**Quiz 2/22**

**Q)**

1. **Signer has \_\_\_\_\_ Key?**
2. **What to send to the receiver?**

**A)**

1. Signer has Private Key
   1. Data
      1. Data is the actual information that the sender wants to transfer
   2. Digest (Hash of the data)
      1. By sending a digest the receiver can verify that the data received is the same as the data that was sent, this is used to eliminate corruption and detect tampering
   3. Digital signature
      1. The digital signature is used to verify integrity, authenticity, and non-repudiation
   4. Public key
      1. It is asymmetric cryptography used to encrypt messages which can only be decrypted with a private key