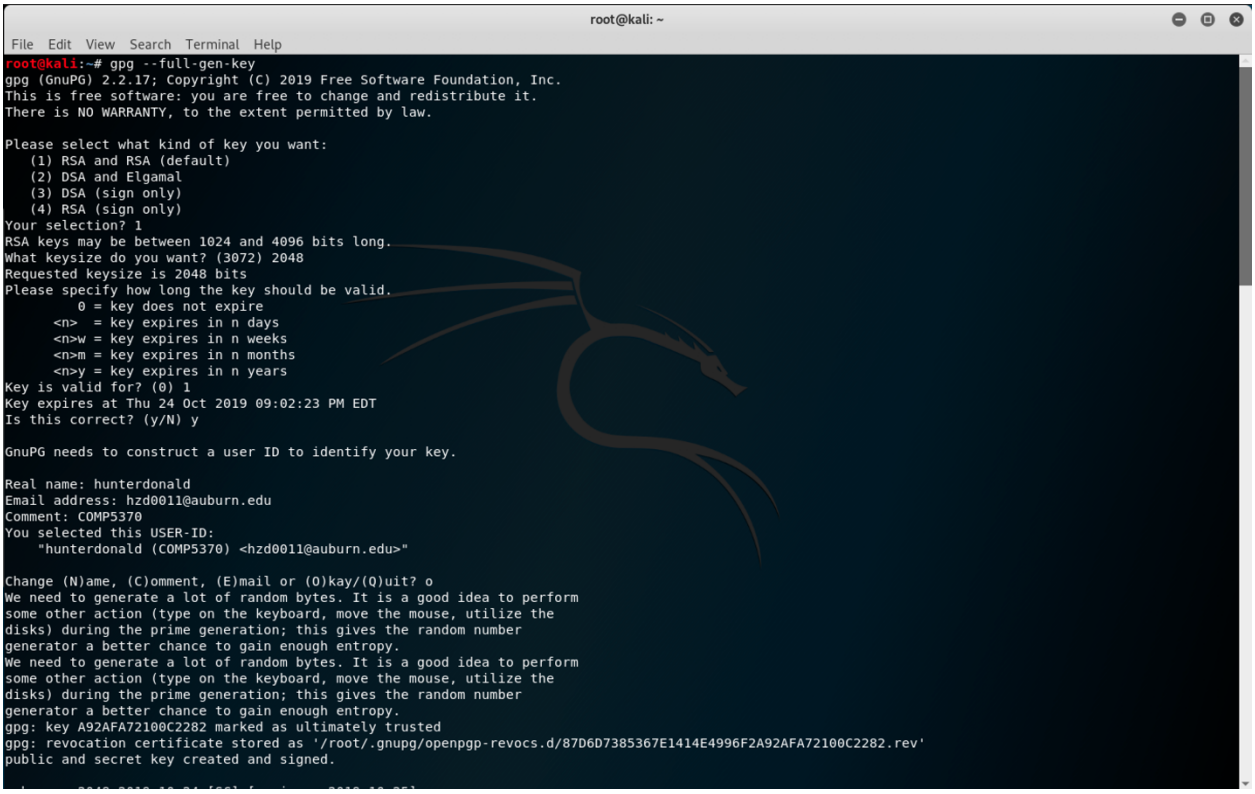
Hunter Donald
hzd0011
COMP 5370
Homework 3

1)

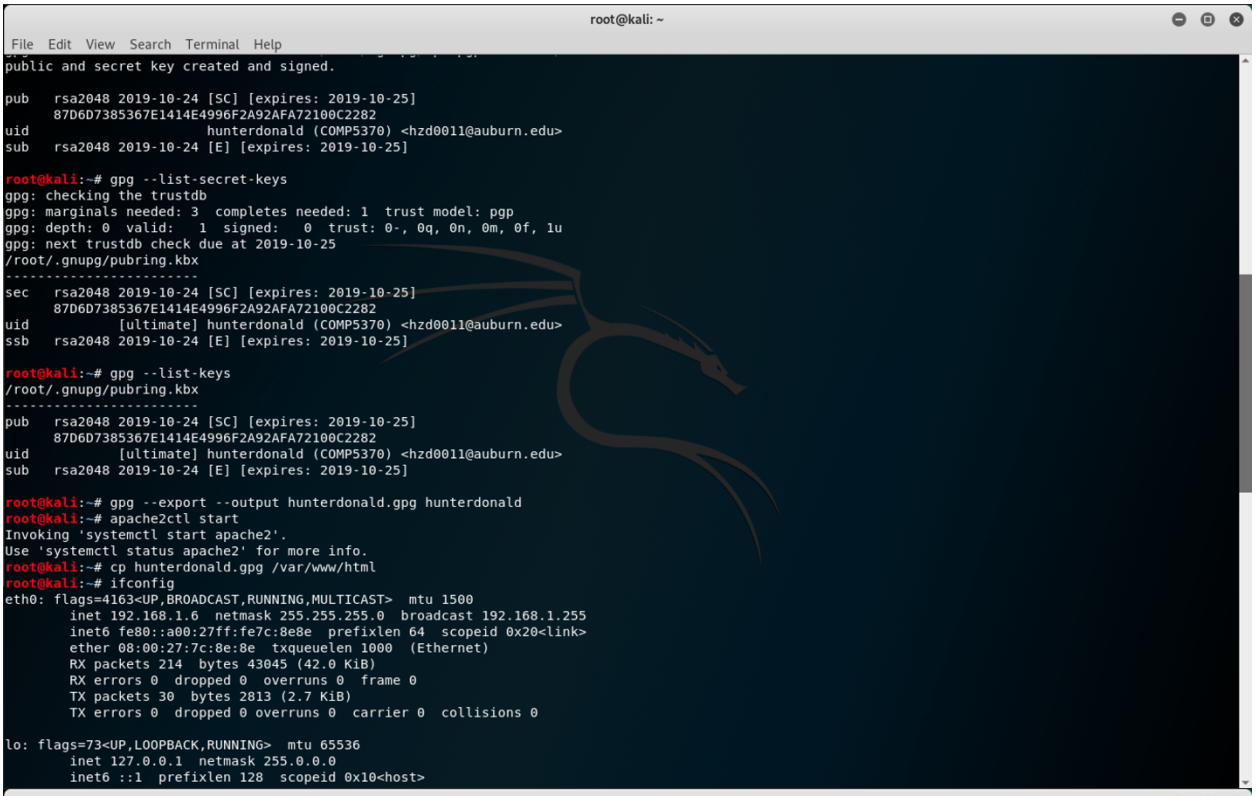
a. The limitations and capabilities of access control mechanisms differ in distributed systems because they may use a variety of access control mechanisms that must be integrated to support the organization's policy.
   i. Lightweight Directory Access Protocol allows a modular, expandable access control and single sign-on solution to be deployed rapidly for all applications in the information system.
   ii. Kerberos uses a trusted third party which provides a means by which constituents of the network can trust each other. These constituents may be any hardware of software that communicates across the network.

b. "chmod u+rwx, g+rx, o-rwx Auburn_Security_Mechanisms"

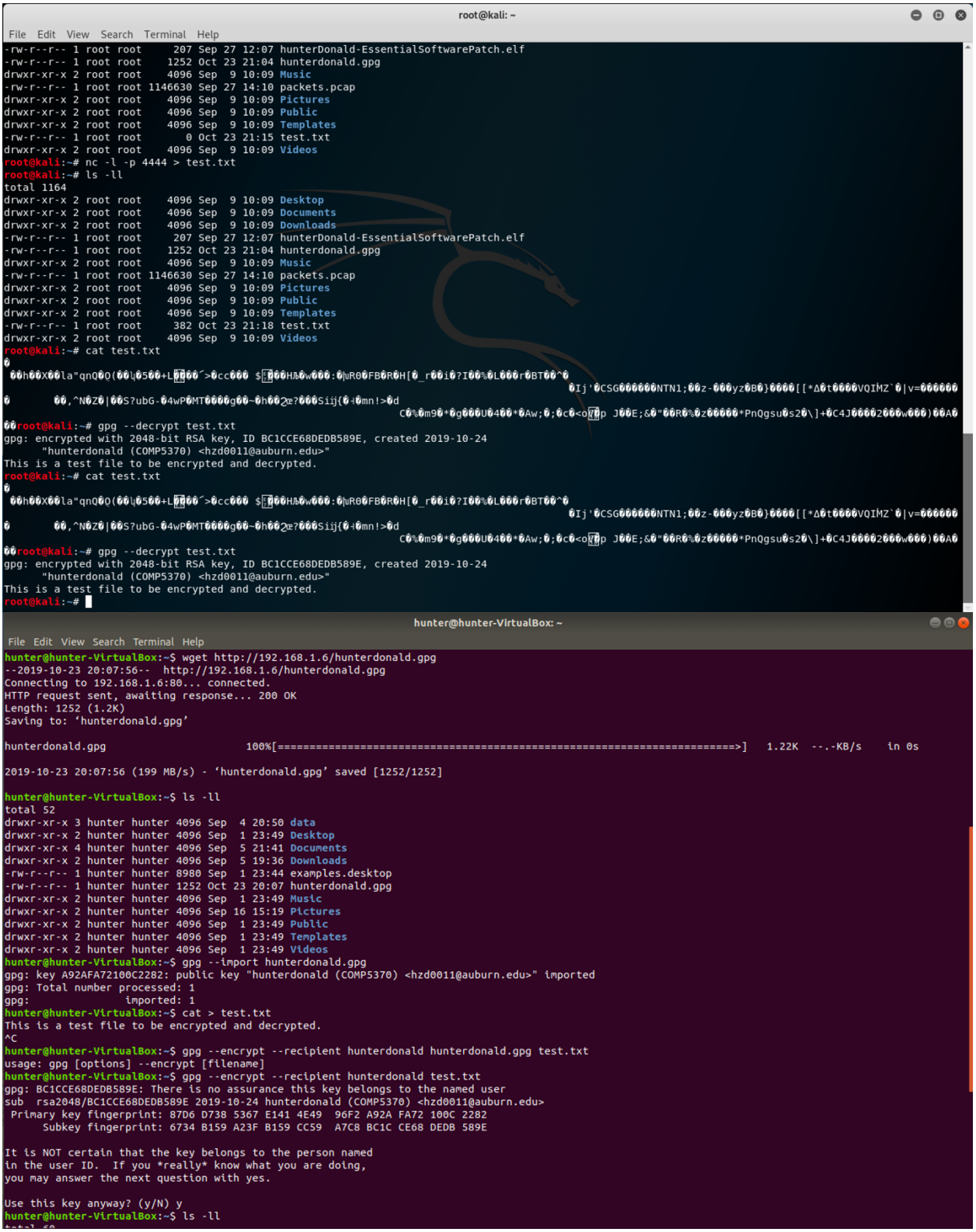
2)



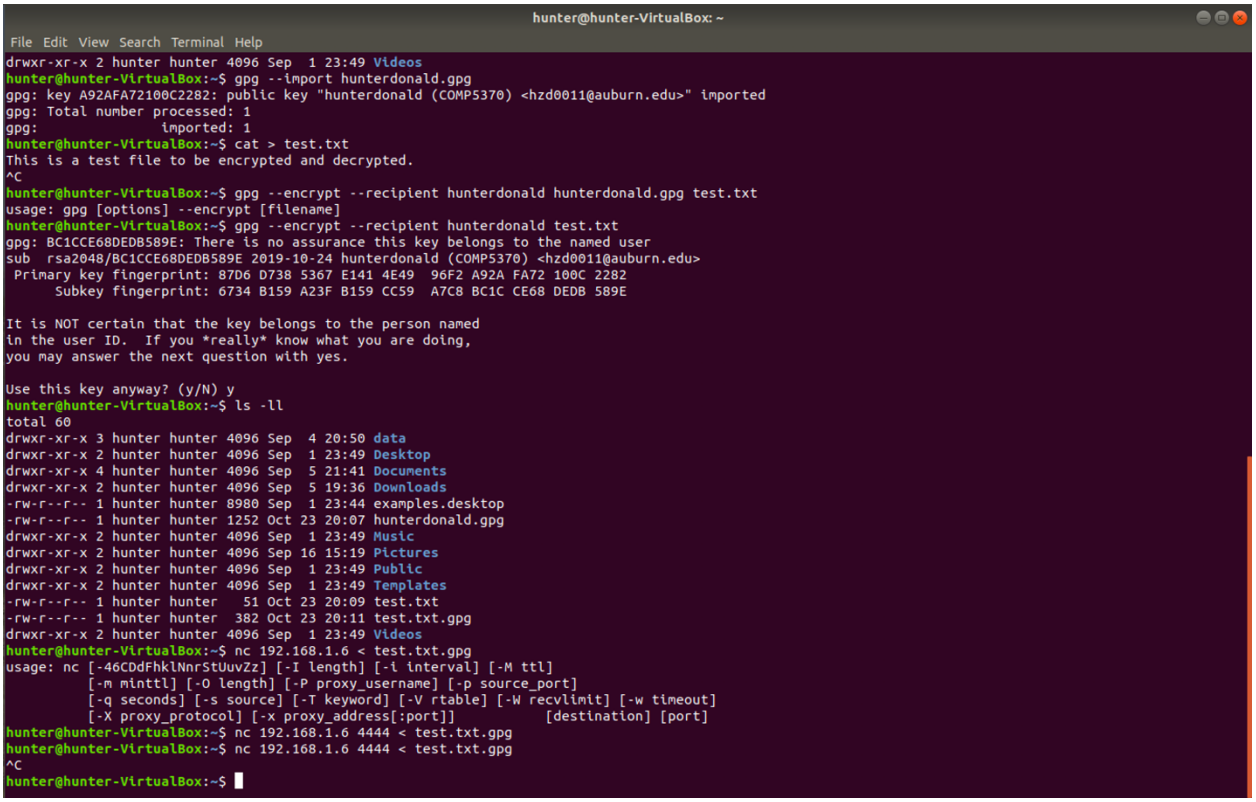
Hunter Donald
hzd0011
COMP 5370
Homework 3



Hunter Donald
hzd0011
COMP 5370
Homework 3



Hunter Donald
hzd0011
COMP 5370
Homework 3



3)

Original Data: 100110111010011

??1?001?10111010011

P_1 = ?101111101 = 1
P_2 = ?101010111 = 0
P_4 = ?0011101 = 0
P_8 = ?1011101 = 1

Encoded data: 10100011101110100 11

Hunter Donald
hzd0011
COMP 5370
Homework 3

4)

a. If the key is known, take the location in the alphabet of the first letter of the ciphertext and subtract the location of the first letter of the key from that. If the result is negative, add the length of the alphabet to the result. The result of the subtraction will be the location in the alphabet of the first deciphered letter. Repeat this for the second letter of the ciphertext and the second letter of the key, then the third, and so on until the entire key has been used. Once the entire key has been used, go back to the first letter of the key and keep going until all of the ciphertext is deciphered.

b.

i. For a known plaintext attack, the attacker has the original plaintext and the encrypted ciphertext. To determine the key, take the location of the first letter of the ciphertext and subtract the location of the first letter of the plaintext to get the location of the first letter of the key. If this value is negative, add the length of the alphabet to get the result. Repeat this for the second letter of the cipher text and plaintext, and so on until the entire key has been revealed. Once the key is revealed, the attacker is able to decrypt anything encrypted with that key using the same method described in problem 3 a.

ii. For a chosen ciphertext attack, the attacker can send the victim some ciphertext, and the victim will send back the plaintext. Now that the attacker has the ciphertext and its corresponding decrypted plaintext, the attacker can use the same method for a plaintext attack to determine the key.

iii. For a chosen plaintext attack, the attacker sends the victim some plaintext and the victim will send back the corresponding ciphertext. With this attack, the attacker is able to strategically choose the plaintext so that the key will be revealed more easily.

c.

i. The attack I used to break this cipher was a simple brute force attack where I tried every possible key.

ii. To determine the key, since the ciphertext has a fair amount of two letter words, I declared an array with some of the most common two letter words. I then used that array to count the number of unique common words in the plaintext from each key and chose the key which yielded the highest number of unique common words in its respective plaintext.

iii. Key: AUB
Deciphered text: TO BE OR NOT TO BE THAT IS THE QUESTION