SENG2250/6250 System and Network Security
Self-Quiz Week 12, Semester 2, 2020

True/False Questions

1. SMTP is a protocol to send and retrieve emails.
   False. SMTP stands for Simple Mail Transfer Protocol. It sends an email to the receiver's mail server. The receiver needs to use POP (Post Office Protocol) or IMAP (Internet Mail Access Protocol) protocols to retrieve emails.

2. A web-based email system can use TLS/SSL, such as https://mail..., to provide end-to-end security that the email is readable to the sender and receiver only.
   False. It is not end-to-end secure. "https" links establish a secure channel between a client (sender or receiver) and the mail server. The mail server can have the key to decrypt and read the data (email). PGP (Pretty Good Privacy) is a candidate for end-to-end secure email systems.

3. PGP proceeds an email in the order of "sign-compress-encrypt".
   True.

4. PGP client maintains two key rings: the private key ring and the public key ring.
   True.

5. S/MIME uses the web of trust model to manage the trustworthiness of public keys.
   False. S/MIME uses X.509 v3 certificates to verify public keys. It relies on the public key infrastructure. PGP, instead, uses web of trust model for public key management.

Short-Answer Questions

6. Briefly describe the public key management system of PGP.
   - Each PGP user assigns a trust level to other users (Owner Trust Field)
   - Each user can certify (sign) the public keys of users he/she knows.
   - In the public key ring, each entry stores a number of signatures that certify this public key.
   - PGP automatically computes a trust level for each public key (Key Legitimacy Field) in the key ring.