Week Two

Assignments

Prior to the next class, be sure to complete the readings specified in Table 1-1.

Source	Reading
Fundamentals of Secure Computer Systems	Ch 3 Symmetric Key Cryptosystems Ch 4 Cryptographic Hash Functions Ch 5 Public Key Cryptosystems and Digital Signatures, Ch 6 Other Security Building Blocks (6.1 Secret Splitting and 6.4 Cryptographic Protocols, Pages 94-96 and 102-109)
Cryptography Decrypted	Ch 5 DES isn't Strong Anymore Ch 6 Evolution of Cryptography Ch 7 Secret Key Assurances Ch 8 Problems with Secret Key Exchange
Outside Reading	Schneier, Bruce; Why Cryptography is Harder than it Looks, Information Security Bulletin, 1997.

Table 1-1 Week Two Readings

For your outside reading, please download and read Burce Schneier's "Why Cryptography is Harder than it Looks." Note that Google Scholar shows that there are 81 versions of this document on the Web.

Four Questions

1. According to Schneier, "…the cryptography on the market now doesn't provide the level of security it advertises". Why is that?

2. Schneier makes the point that "Security is different than other design requirements." Explain how it is different.

3. Schneier states that "Cryptographic system designs are fragile." What does he mean by that?

4. Schneier states that "Laws are no substitute for engineering." Elaborate on what he means by that.

Prior to the beginning of next class, post your answers online. Your posting will later become the part of your online class portfolio.

Online Journal Assignment
For your online journal, you will need to find a current (within the last month) report of a cyber security incident that involved wireless networking. The incident could involve a cryptographic related vulnerability or other problem such as password cracking, bad certificates, man in the middle SSL or similar attacks/problems.

You should write a minimum of one paragraph explaining why you have selected that particular incident and why the incident is important. Your journal should also include a link to the original article.