CSEC 101 Lab 5: Using PKI – Lab Report

Name: Sanchit Monga

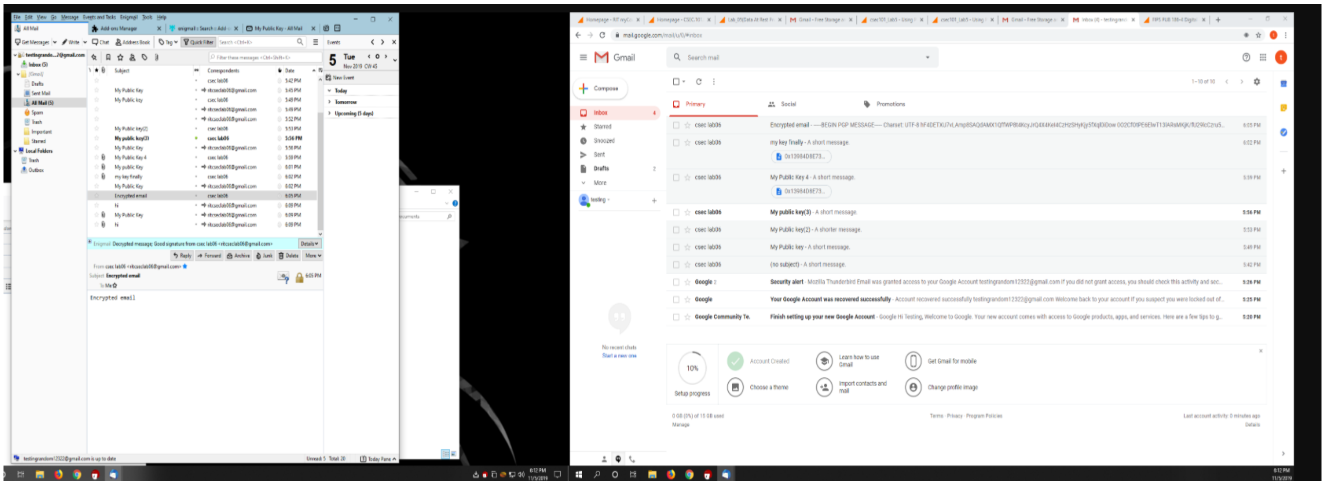
Activity 2 – Set up your email   with your partner

1. (5 points) What is Gpg4win? And very briefly specify why is Gpg4win used?
   It is an email and file encryption package which uses GnuPG public key cryptography for data encryption and digital signatures.
   It is used for encryption.

2. (5 points) What is Thunderbird? And very briefly specify why is Thunderbird used?
   Thunderbird is the free opensource, cross-platform application for managing email, news feeds, chats and new groups.
   It is a local email application rather than a browser and is easier to use.

3. (5 points) What is Enigmail? And very briefly specify why is Enigmail used?
   Enigmail is an add-on to the Thunderbird software which allows users to access the authentication and encryption features provided by GnuPG.
   It is used to access the encryption features of GnuPG.

4. (5 points) Provide screen shots of your email app in the web browser and in Thunderbird



Subject	Correspondents	Date
	csec lab06	5:42 PM
My Public Key	ritcseclab06@gmail.com	5:45 PM
My Public key	csec lab06	5:49 PM
	ritcseclab06@gmail.com	5:49 PM
	ritcseclab06@gmail.com	5:52 PM
My Public key(2)	csec lab06	5:53 PM
My public key(3)	csec lab06	5:56 PM
My Public Key	ritcseclab06@gmail.com	5:58 PM
My Public Key 4	csec lab06	5:59 PM
My public Key	ritcseclab06@gmail.com	6:01 PM
my key finally	csec lab06	6:02 PM
My Public Key	ritcseclab06@gmail.com	6:02 PM
Encrypted email	csec lab06	6:05 PM
hi	ritcseclab06@gmail.com	6:09 PM
My Public Key	ritcseclab06@gmail.com	6:09 PM
hi	ritcseclab06@gmail.com	6:09 PM

Enigmail Decrypted message; Good signature from csec lab06 <ritcseclab06@gmail.com>

From csec lab06 <ritcseclab06@gmail.com>
Subject Encrypted email
To Me
6:05 PM

```
Encrypted email
```

csec lab06	Encrypted email - -----BEGIN PGP MESSAGE----- Charset: UTF-8 hF4DETXU7vLAmp8SAQdAMX1QfWP8t4KcyJrQ4X4Kel4CzHzSHyKjy5fXql0iDow 0O2Cf0tPE6EIwT13lARsMKjK/fU29lcCzru5...	6:05 PM
csec lab06	my key finally - A short message. 0x13984D8E73...	6:02 PM
csec lab06	My Public Key 4 - A short message. 0x13984D8E73...	5:59 PM
csec lab06	My public key(3) - A short message.	5:56 PM
csec lab06	My Public key(2) - A shorter message.	5:53 PM
csec lab06	My Public key - A short message.	5:49 PM
csec lab06	(no subject) - A short message.	5:42 PM
Google 2	Security alert - Mozilla Thunderbird Email was granted access to your Google Account testingrandom12322@gmail.com If you did not grant access, you should check this activity and sec...	5:26 PM
Google	Your Google Account was recovered successfully - Account recovered successfully testingrandom12322@gmail.com Welcome back to your account If you suspect you were locked out of...	5:25 PM
Google Community Te.	Finish setting up your new Google Account - Google Hi Testing, Welcome to Google. Your new account comes with access to Google products, apps, and services. Here are a few tips to g...	5:20 PM

5. (7.5 points) When Encrypting the email, you send to your partner, what key did you use?
   I used my private key to encrypt the email.

6. (7.5 points) When your partner Decrypted the email you just sent, which key did the partner use?
   My partner used my public key to decrypt the email.

For question 7. – 8. use FIPS PUB 186-4 Digital Signature Standard.pdf provided, see section 3, "General Discussion". If using different references, then cite references used for researching this question and what steps you used to verify the information'

7. (7.5 points) When signing the email, you send to your partner, what key did you use?
   I would use my private key to sign the email.

8. (7.5 points) When your partner verified the signature of the email you just sent, which key did the partner use?
   To verify my signature my partner will use my public key.

9. (20 points) Explain why there is a difference between how the Key pair, Private & Public keys, are used for encryption and for signature. And explain how these two methods reduce the risks of network security vulnerabilities and threats
   The public key of the recipient can be used to encrypt the message, which is in turn decrypted using a private key. Secondly, public key cryptography is used as digital signatures.
   The digital signature includes a signature generation process and a signature verification process. The public key can be shared with everyone, whereas the private key must be kept secret. The RSA encryption algorithm is the most widely used public key algorithm, partly because both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it.
   This reduces the risks of network security vulnerabilities and threats.

10. (10 points) How was Confidentiality implemented?
    Confidentiality was implemented by encrypting the email.

11. (10 points) How was Integrity implemented?
    Integrity was accomplished when the message was encrypted and signed by the sender and verified by the receiver using the private and public keys.

12. (10 points) How was Non-Repudiation implemented?
    Non-Repudiation was accomplished as email was signed by the end user which verifies that email was sent by him.