Homework 8 – Due Tuesday, March 28

1. Give the RSA algorithm, including descriptions of how keys are generated and how encryption and decryption work. Use formulas, and describe the size of values (i.e., number of bits) used in a typical real system. Explain why decryption is the inverse if encryption (i.e., what is the mathematics that explains why $M = D(PR_a, E(PU_a, M))$ for all messages M).

2. Joe makes a system using RSA for public key cryptography, but in the key generation routine uses the standard C library `rand()` function for random values, which uses a 15-bit value for a seed. Why is this insecure? Be very specific in your answer, describing a real, practical attack with an explanation of the time complexity of the attack.

3. The basic Diffie-Hellman key exchange protocol is vulnerable to a "man-in-the-middle" attack, as explained in the textbook. Describe this attack.