CS361 Questions: Week 12

These questions relate to Modules 15. Type your answers and submit them on Canvas.

Lecture 66

1. What is PGP?
2. What motivated Phil Zimmerman to develop it?
3. Does PGP provide effective security?
4. If PGP is freeware, why would anyone bother to purchase support?

Lecture 67

1. Explain the PGP authentication protocol.
2. Explain the PGP confidentiality protocol.
3. How do you get both authentication and confidentiality?

Lecture 68

1. Besides authentication and confidentiality, what other "services" does PGP provide?
2. Why is compression needed?
3. Why sign a message and then compress, rather than the other way around?
4. Explain radix-64 conversion and why it's needed?
5. Why is PGP segmentation needed?

Lecture 69

1. What are the four kinds of keys used by PGP?
2. What special properties are needed of session keys?
3. How are session keys generated?

4. Assuming RSA is used for PGP asymmetric encryption, how are the keys generated?

5. How are the private keys protected? Why is this necessary?

6. Assume principals user, key-server, and database. Write in protocol notation the protocol for sending to the database a newly generated and encrypted (with the passphrase-based key) private key. Assume the user supplies the passphrase, and the key-server generates and encrypts the new private key

Lecture 70

1. If a user has multiple private/public key pairs, how does he know which was used when he receives an encrypted message?

2. What's on a user's private key ring?

3. What's on a user's public key ring?

4. What are the steps in retrieving a private key from the key ring?

5. What is the key legitimacy field for?

6. How is a key revoked?