Homework 12 – Due Tuesday, April 25

For problems 1 and 2 below, see what you can calculate based on the formulas for r and s, as well as the information that is known by the attacker (as described in each problem). 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.

1. 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)?

2. The "per message" part of the phrase "per message secret number" is vital. If an attacker could trick a signer into signing two different messages, say M_1 and M_2, using the same secret k, what can the attacker figure out from knowledge of those two signatures and the two messages.

3. The secure chat protocol that we have developed for the project in this class is not perfect. Describe at least one way the security of the system could be compromised (if you make any assumptions, make sure they are clearly stated).