ITBU 443: Threats and Counter Measures, Homework 14

Chapter 20, *Computer Security, Principles and Practices*

Readings

Read chapter 20 in the *Computer Security, Principles and Practices* book.

Discussion Questions

Answer the discussion questions in writing.

1. List the five ingredients of a symmetric encryption scheme.
2. What does it mean to say that an encryption scheme is *computationally secure*?
3. Give a brief summary of a Feistal Network.
4. 3DES uses this formula. Give a step by step, English translation of this formula.

   $$C = E(K_3, D(K_2, E(K_1, p))) \tag{1}$$

5. In the AES, four different stages are used, one of permutation and three of substitution. Explain the four different different stages of AES.
6. Explain what an *S-box* is, and detail how it is created. (This should be a simple, short answer.)
7. On page 618 of the book, in the subsection entitled *Add Round Key Transformation*, there is depicted an example of three boxes. The upper left square of each box contains the following three values: `47, AC, EB`. Using ordinary arithmetic, show how this is done. Note that this uses hexidecimal and binary digits. Here is a hint:

   ```
   0x74 = 0 1 0 0  0 1 1 1
   0xAC = 1 0 1 0  1 1 0 0
   0xEB = 1 1 1 0  1 0 1 1
   ```

8. Explain the difference between a *block cipher* and a *stream cipher*.
9. List some applications that use the RC4 algorithm.
10. Describe how the ECB mode works.
11. What is an *initialization vector*? What is it used for?