

# **Homework 1**

## **Required Reading Assignment**

**to be completed by Wednesday, September 9, 4:30pm**

W. Stallings, "Cryptography and Network-Security: Principles and Practice," 8<sup>th</sup> or 7<sup>th</sup> edition

Chapter 3.1 Symmetric Cipher Model

Chapter 9.1 Principles of Public-Key Cryptosystems

Chapter 1.3 Security Attacks

Chapter 1.4 Security Services

Chapter 11.1 Applications of Cryptographic Hash Functions

Chapter 12 (only Sections 12.1-12.6) Message Authentication Codes

Chapter 13.1 Digital Signatures.