The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 10
April 7, 2014

Assignment 5 – Due Monday, April 14

Note: This homework assignment is worth 50 points.

1. The beginning of this problem is similar to a problem on your last homework: Use Table 8.1 on page 234 to pick two random primes (p and q) in the range $1500, \ldots, 2000$. Compute $n = pq$ and $\phi(n)$, and . let's use b to represent $\phi(n)$ (i.e., $b = \phi(n)$). Find the prime factorization of b and then use the equation from Problem 8.12 (page 264) to find $\phi(b)$. Pick a random e that is relatively prime to b, and use the technique from Problem 5 on your last homework to compute the multiplicative inverse of e modulo b — call this d. Finally, verify that these values work as RSA keys: Pick two different random messages m_1 and m_2 in the range $0, \ldots, n-1$ — for each one, compute $c_i = m_i^e \bmod n$ and $r_i = c_i^d \bmod n$, and if everything works you should have $m_i = r_i$.

2. OAEP, described at the bottom of page 277 in the textbook and illustrated in Figure 9.10, is a very important technique — without it, the RSA encryption function is deterministic and stateless, and so cannot be IND-CPA secure! However, using OAEP (or any technique that adds non-determinism) reduces the size of plaintexts that can be encrypted. Assuming that OAEP is using a 160-bit seed and a hash function that produces a 160-bit value, how large a plaintext can be handled using RSA with 2048-bit key? Note that you can't really get enough information from the brief description in the book to determine this — search and find a more precise description of OAEP online (and make sure you cite any source that you use!).

3. The "man-in-the-middle attack" for the Diffie-Hellman Key Exchange (described starting on page 290) is a serious problem that stems from the fact that Alice cannot guarantee that the message she sends to Bob is the same as the message that Bob receives. Consider using a public web site (like a discussion forum) as follows: Alice and Bob post their values Y_A and Y_B on this site, and they retrieve the other side's value from this site. Alice and Bob can also check the web site (from different hosts if they want to disguise their identity) to see if the correct value is being provided by the public web site. Does this solve the problem? Address issues such as how you identify another user, whether the communication link that Alice and/or Bob uses is compromised, etc.

4. Page 311, Problem 10.12

5. Page 311, Problem 10.13