Tanner Krebs, Gerardo Lopez, William Thornton
Math 314
Due: 11/28/17

COSC/MATH - 314

Assignment 9

Problem 1: If a number n is composite but in the Miller-Rabin algorithm Test (n,a) outputs "n is probably prime" (see my notes, or the textbook page 178), then a is said to be a false Miller-Rabin witness for n. Show that 2 is a false Miller-Rabin witness strong for 2047.

Problem 2: Let $p = 101$ (note that 101 is a prime number). It is known that 2 is a primitive root of 101. For any number n in the range $1, 2, ..., 100$, we denote by $L_2(n)$ the value $k \epsilon (1, 2, ..., 100$ such that $2^k = n$ (mod 101) (i.e., L_n is the discrete log of n mod 101).

(a.) What is $L_2(1)$? Justify your answer. (Note: The answer $k = 0$ is not valid, because k has to be in the set $(1, 2, ..., 100)$.

(b.) Using the fact the $L_2(3) = 69$, determine $L_2(9)$

Problem 3: In the El Gamal cryptosystem, Alice and Bob use $p = 17$ and $a = 3$. Bob choses his secret to be $a = 6$, so $\beta = 15$. Alice sends the ciphertext $(r, t) = (7, 6)$. Determine the plaintext m.

Problem 4: Exercise 7, page 215 in the texbook.