




Chapter 5 - Key Terms

 Term	 Page	 Summary
<u>Block Ciphers</u>	578	A symmetric key cipher that operates on a group of bits called a block. The same key is used to encrypt and decrypt.
<u>Symmetric Algorithms</u>	588	An encryption algorithm that uses the same key to encrypt and decrypt.
<u>Asymmetric Algorithms</u>	578	An encryption algorithm that uses two different keys: private & public, these make a key-pair.
<u>Hashing Algorithms</u>	582	An algorithm used to verify data integrity.
<u>Digital Certificates</u>	580	A digital entity used to verify that the user is who he or she claims to be and provide the receiver a means to encode a reply. Can apply to systems as well.
<u>Certificate Authority</u>	579	A system that generates and issues digital certificates to users and systems.
<u>Advanced Encryption Standard (AES)</u>	577	A symmetric-key encryption algorithm used by most modern crypto implementations. Defined in FIPS PUB 197: "Advanced Encryption Standard (AES)" and ISO/IEC 18033-3: "Block Ciphers".
<u>Online Certificate Status Protocol (OCSP)</u>	585	A protocol used to perform certificate validation.