Lesson 8 Security Objectives

You can use cryptography to address many security objectives. Specifically, it offers the following capabilities:

- **Privacy or confidentiality:** Cryptography scrambles information so that only someone with the right cipher and key can read it. Note that this person could include a cryptanalyst.
- **Integrity:** Cryptography protects integrity by providing checksums or hashes. These can be compared against a known table of good values to prove the data has not changed.
- **Entity authentication or identification:** A person with the cryptographic key can encode or decode a message. If a business relationship requires that this key remain a secret, possession is proof of a valid identity.
- **Message authentication:** Similar to entity authentication, a coded message with a private key proves the identity of the writer of the message. Again, this stipulation should be part of any business contract or formal relationship.
- **Signature:** Cryptography provides a way to make a digital signature, which proves that a given person sent a specific message.
- **Access control:** Cryptography enables a person to encrypt privileged resources or data so that only authorized people can decrypt them.
- **Certification:** A trusted entity can certify a message or data by adding a cryptographic checksum and a digital signature.
- **Time stamping:** Using asymmetric key cryptography, a trusted device can issue time stamps that cannot be forged. Time stamping binds a hash of the time-stamped information with the output of a secure, reliable clock.
- **Witnessing:** A third party can add a cryptographic checksum to data to prove it exists in a given format at a particular time.
- **Ownership:** A cryptographic hash can be created by an owner of the data, added to the data, and then submitted to a trusted third party for corroboration. This identifies an entity as the data’s owner.
- **Anonymity:** Using cryptography, a person can conceal the identity of an entity by passing information in an encrypted format that monitors cannot interpret. Also, using a series of encrypted “hops” and getting rid of logs can provide an entity with anonymous presence on the Internet.
- **Nonrepudiation:** An asymmetric key signature of data, agreed to as part of a business relationship, can prove the sender’s identity to the receiver.