ITBU 443: Threats and Counter Measures, Homework 15

Chapter 21, *Computer Security, Principles and Practices*

Readings

Read chapter 21 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. (Not in book) When we say that a hash function is a "one way function" or a "trap door function," what do we mean?
2. Explain this formula, using the definition of the symbols as shown in the book:

$$C_i = b_{i1} \oplus b_{i2} \oplus \ldots \oplus b_{im} \tag{1}$$

3. How do SHA-256, SHA-384, and SHA-512 differ?
4. In the description of SHA-512, the book contains this statement: "The message is padded so its length is congruent to 896 modulo 1024 [length $\equiv$ 896 (mod 1024)]" How is the value 896 calculated?
5. The book discusses MAC, or *message authentication code*. What is the purpose of MAC? Why is it important?
6. What is a *birthday attack*? What is a good defence against it?
7. Message encryption has addressed confidentiality and integrity separately. (a) Why was this true? (b) Why us it good to address both together? (c) What is significant about *authenticated encryption*?
8. (a) What is a *nonce*? (b) Why is a nonce used for authentication? (c) Why does it make sense that "the only requirement is that if muliple messages are encrypted with the same key, a different nonce must be used each time such that each nonce is only used once."
9. Describe in general terms how public key encryption works.
10. Describe in general terms how the Dffie-Hellman algorithm works.
11. At the bottom of page 654 in the book, an example of Diffie-Hellman is given using the values $q = 354, \alpha = 3, X_A = 97, X_B = 233$. Give another example using different values.
12. (a) What is a *man in the middle* attack? (b) How is it accomplished? (c) What is one defense against it?