Project 3: Password and Key

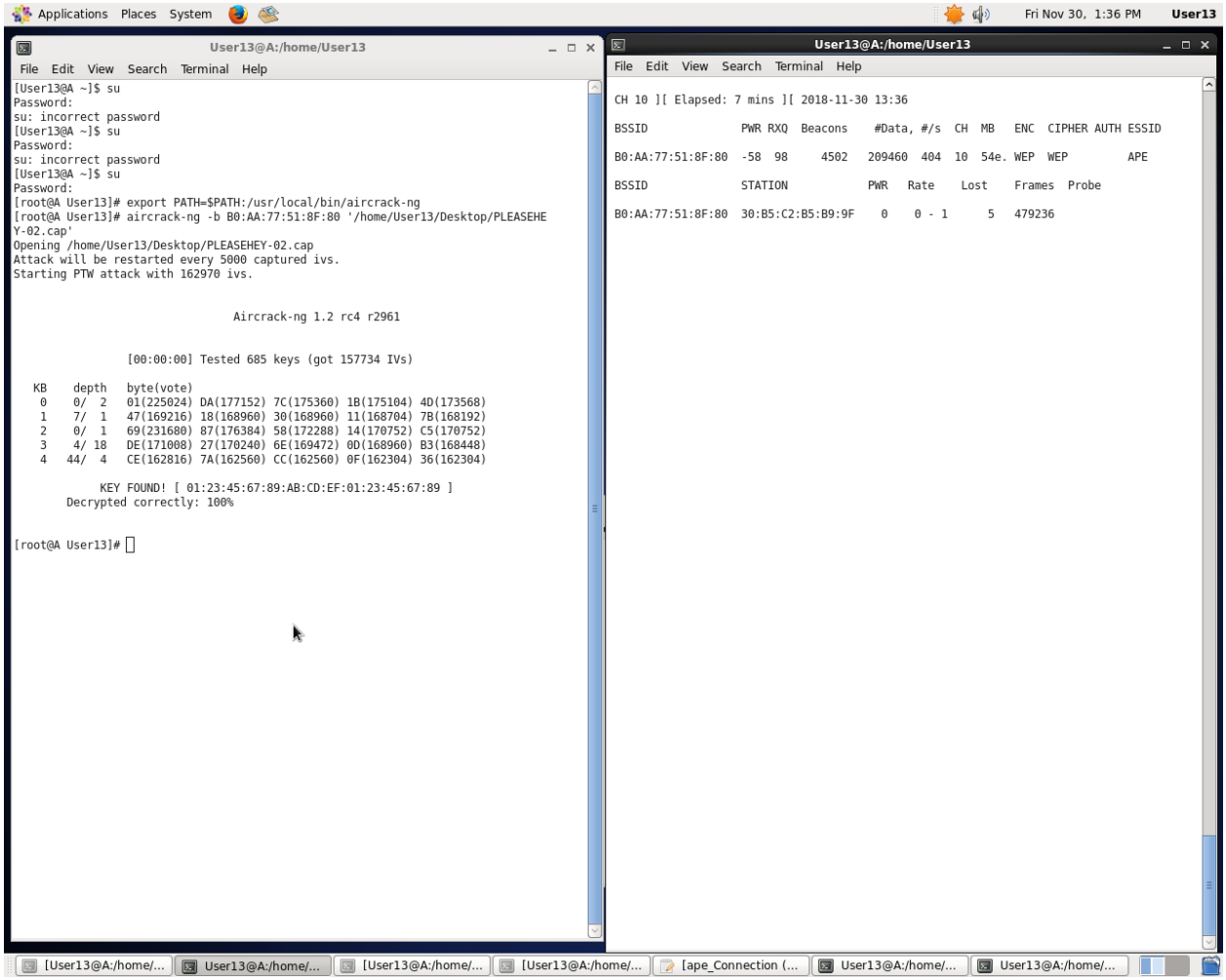
Miguel Archundia
Jacobo Sanchez
Derek Hernandez
Salvador Romero Mondragon

Section I (Introduction)

Miguel did task 1 . Miguel, Derek and Jacobo did task 2. Miguel , Derek and Romero did task 3. Miguel , Derek and Jacobo did Task 4. Miguel and Jacobo wrote the introduction. Derrick and romero compiled the screenshots. Miguel and Jacobo consulted in answering the remaining questions.

Section II (Task II)

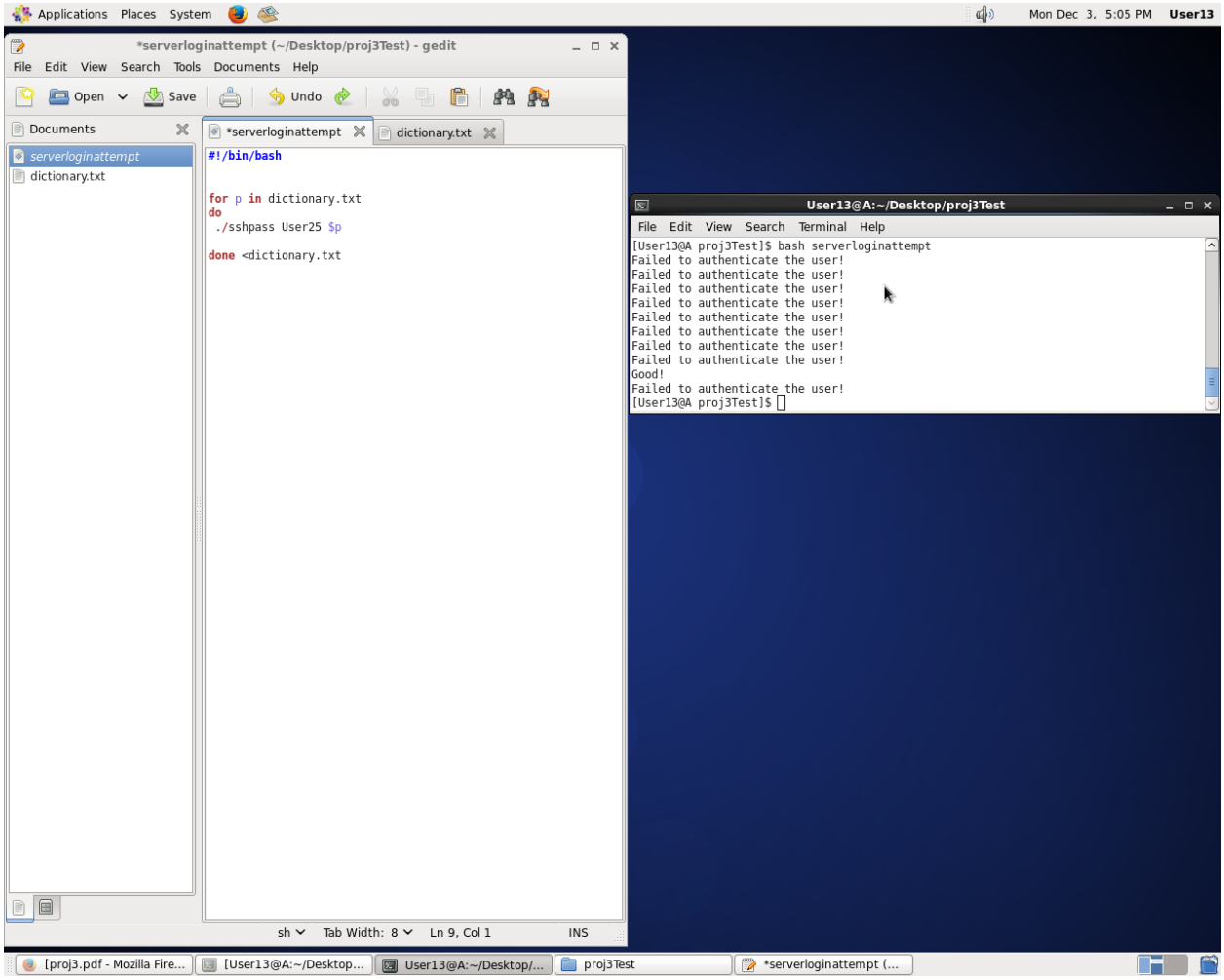
a) **Screenshot running aircrack and obtaining the key**
b) Report how long it takes to crack the WEP key and how many packets are captured in order to crack the key.



Once we allowed it to gather data for about 15 minutes we found the key almost immediately.

Section III (Task III)

a)Screenshot of program when testing each password and obtaining the password to computer E.2. as “user”



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

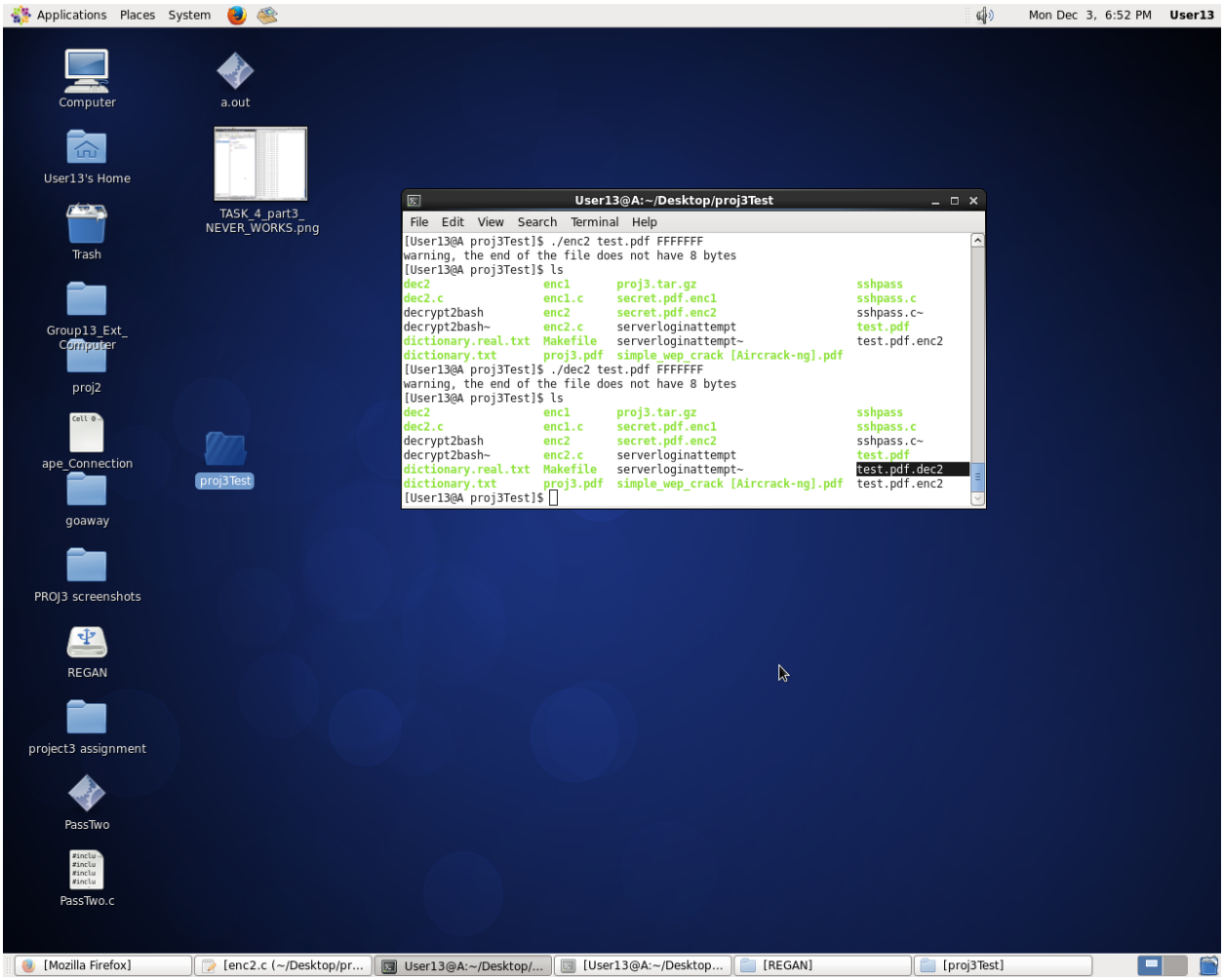
It took about 30 seconds per password.

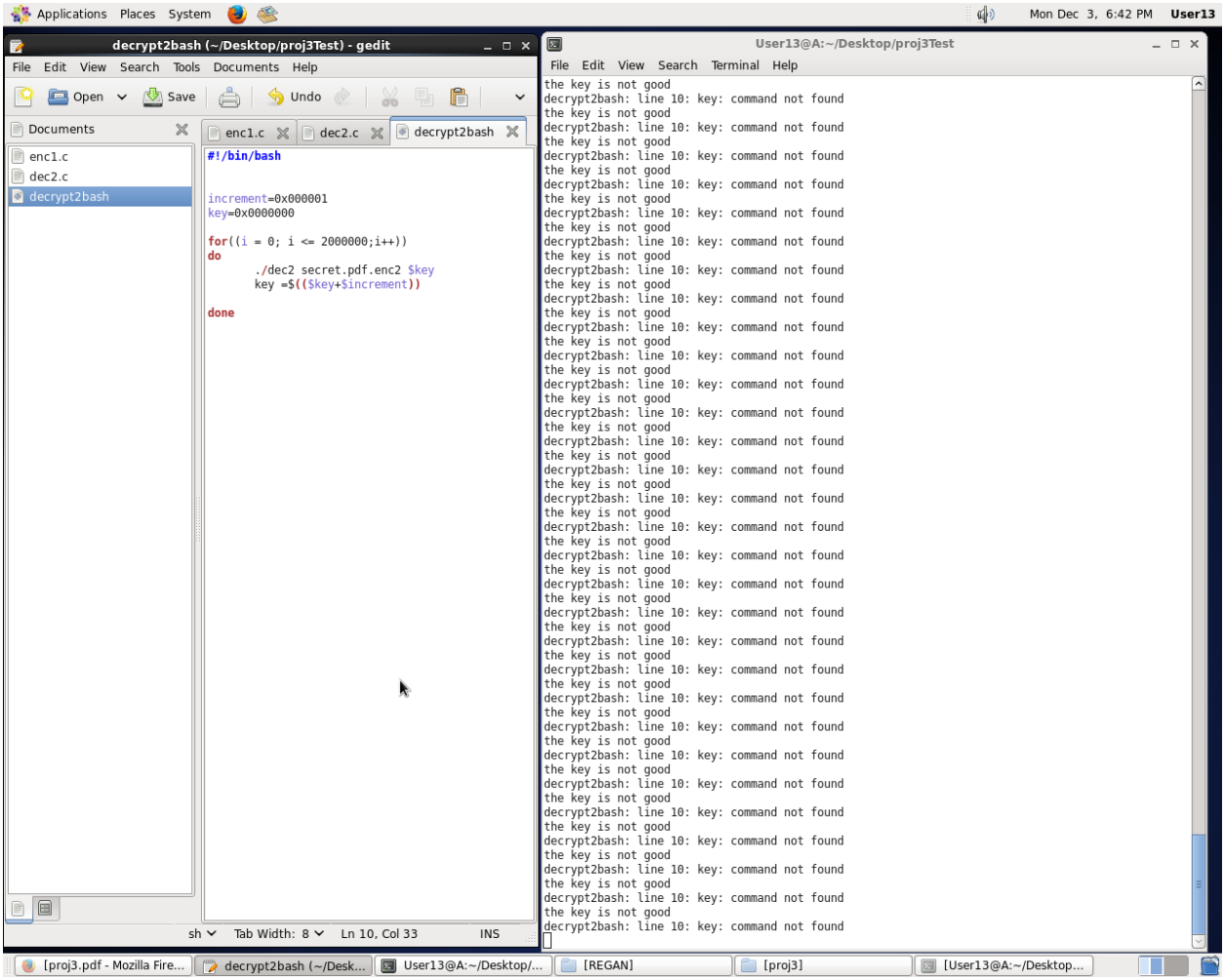
c) If the password is in the file “dictionary.real.txt” estimate how long it will take to find the password

If the 30 second rule holds true it would take about 30 seconds for each password and this real dictionary.txt is thousands of lines long. While it is still n time complexity the “n” in this case is extremely long and would take hours to completely search linearly through the list. .

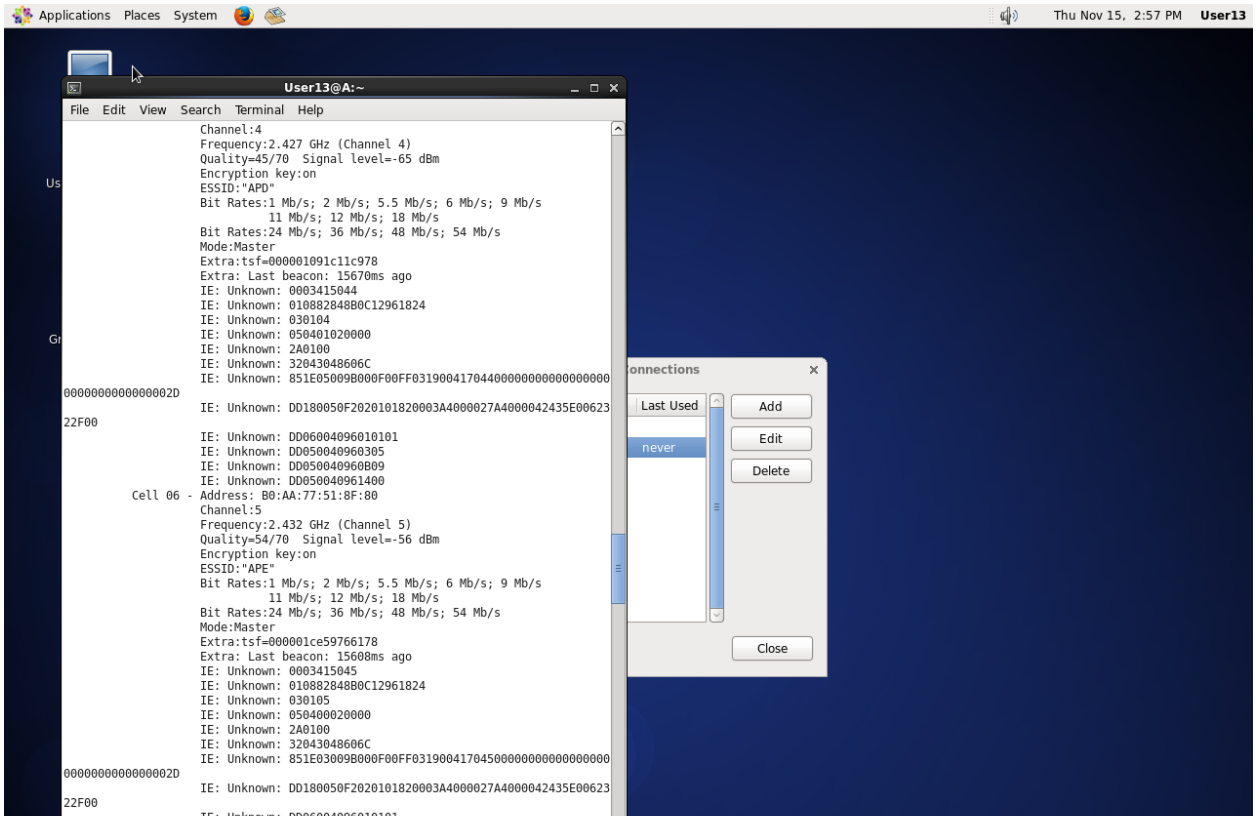
Section IV (Task IV)

a) Screenshot of cryptanalysis program when you get the key and the content of the encrypted file secret.pdf.encl.
b) Screenshot of DES program when it deciphers a test file.





c) Screenshot of DES program brutal forcing cracking the key.



d) Report how many keys are tested in 10 minutes

It tested about 5 keys a second so at 5 keys/per second for 10 minutes it would test about 3000 keys.

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

If keys are 7 bytes the max hex number would be FFF FFFF which is equivalent to 268,435,456 million keys to search through. Which at the current rate on the lab machines would take 53,687,091.2 minutes to complete. This is about 1000 minutes more than the total minutes of a year.