MIT World Peace University

Information and Cyber Security

Assignment 8

Naman Soni Roll No. 10

Contents

1 Aim

Demonstrate Email Security using: PGP or S/MIME for Confidentiality, Authenticity and Integrity.

2 Objectives

To learn secure email communication

3 Theory

The steps for secure email message exchange using PGP:

- Install PGP software: Install PGP software on your computer. There are many different PGP software programs available, such as GnuPG or Symantec Encryption Desktop.
- Generate public and private keys: Generate a pair of public and private keys using the PGP software. The private key should be kept secret and protected with a strong passphrase, while the public key can be shared with others.
- Generate public and private keys: Generate a pair of public and private keys using the PGP software. The private key should be kept secret and protected with a strong passphrase, while the public key can be shared with others.
- Share public keys: Share your public key with the person you want to exchange encrypted emails with, and ask them to share their public key with you.
- Import public keys: Import the public keys of the people you want to communicate with into your PGP software.
- Compose the message: Compose the message you want to send using your email client.
- Encrypt the message: Use your PGP software to encrypt the message using the public key of the recipient. This will ensure that only the recipient with the corresponding private key can read the message.
- Sign the message: Sign the encrypted message using your private key. This will allow the recipient to verify that the message came from you and has not been tampered with.
- Send the message: Send the encrypted and signed message using your email client.
- Receive and decrypt the message: When you receive an encrypted and signed message from someone, use your PGP software to decrypt the message using your private key, and verify the signature using the sender's public key.

4 Programming Language Used

Python

5 Conclusion

Thus, we learned how to use PGP in python.

6 FAQ's

6.1 How email security is provided through PGP?

Ans.

- PGP (Pretty Good Privacy) provides email security through a combination of encryption, digital signatures, and compression. When a user sends an email using PGP, the message is encrypted using a symmetric key algorithm.
- The symmetric key is then encrypted using the recipient's public key, which is obtained from a key server or a public key directory. The encrypted message and the encrypted symmetric key are then sent to the recipient, who can decrypt the message using their private key.
- PG also allows users to sign their emails digitally using their private key. The digital signature provides a way for the recipient to verify that the email was actually sent by the claimed sender, and that it has not been altered in transit.
- In addition, PGP can compress the message before encryption, which can reduce the size of the message and make it easier to send over a slow or unreliable connection.

6.2 What type of encryption is PGP?

Ans. PG uses a combination of symmetric and asymmetric encryption. The symmetric encryption algorithm is used to encrypt the message itself, while the asymmetric encryption algorithm is used to encrypt the symmetric key.

The symmetric encryption algorithm used in PG is typically AES (Advanced Encryption Stan-dard), which is a widely used and highly secure algorithm. The asymmetric encryption algorithm used in PG is typically RSA (Rivest-Shamir-Adleman), which is also widely used and highly secure.

6.3 What is the key size allowed in PGP

Ans. PG supports a wide range of key sizes, from 512 bits to 4096 bits. The key size determines the level of security provided by the encryption algorithm.

In general, larger key sizes provide stronger security, but they also require more processing power to encrypt and decrypt the data. For most purposes, a key size of 2048 bits is considered to be sufficient, but some applications may require larger key sizes for enhanced security.