Homework 9 – Due Tuesday, April 10

1. There are two main authenticated encryption techniques described in the book, CCM and GCM. Describe at least two advantages of GCM over CCM.

2. Both MACs and digital signature schemes are designed with the goal of being resistant to "existential forgery." Describe what this means and why this is an important property.

3. The Digital Signature Algorithm (see Figure 13.3 on page 410) starts by selecting what the book calls the user's "per message secret number" k, after which $r = (g^k \bmod p) \bmod q$ becomes part of the signature. Since k is just a random value, not related to the signer's private key, is it important to protect k? In particular, what would be the consequences if an attacker could learn k in addition to the signature (r, s)?

   [*Hint: See what you can calculate based on the formulas for r and s, as well as the information that is known by the attacker. Try taking the formulas and multiplying through by values, or subtracting formulas to see what cancels out, or doing other basic algebraic manipulations to see what you can have "pop out" of the formulas.*]