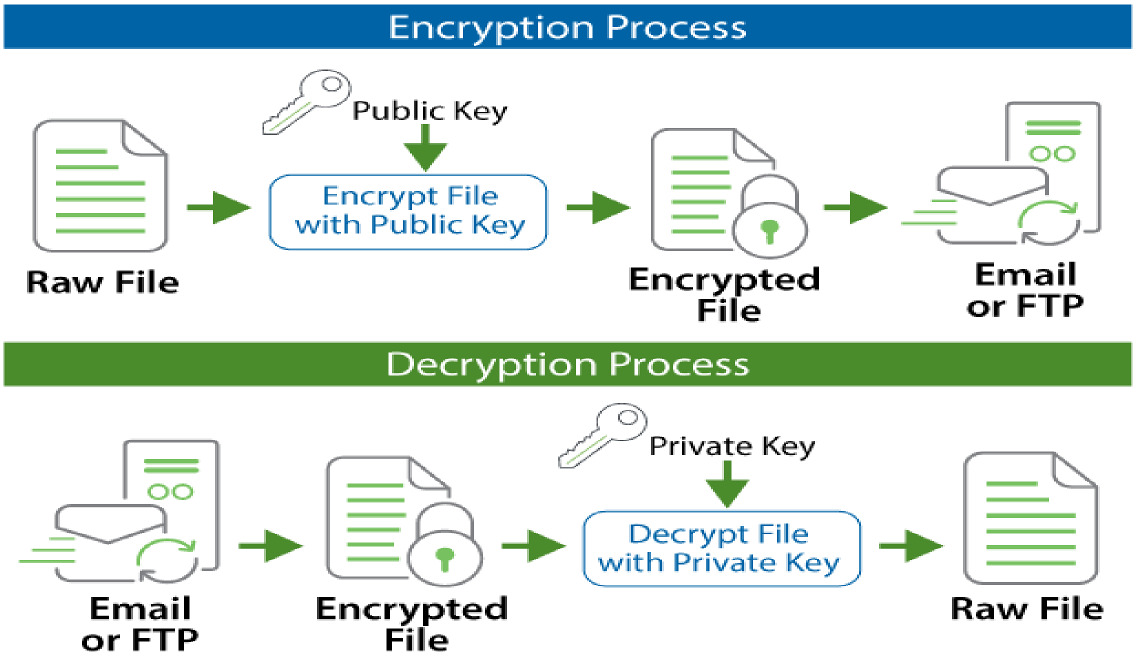
Network Security - C2 Assignment 3
Date: 25-10-20
Group Number-23

Soumyadeep Basu, Kumar Utkarsh, Rohit Haolader, Raushan Raj, Suryasen Singh

Key Management in PGP and S/MIME

What is PGP encryption-

PGP stands for **P**retty **G**ood **P**rivacy and it allows people to communicate privately online. When you send a message to someone using PGP, the text is first converted to a ciphertext which can be accessed only by a key. This key is present with the receiver who is able to convert the ciphertext back to the intended text.PGP uses a combination of **symmetric key encryption** (i.e., a single-use session key encrypts and decrypts the message) and **public key encryption** (i.e., the keys unique to the recipient encrypt and decrypt the session key).



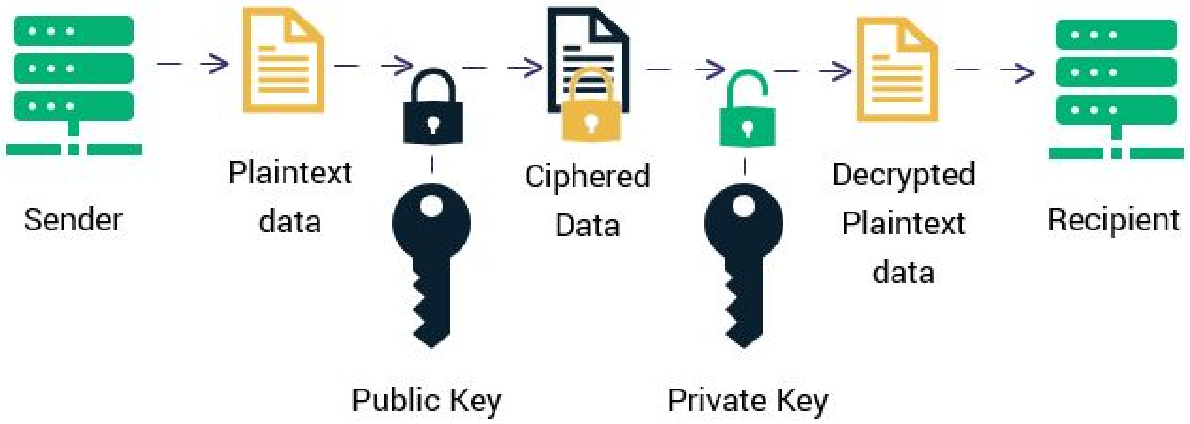
Given below are the methods in which PGP uses the keys-

1. The first thing PGP does is generate a random session key.
2. Next, the session key is encrypted using the recipient's public key.
3. When the recipient receives an encrypted message, they decrypt the session key using their private key. The plaintext session key then decrypts the message.
4. PGP combines the efficiency of symmetric encryption and the convenience of public key encryption.
5. A digital signature proves to the recipient that an attacker has not manipulated the message or the sender.

What is S/MIME encryption-

S/MIME is based on asymmetric cryptography that uses a pair of mathematically related keys to operate – a public key and a private key. It is computationally infeasible to figure out the private key based on the public key. The email can only be decrypted with the corresponding private key, which is supposed to be in sole possession of the recipient. S/MIME also allows you to leave your digital signature on your mail so that when the recipient uses your public key for decrypting it, they are able to verify that the email really came from you.

S/MIME provides the authentication, message integrity and non-repudiation of origin and data security services for electronic data transmission applications.



Although PGP and S/MIME are pretty similar in their working, they have differences in the method of handling the keys. The differences are as follows

1. PGP allows one user to directly give a public key to another user or vice versa. In PGP each user is allowed to decide the length of trust in the received keys. In S/MIME , the sender or receiver does not reply on exchanging the keys in advance and share a common certifier on which they rely.
2. Since PGP protocol was developed to handle plain email or text messages and depends on each user's key exchange. S/MIME uses hierarchically validated certifier for key exchange.
3. PGP contains 4096 public keys whereas S/MIME has 1024 public keys.