

Week One

Assignments

Review the Class Syllabus and the Class Schedule. Prior to the next class, be sure to complete the readings specified in Table 1-1.

Source	Reading
Guideline for Implementing Cryptography in the Federal Government NIST SP 800-21 [1]	Unit 1 Introduction Unit 2 Standards and Guidelines Unit 3 Cryptographic Methods Unit 4 General Implementation Issues Unit 6 Selecting Cryptography - The Process
Tjaden; Fundamentals of Secure Computer Systems; Franklin, Beedle & Associates; 2004, ISBN 1-887902-66-X	Chapter 1 Introduction Chapter 2 Classic Cryptography
Mell, H.X., Baker, D., Cryptography Decrypted, Pearson Education, 2001, ISBN-10 0201616475	Part 1A Secret Key Cryptography Ch 1-- 4 Locks and Keys Substitution and Caesar's Cipher Transposition Ciphers: Moving Around Diffuse and Confuse

Table 1-1 Reading Assignment Week One

As you can see from Table 1-1, in addition to readings from the assigned texts, you need to download and read selections from the National Institute of Standards and Technology's (NIST), Special Publication SP 800-21 "Guideline for Implementing Cryptography in the Federal Government".[1]

Outside Reading Assignment

For next week, please write brief but complete answers to the following questions concerning NIST 800-21.

1. As specified in SP800-21, what is cryptography's purpose?
2. What process is specified for implementing cryptographic applications within an organization?
3. Create a table that lists and defines each basic cryptographic mechanism.
4. Briefly describe the process, articulated within NIST SP-800-21, for selecting cryptographic controls.
5. Expound upon the Information Security in SDLC as shown in Chapter 6, Figure 9. [1]

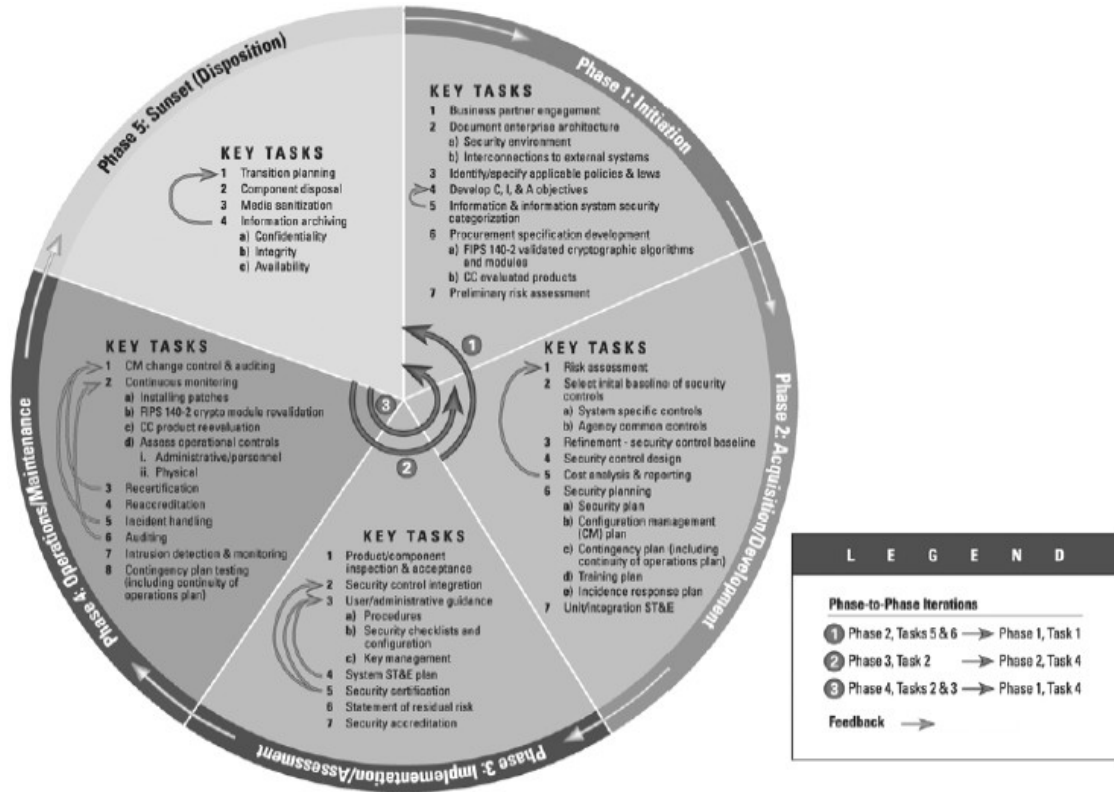


Figure 9: Information Security in the System Development Life Cycle

Figure 1-1 Information Security in the System Development Live Cycle

Prior to the beginning of next class, you should post an electronic version of the essay on your online class portfolio.

Online Journal Assignment

For your online journal, you will need to find a current (for example from the last month) report of an incident that appropriate use of cryptography could have mitigated or prevented. Write a minimum of one paragraph explaining why you selected that particular incident. Write another paragraph explaining how cryptography could have mitigated, or prevented, the incident.

Your journal should also link to the original article.

[1]
http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf