The University of Newcastle
School of Information and Physical Sciences

SENG2250/6250 System and Network Security
Week 12 Lab

Part 1: Internet Protocol Security

Internet Protocol Security (IPSec) is a comprehensive suite of protocols and standards used to secure and protect data transmitted over IP networks, including the internet. It plays a vital role in ensuring the ***confidentiality***, ***integrity***, and ***authenticity*** of data as it travels across potentially untrusted networks.

Key features of IPSec include:

1. **Authentication**: IPSec allows systems to verify the identity of communicating parties, ensuring that data is exchanged between trusted sources.
2. **Encryption**: It provides robust encryption mechanisms to safeguard the confidentiality of data, making it unintelligible to unauthorized parties.
3. **Data Integrity**: IPSec verifies that data remains unaltered during transmission, protecting against unauthorized modifications.
4. **Access Control**: It enables control over who can access network resources and data, enhancing network security.

IPSec is often used for setting up Virtual Private Networks (VPNs) to create secure, encrypted connections over the internet, enabling safe remote access to corporate networks or securing data transfers between sites. In summary, IPSec is a crucial component of network security, enhancing the protection of data in an environment where security and privacy are paramount concerns.

Work with your lab demonstrator to answer the following questions:

Q1. What are the two security protocols defined in IPSec?

Q2: What are the security services provided by IPSec?

Q3: Can we use IPSec to protect the MAC information of a user?

Q4: What are the IPSec transport mode and tunnel mode? What are the differences?

Q5: Why does ESP include a padding field?

Q6: What is a security association?

Q7: Explain the entries in the following table.

Protocol	Source IP	Source Port	Destination IP	Destination Port	Action	Comments
TCP	10.1.2.156	*	10.1.2.132	80	Bypass	Unprotected traffic
TCP	10.1.2.156	*	10.1.2.133	443	Bypass	-
ICMP	10.1.2.156	*	*	*	Bypass	Error messages
*	10.1.2.156	*	*	*	Protected: ESP transport-mode	Encrypted traffic
*	10.1.2.156	*	10.1.2.10	*	Discard	-

Part 2 Pretty Good Privacy (PGP) - not examinable

Pretty Good Privacy (PGP) for Email Security: PGP is an encryption and authentication program that provides a high level of email security. It was created to address the need for secure and private email communication in an age of digital information sharing.

Key aspects of PGP for email security include:

1. **End-to-End Encryption**: PGP uses a combination of public and private keys to encrypt email messages. The sender uses the recipient's public key to encrypt the message, and only the recipient's private key can decrypt and read it. This ensures that even if intercepted during transmission, the email remains secure.
2. **Digital Signatures**: PGP allows users to digitally sign their emails using their private key. This signature verifies the sender's identity and ensures that the email content has not been tampered with during transit.
3. **Key Management**: Managing PGP keys is crucial for security. Users must safeguard their private keys and share their public keys with trusted contacts. Public key servers help in distributing and discovering public keys.
4. **Open Source**: PGP is an open-source technology, meaning its source code is accessible and can be audited for security. There are various email clients and tools that support PGP, making it accessible to a wide range of users.

PGP is widely used by individuals and organizations to protect the confidentiality and integrity of their email communications. It provides a robust defence against eavesdropping, data breaches, and unauthorized access to sensitive information, making it an essential tool for email security in the digital age.

In this part of the lab, you will use PGP to improve email security. This part uses an online PGP tool: https://pgptool.org/

Task 1: Create Public/Private Key Pair for PGP

PGP needs to perform public-based encryption and digital signature for data security. To use public key based cryptographic algorithms, it is required to create your public and private keys. In PGP, you will have different key generation options which depend on the different cryptographic algorithms. In this task, we will create your RSA keys.

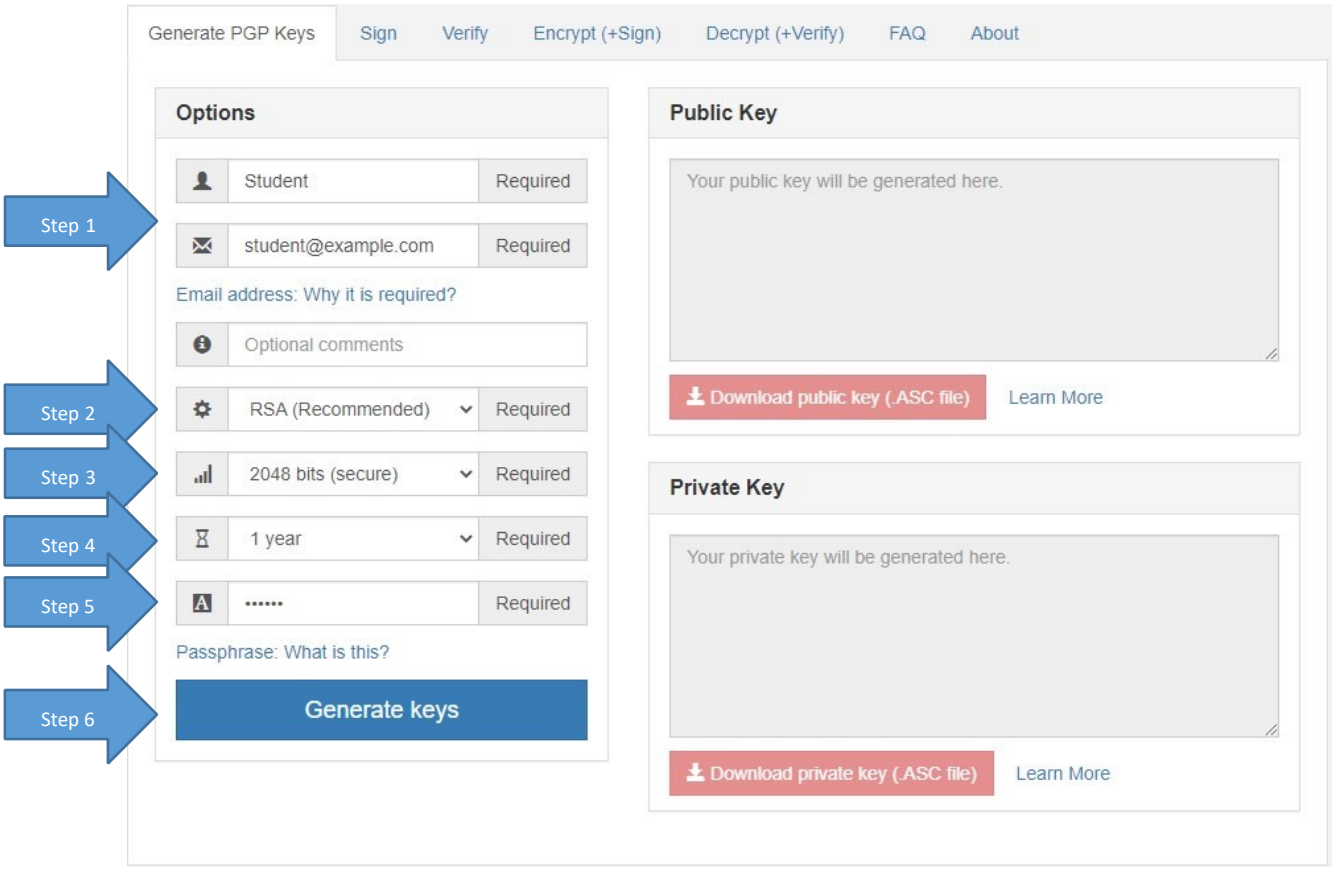

Figure 1. Public and private key generation

1. Select “Generate PGP Keys”.
   Enter the name “Student” and email address “student@example.com” (Figure 1). **Do not use your real name or email address**.
2. Select “RSA (Recommended)” as the cryptographic algorithm.
3. Select “2048 bits (secure)” as the size of the RSA public and private keys.
4. Select “1 year” for the expiry duration.
5. Choose a passphrase.
   A high-quality password can significantly improve the security of the keys. You will need to use it later, so write it down.

Where will the passphrase be used and how?

6. Click “Generate keys”.
   This step creates a kind of “certificate” (ASC files) of your public key.
7. Download the public key file to the Downloads folder and rename it to “student-pub.asc”.
8. Download the private key file to the Downloads folder and rename it to “student-sec.asc”.

Task 2: Generate Public and Private Keys for a Receiver

To use PGP for email transmission, you need to have sender/recipient public keys. In practice, public key information is exchanged before the sending/receiving. In this task, we create a dummy user to demonstrate it locally.

Repeat the steps of task 1 to generate public and private keys for user "**receiver**" and email address "**receiver@example.com**". You should create the following two files at the end.

- Public key file: receiver-pub.asc
- Private key file: receiver-sec.asc

Task 3: Encrypt and Sign a Message

1. Create a text file "t4sec.txt" on the Desktop. Enter any message then save the file.
2. On the website, select "Encrypt (+Sign)" and choose the receiver's public key (receiver-pub.asc), the signer's private key (student-sec.asc) and the plaintext file (t4sec.txt) as in Figure 2.
3. Enter the passphrase of the **Student** and click "Encrypt the message".
4. Download the encrypted message.

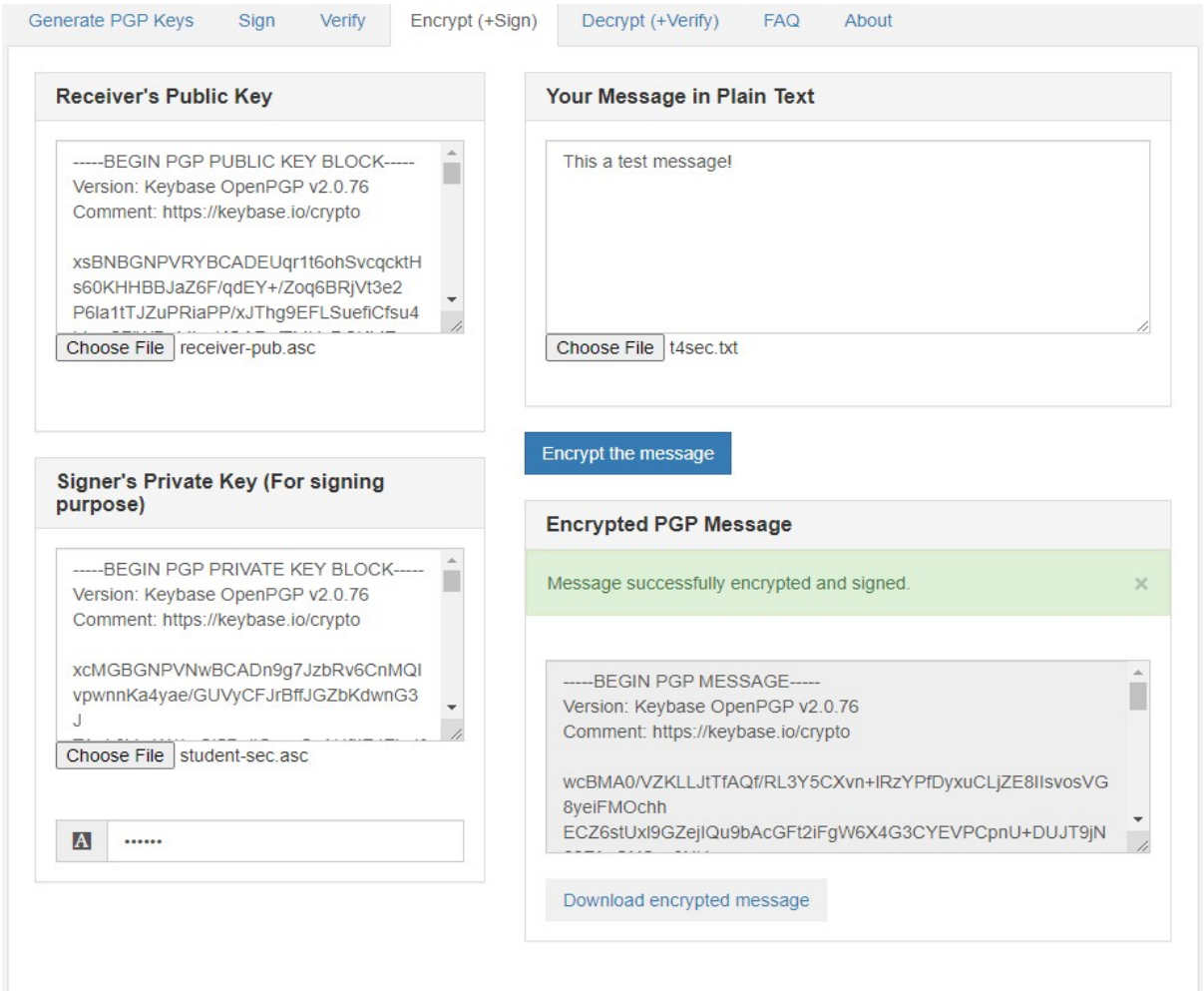

Figure 2. Sign and encrypt a message

Task 4: Encrypted Email

In Task 3, the file "t4sec.txt" has been encrypted and signed. The protected file

“t4sec.txt.encrypted_and_signed.txt” can be sent as an attachment of an email for security protection. In this case, the sender must write email content to the t4sec file.

Your task: Select the “Decrypt (+Verify)” tab on the website. Make sure the corresponding files and information are provided. **Then, decrypt and verify the “t4sec.txt.encrypted_and_signed.txt” file to recover the text message.**

Task 5: Send an Email to Peer

Find another student in your lab and send an encrypted email via your university email address.

- Discuss what should be prepared before sending an email and how to use the provided website to generate and read the messages.
- Discuss how you decide the trust of the sender and receiver’s public keys. Is that the same as in the PKI system?

Part 3: Assignment 3 Help