ITBU 443: Treats and Counter Measures, Homework 02

Chapter 02, *Computer Security, Principles and Practices*

Readings

Read chapter 02 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. Describe the five ingredients of a *symmetric encryption* scheme.
2. What are the two requirements for strong symmetric encryption?
3. What is the difference between a *block cipher* and a *stream cipher*?
4. What is a typical use for a stream cipher?
5. Explain why a one way hash function is so useful in computing.
6. How would you use a password hashing scheme? If you can't read the password, what good is it?
7. (Not in book) Your grandmother has asked you to explain the Diffie-Hellman algorithm. How would you explain it to her in simple terms?
8. List the six requirements for public key cryptography.
9. Name three uses of a digital signature.
10. What is the X.509 standard?
11. Give one example of harm caused by the failure of a system to encrypt data that is not in the book.