CS 4920/5920 Applied Cryptography Spring 2018

Assignment 5

This homework is due at the beginning of class on April 9th.

Problem 1.

Find all primitive roots of 7. Construct a table like Table 2.7 ("Powers of Integers, Modulo 19") to find the primitive roots.

Problem 2.

This problem is about the Miller-Rabin test.

a. Show that, if n is an odd composite integer, then the Miller-Rabin test will return *inconclusive* for a=1 and a= (n-1).
b. If n is composite and passes the Miller-Rabin test for the base a, then n is called a *strong pseudoprime to the base a*. Show that 2047 is a strong pseudoprime to the base 2.

Problem 3.

Perform encryption and decryption using the RSA algorithm, as in Figure 9.5, for the following:

a. $p = 5$; $q = 11$, $e = 3$; $M = 9$
b. $p = 7$; $q = 11$, $e = 17$; $M = 8$
c. $p = 11$; $q = 13$, $e = 11$; $M = 7$
d. $p = 17$; $q = 31$, $e = 7$; $M = 2$

Problem 4.

In an RSA system, the public key of a given user is e = 31, n = 3599. What is the private key of this user? *Hint*: First use trial-and-error to determine p and q; then use the extended Euclidean algorithm to find the multiplicative inverse of 31 modulo ϕ(n).

Problem 5.

Use the fast exponentiation algorithm of Figure 9.8 to determine $5^{596} \bmod 1234$. Show the steps involved in the computation by identifying the *c* and *f* values over the iterations across *i*. You may use a computer to implement the algorithm.