Name: _____

Read and take notes on the introduction to Chapter 14 Sketches of Protocols and Sections 14.1 and 14.2 Basic Public Key Protocol and Secret-Sharing. In Section 14.2, focus on the big ideas and not on the mathematical details of the secret-sharing model. If you are interested in understanding the mathematical details, see Sections 10.1 and 10.2 on Sun-Ze's Theorem and its application to solving systems of linear congruences.

Reading Questions

1. Make sure you understand the following terms: passive and active eavesdroppers, passive and active cheaters, signature, man-in-the-middle attack, certificate authorities, timestamp, threshold scheme.

2. Describe the two flaws in the public-key set-up stemming from a lack of identity verification. What can be done to address these flaws?

3. Describe the active eavesdropping that a timestamp is meant to address.

4. In your own words, explain what a threshold scheme is.

5. What struck you in this reading? What is still unclear? What remaining questions do you have?