Week 12 Questions

Lecture 66

1. PGP is Pretty Good Privacy. It uses the best available cryptographic algorithms as building blocks integrated into a general-purpose algorithm that is processor-independent and easy to use.
2. Zimmermann had a strong distrust of the government and believed everyone had an absolute right to privacy.
3. It is extremely secure. In 2003 and 2006, government agencies were unable to crack PGP-encrypted files from seized electronics.
4. You would purchase it so that you know that the software has is authentic. Companies also want a physical entity to call up incase of maintenance and troubleshooting issues.

Lecture 67

1. Sender creates and hashes a message. Then it signs it with its private key and adds it to the hashed message. Receiver decrypts with sender's private key, and creates a new hash code and compares it to the sender's hash code.
2. Sender creates a message and session key. The key is encrypted with the receiver's public key and added to message. Receiver decrypts the session key with its private key and uses that to recover the message.
3. Apply authentication to the original message and confidentiality to the resulting message.

Lecture 68

1. Compression, email compatibility, segmentation.
2. A message may be very large. It is used to save bandwidth.
3. Encryption after compression is stronger because compression reduces redundancies.
4. Radix-64 maps groups of three octets into four ASCII characters expanding the message by 33%. Ensures that your system does not interpret a character as a command and vice-versa, since not all systems are the same.
5. Some mailers limit the message length/email size.

Lecture 69

1. Session keys, public keys, private keys, passphrase-based key.
2. High entropy (random-appearing and not guessable).
3. Session keys are randomly generated bit strings. Takes the previous session key and uses keystroke timing and movement of the mouse.
4. Generate two large prime numbers not guessable to the attacker.
5. User selects a passphrase for encrypting private keys. Even if the attacker can access your computer, they can't use the key because it is encrypted and the decryption key is not stored anywhere on disk.
6. S -> R: $\{K\}_{SHA(passphrase)}$

Lecture 70

1. An ID is generated for each key pair. This ID is sent with the encrypted message and an associative search is used to find the key.
2. Timestamp, key ID, public key, private key, user ID
3. Timestamp, key ID, public key, user ID
4. Use key ID to retrieve the encrypted private key then recover the unencrypted private key with the passphrase. This is then used to recover the session key and decrypt the message.
5. Indicates how much you trust the key belongs to who it says it belongs to.
6. A key revocation certificate is sent out. Recipients are expected to update their public-key rings.