CIS 3362 Test #3: Public Key Encryption

Date: 11/8/2013

Name: ____

Note: For questions with numeric answers, put a box around your final answer.

1) (8 pts) What is the prime factorization of 589449600?

2) (8 pts) What is φ(589449600)?

3) (12 pts) Using Fermat's Theorem, determine 3456^{25190} mod 2099.

4) (12 pts) Using Euler’s Theorem, determine 26^{6051} mod 2664.

5) (10 pts) In an RSA scheme, p = 13, q = 31 and e = 127. What is d?

6) (15 pts) One of the primitive roots (also called generators) mod 29 is 2. There are 11 other primitive roots mod 29. One way to list these is 2^{a1} mod 29, 2^{a2} mod 29, … 2^{a12} mod 29, where 0 < a1 < a2 < … < a12. (Note: it's fairly easy to see that a1 = 1, since 2 is a primitive root.) Find the values of a10, a11 and a12 and the corresponding values 2^{a10} mod 29, 2^{a11} mod 29, and 2^{a12} mod 29.

7) (12 pts) In the Diffie-Hellman Key Exchange, let the public keys be p = 29, g = 19, and the secret keys be a = 11 and b = 13, where a is Alice’s secret key and b is Bob’s secret key. What value does Alice send Bob? What value does Bob send Alice? What is the secret key they share?

8) (10 pts) In El Gamal, Alice chooses $Y_A = \alpha^{XA}$ mod q. Bob, who is sending a message, calculates a value $K = Y_A^k$, where k is randomly chosen with $0 < k < q$. Is it possible that for different choices of k, Bob will calculate the same value K, or will each unique value of k be guaranteed to produce a different value for K? Give a brief rationale for your answer.

9) (10 pts) In a Knapsack Cryptosystem, the private key super-increasing set is {7, 8, 20, 53, 96, 200, 397, 818}. Let the public value u = 1836. Select the private value w = 1645. List the public set of value, in order, that would allow someone to send a message to the person who generated these keys.

9) (3 pts) By what initials is the fast food chain Burger King known? ______________________

Scratch Page - Please clearly label any work on this page you would like graded.