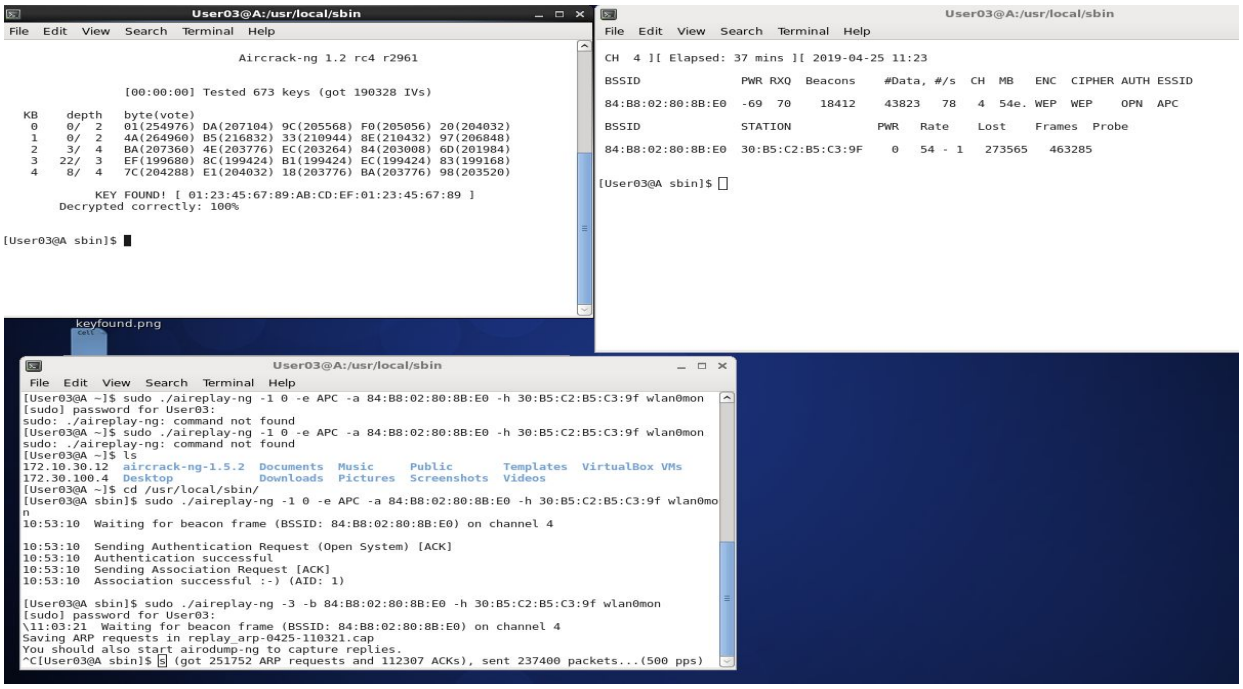
Cynthia Cordova: In this project I helped with task II as we were following the aircrack tutorial and task III and IV on finding the secret pdf files and finding the right key to decrypt them. I helped write some information on section III.

Dylan Olgin: I worked on task 2, setting up the ethernet card, finding the wep key and cracking it. Some of task 3 and most of task 4 using enc and dec for the various files required. Helped gather the screenshots for the report.

Saud Altwayan: I worked with my group on task one, specifically configuring the firewall and fixing the configurations of the computers and first half of task 2, specificaly 1 to 3. I did not work on any part in task 3. I also worked with the group on the first half of task 4. I helped gather the screenshots with the group for the report, specifically task 4.

Section II (Task II):

a) Show the screen shot when you are running aircrack and obtaining the key.



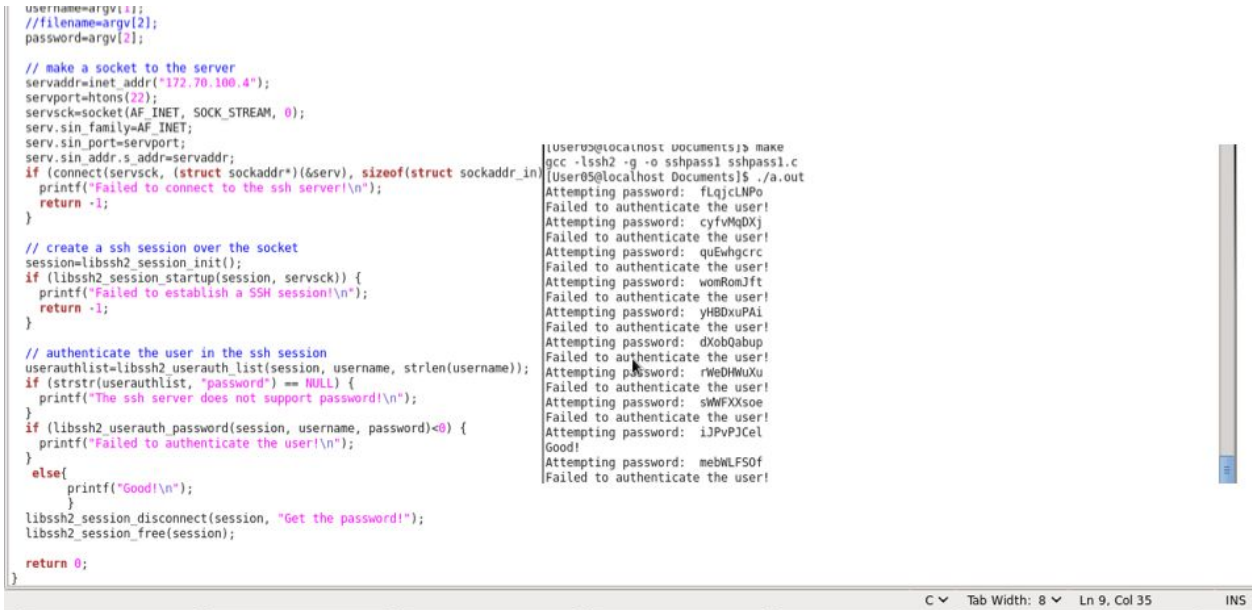
b) Report how long it takes to crack the WEK key and how many packets are captured in order to crack the key.

Initially, it took us 36 minutes to crack the key and we captured 284,035 packets in the process. After rerunning this section of aircrack again to find the quickest time, we were able to find the key in around 4 minutes and 60,000 packets.

```
[User03@A sbin]$ sudo ./aireplay-ng -3 -b 84:B8:02:80:8B:E0 -h 30:B5:C2:B5:C3:9f wlan0mon
[sudo] password for User03:
\11:03:21  Waiting for beacon frame (BSSID: 84:B8:02:80:8B:E0) on channel 4
Saving ARP requests in replay_arp-0425-110321.cap
You should also start airodump-ng to capture replies.
Read 605359 packets (got 4462 ARP requests and 2786 ACKs), sent 4257 packets...(499 pps)
```

Section III (Task III):

a) Show the screenshot of your program when you are testing each password and obtaining the password to ssh Computer B.2 as “User”.



b) Report how long it takes to find the password.

Since the list only contained 10 entries it took about 4 and a half minutes to find the correct password in the short list shown above.

c) If the password is in the file “dictionary.real.txt”, estimate how long it will take to find the password.

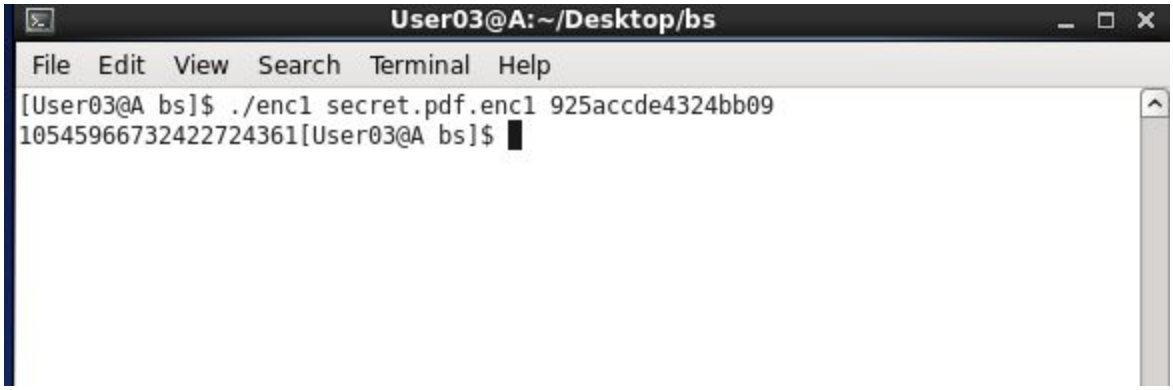
If the password was to be searched for in the file “dictionary.real.txt”, it will take an estimated:

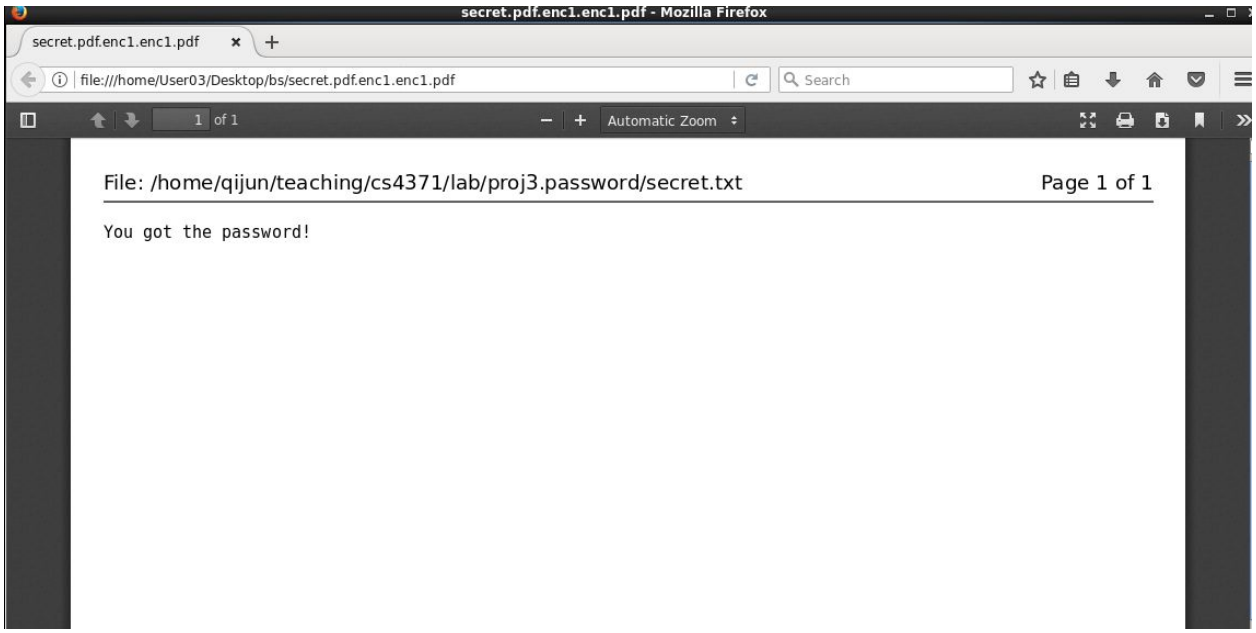
14394810 seconds = 239913.5 minutes = 3998.55833 hours = 166.606597 days

This is based on the assumption that the last password attempted is the correct one. According to these calculations it takes roughly 30 seconds per password, 29.99993 seconds, so hope that the password starts with either a number or an A.

Section IV (Task IV):

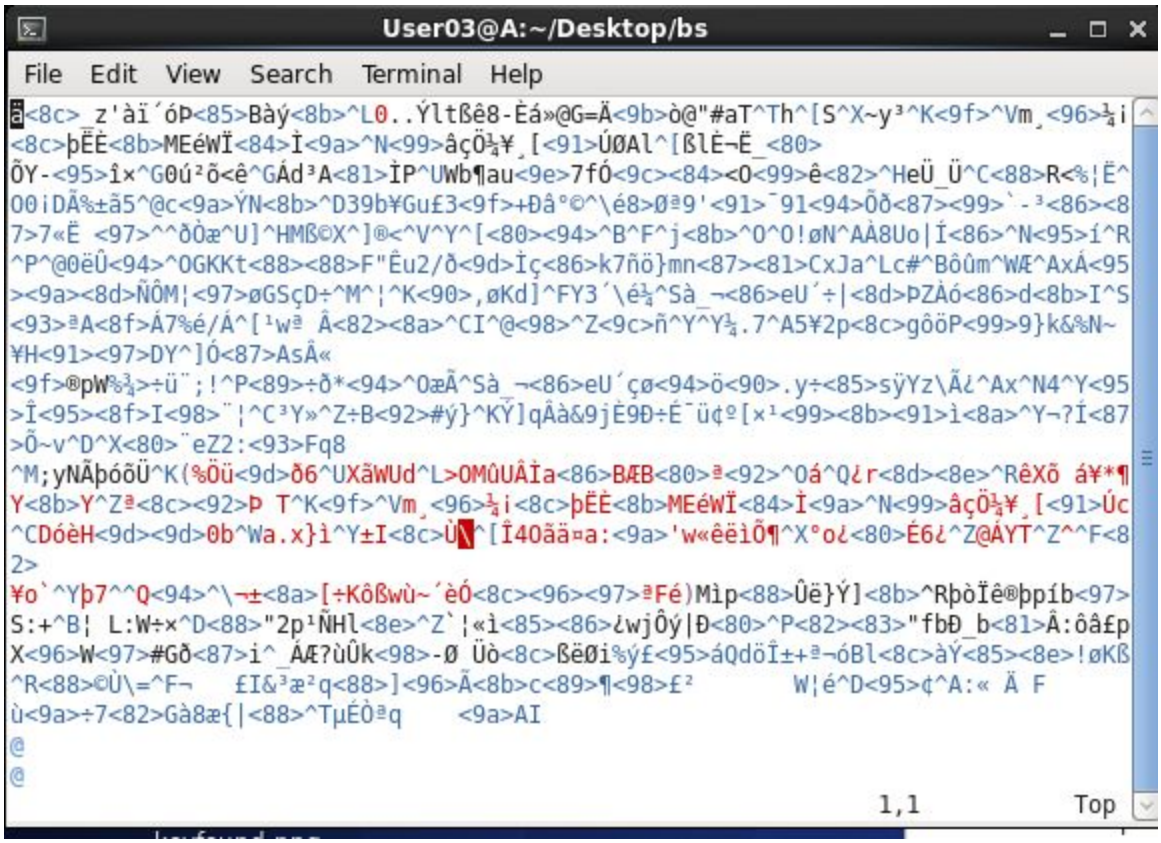
a) Show the screen shot of your cryptoanalysis program when you get the key and the content of the encrypted file secret.pdf.enc1.



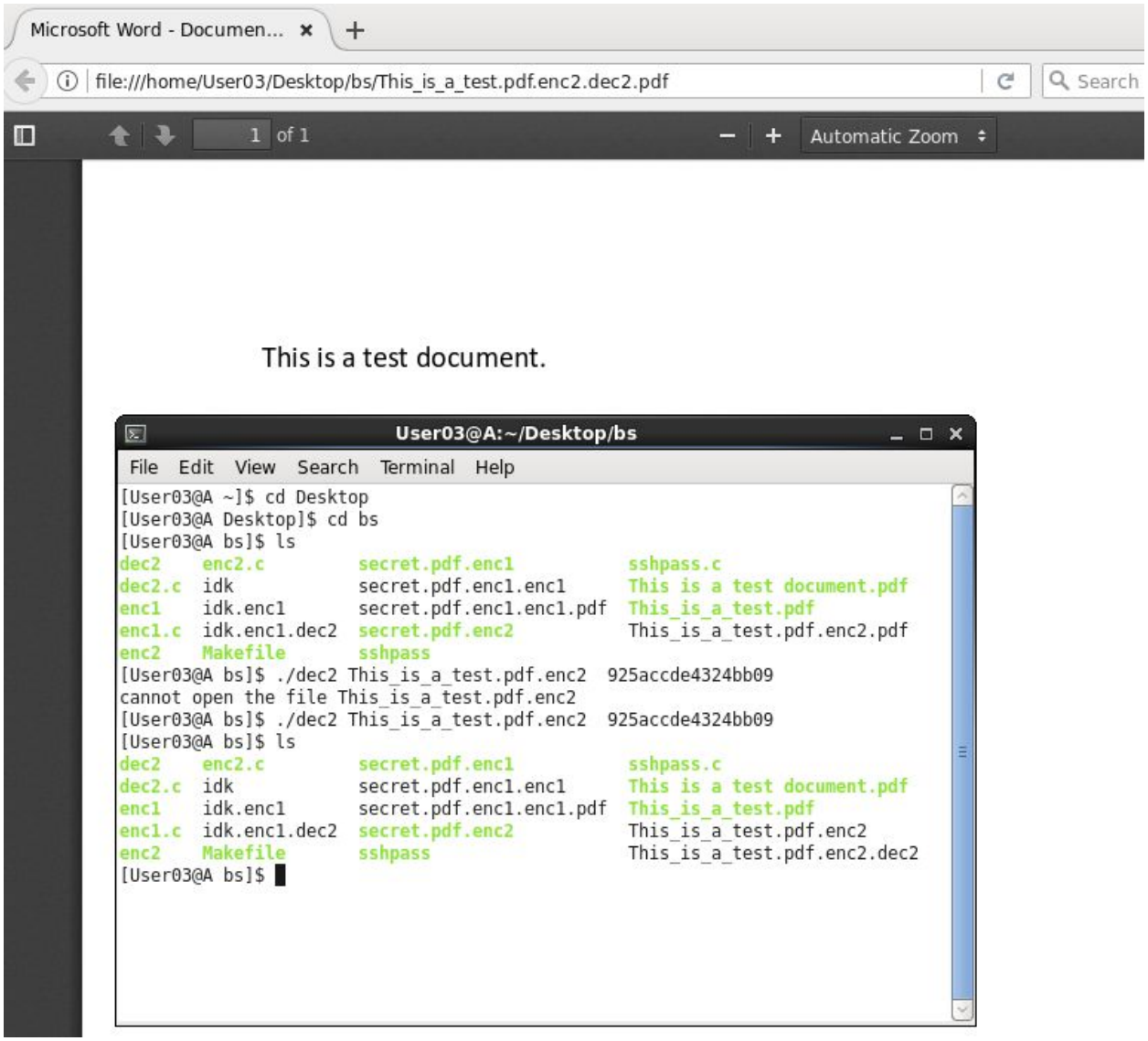


b) Show the screen shot of your AES program when it deciphers a testing file. The test file is created by you and encrypted by enc2.c.

Our encrypted test file



Decrypted Test file



c) Show the screen shot of your AES program when you are brute force cracking the key.

```
File  Edit  View  Search  Terminal  Help
trying key: 78359185
trying key: 78359186
trying key: 78359187
trying key: 78359188
trying key: 78359189
trying key: 78359190
trying key: 78359191
trying key: 78359192
trying key: 78359193
trying key: 78359194
trying key: 78359195
trying key: 78359196
trying key: 78359197
trying key: 78359198
trying key: 78359199
trying key: 78359200
trying key: 78359201
trying key: 78359202
trying key: 78359203
trying key: 78359204
trying key: 78359205
trying key: 78359206
trying key: 78359207
trying key: 78359208
trying key: 78359209
trying key: 78359210
trying key: 78359211
trying key: 78359212
trying key: 78359213
trying key: 78359214
trying key: 78359215
trying key: 78359216
trying key: 78359217
trying key: 78359218
trying key: 78359219
trying key: 78359220
trying key: 78359221
trying key: 78359222
trying key: 78359223
trying key: 78359224
trying key: 78359225
trying key: 78359226
trying key: 78359227
trying key: 78359228
trying key: 78359229
trying key: 78359230
trying key: 78359231
trying key: 78359232
trying key: 78359233
trying key: 78359234
trying key: 78359235
trying key: 78359236
trying key: 78359237
trying key: 78359238
trying key: 78359239
trying key: 78359240
trying key: 78359241
real    10m0.001s
user    1m17.157s
sys     4m23.613s
[root@localhost SEC]#
```

d) Report how many keys are tested in 10 minutes.

Shown below.

e) Estimate how long it will take to find the key.

Note that you may not be able to find the key given the current hardware.

Total Keys = 1.844674407E19 (2^64)

Keys Tested in 10 minutes = 78359241

Estimated Keys Tested in an hour = 470155446

Total Keys/Estimated Keys Tested in an hour = 3.923541508E10

It would take a maximum time of:

3.923541508E10 hours

Over 1 trillion days

Over a million years

Over 44k centuries

to attempt all current passwords on the given hardware. Goodluck!