Lab Report 7

1. Assessment Sheet
2. **If you and another person want to encrypt messages, should you provide that person with your public key, private key, or both**

In this case, we should provide our public key to another person.

1. **What does Kleopatra allow you to do once it is installed?**

Kleppatra allows us to generate private key and public key and also allow us to decrypt files by using those private key and public key.

1. **What key type was used to create the certificate on Kleopatra? What other types of encryption key types are possible?**

In this case, by default, Kleopatra use RSA 2048 bits key type and it also provide key type of DSA 2048 bits (Digital Signature Algorithm). Besides these two, we still have RSA 3072bits, RSA 4096bits, DSA3072bits, DSA4096bits.

1. **What was the fingerprint generated with your Kleopatra certificate?**

In Vworkstation desktop we have generated the following fingerprints

31187A9478768F7A2407139FF2F62891E1880C53

In the Vworkstation targetwindows01, we have generated the following fingerprints

CFD216DCCF22F72D94FFC41F6284F7933700C74C

1. **If someone sends you his public key and you import it into Kleopatra, will he be able to decrypt the encrypted messages you send him?**

Yes, of course, this is the symmetric encryption which both sides shared the same public key. So the receiver could use this public key to decrypt the message.

1. Challenge Questions

**Description: 1) what is the difference between RSA and DSA encryption; 2) Would it be possible to encrypt the secret-message.txt file using only the TargetWindows01 public key? What would be the ramifications of doing this?**

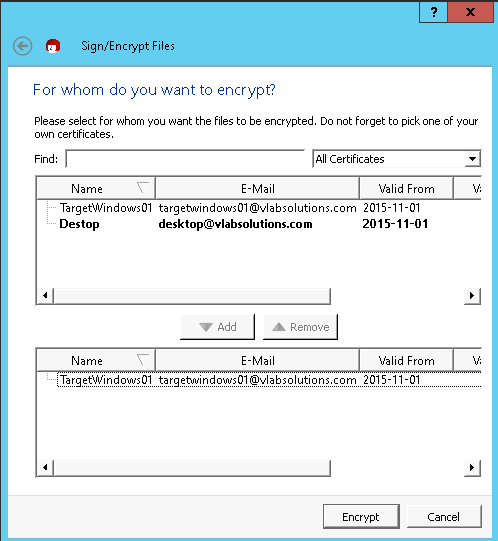
1. What the difference between RSA and DSA

The major difference of these two algorithm is that the speed of encryption and decryption. For RSA, it can encrypt at a relative faster speed but slower speed for decryption while for the DSA, it can decrypt at a relative faster speed but encrypt at a very slow speed.

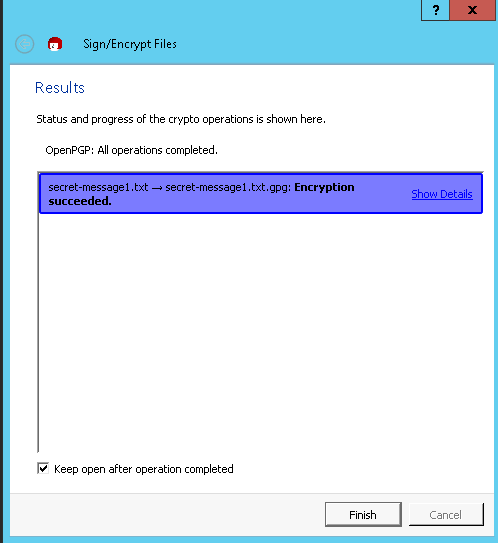
1. Would it possible for encrypt the secret-message.txt using only the targetwindows 01 public key

Yes, we could encrypt it along with targetwindows 01’s public key.

1. Select public key encryption



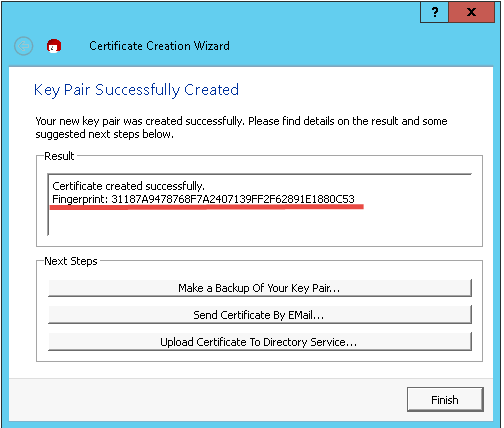
1. Successfully encrypted



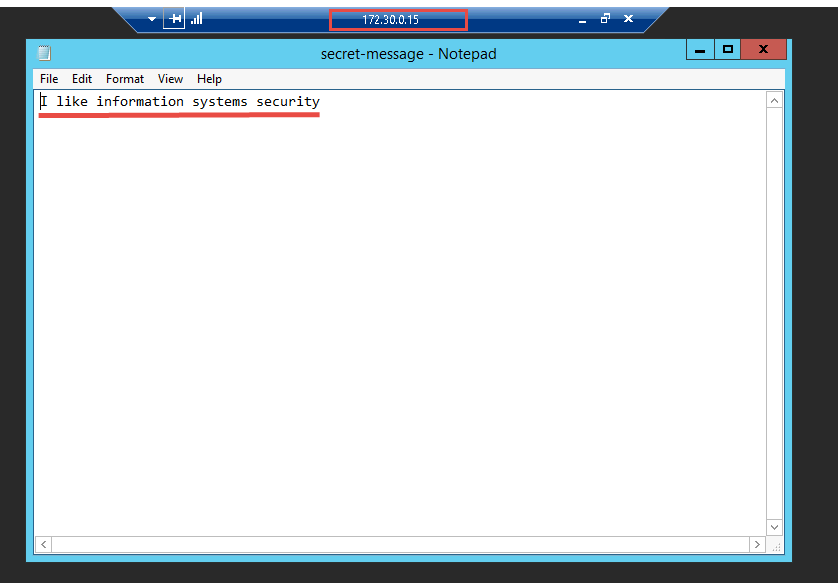
1. What ramifications of doing this (question 2’s action)

The problem of only using public key to encrypt file is that we cannot guarantee the authentication of the sender. It is vulnerable to man-in-the-middle attack. Thus, we should include the sender’s private key to verify the authentication in order to trust the sender.

1. Report Screenshot
2. Desktop certification fingerprints



1. Kleopatra decryption results



1. Other additional supporting text/image content

Lab Report 12

1. Assessment Sheet
2. **Compare the hash values calculated for Example.txt that you documented during this lab. Explain in your own words why the hash values will change when the data is modified.**

If the file data are not modified, the hash must be the same one that the first time generate hash value for the file. Because any hash algorithm has a property that the same file should have the same hash value no matter how many times we perform the same hash operations to the file. Actually, the hash value was calculated by a series of unique characteristics of the file like the length, size, and contents and so on. As a result, as long as these unique characteristics have been changed, the hash result obtained from the same hash function must be different.

1. **Why are the MD5sum and SHA1sum hash values the same every time you calculate for the example.txt file? What if it were different when you recalculated the hash value at the other end**

One of the most important reasons for using hash values is that no matter how many times we perform the same hash operations to a file or something else, the result should be stable unless there is any changes happened to that file. Because of this attribute, hash can be used as a best integrity checking tool. And, in addition, the hash value should be the same regardless of which end we use as long as we apply the same hash function.

1. **If you want secure e-mail communications without encrypting an e-mail message, what other security countermeasure can you deploy to ensure message integrity?**

In this case, we can use multiple hash functions to calculate several hash values for the original email message. And, we send these hash values to the receiver along with the mail message. When receiver received the message, he/she could run the same hash functions to calculate the hash value of the message. If the hash values are all match up with the hash values that are sent along with email, we can know that the email message doesn’t been corrupted and compromised while transmission.

1. **What is the –e switch used for with running the GnuPG command**
2. Extract
3. Encrypt data
4. Export

Answer: C

1. **What is the difference between MD5sum and SHA1sum hashing calculations? Which is better and why?**

MD5sum uses 128-bit hash while SHA1sum uses 160-bit hash, which means that the SHA1sum are much slower to calculate.

1. **Name the cryptographic algorithms used in this lab**

MD5 and SHA1

1. **What do you need if you want to decrypt encrypted messages and files from a trusted sender?**

If the senders has been trusted, as receiver only need to use his/her private for decrypting the message.

1. **What is the –d switch used for when running the GnuPG command?**
2. Detach
3. Destroy
4. Decrypt data

Answer: C

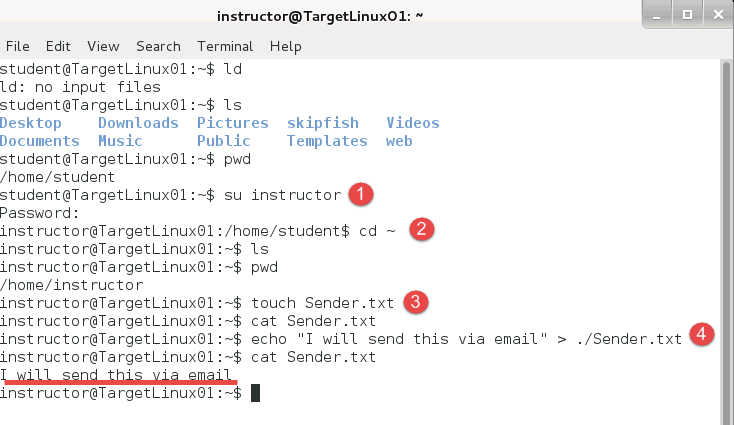
1. **When creating a GnuPG private key, what are ways to create entropy?**

In this case, we use “find \* / && find \* / ” command to generate enough random numbers so that the private key can be created.

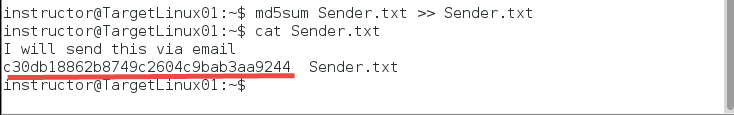
1. Challenge Questions

**Description: create a new text file call Send.txt, apply an MD5 hash to the file, and then use GnuPG to encrypt and decrypt it.**

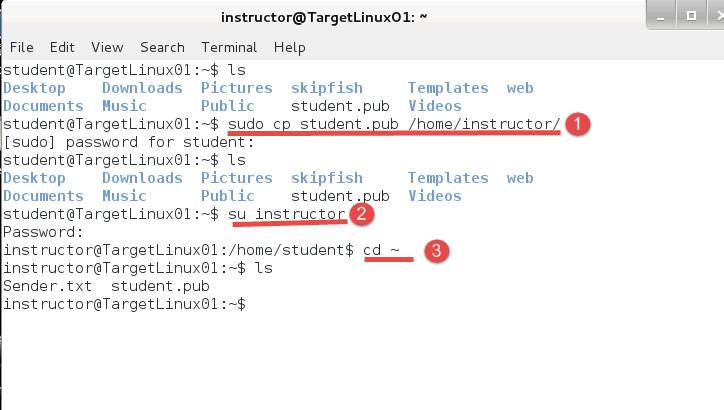
1. Create a file named “Sender.txt” and insert lines to that file



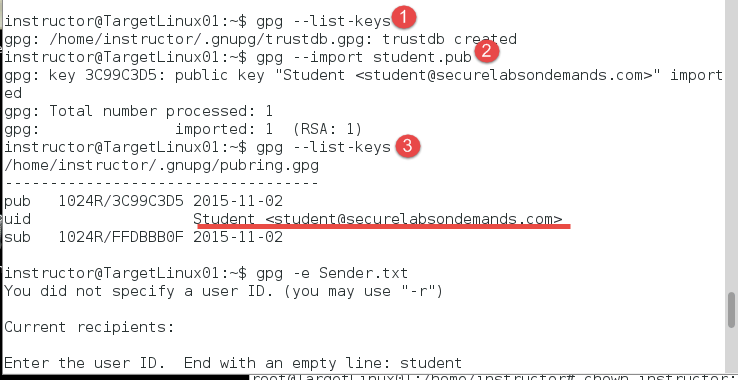
1. Add an MD5sum hash to the file

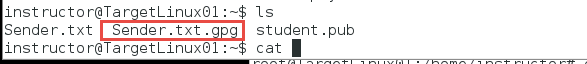


1. Share student public key with the instructor account, so the instructor can send encrypted messages to the student



1. Using the instructor’s account, encrypt Send.txt using GneuPG

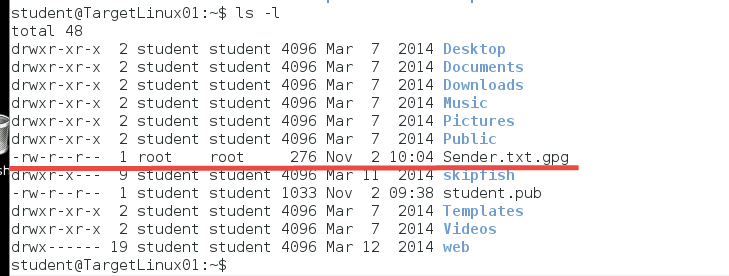




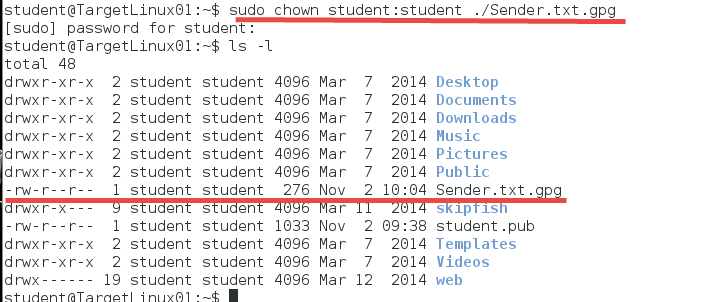
1. Copy the file to student’s home folder, change permissions on the file, and then decrypt Send.txt using the student account.
2. Copy encrypted txt file to student home.



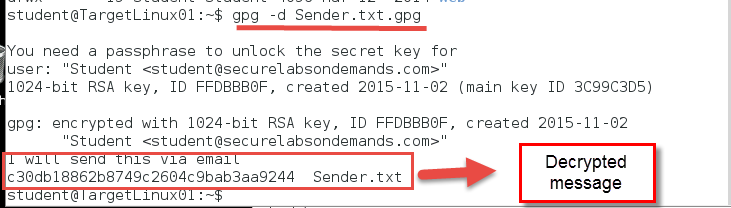
1. View the permission of Sender.txt.gpg



1. Change permissions to student:student of Sender.txt.gpg



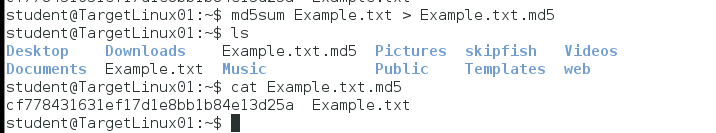
1. Decrypt the encrypted message



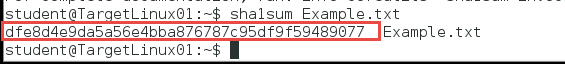
1. Report Screenshot
2. Md5sum of Example.txt



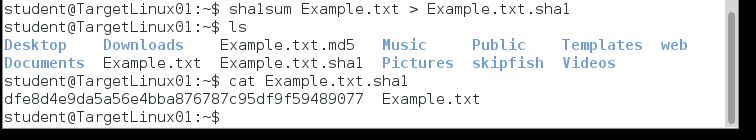
1. Contents of Eample.txt.md5



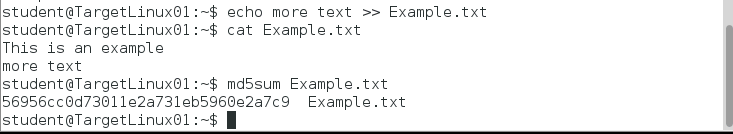
1. SHA1sum hash strings



1. Contents of Example.txt.sha1



1. MD5sum hash string



1. SHA1sum hash string



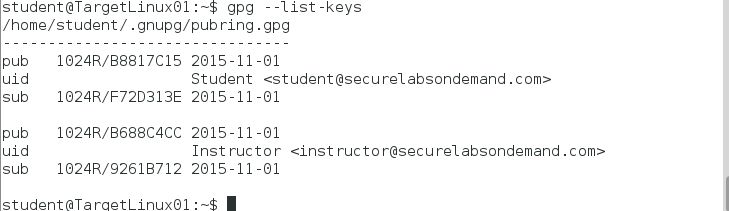
1. Content of /home/student



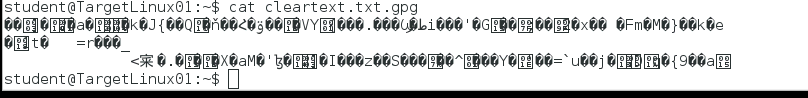
1. Content of /home/instructor



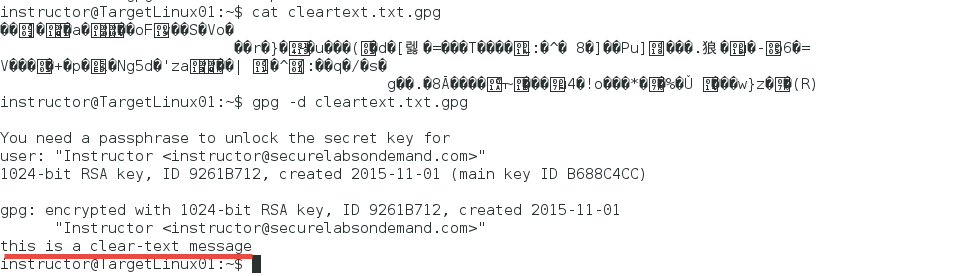
1. GnuPG keys



1. Content of the encrypted file



1. Contents of the cleartext.txt.gpg



1. Other additional supporting text/image content