Assignment #8, CSE 191

Fall, 2014

General Guidelines:

This assignment will NOT be collected, nor graded. However, you should carefully complete it as if it were to be graded. There will be a quiz based on this assignment (with very similar problems) during the week Nov 17 - 21.

The solution will be posted on Monday, Nov 17.

1. (0 points). Page 272, Problem 5.

2. (0 points). Page 272, Problem 6.

3. (0 points). Page 272, Problem 14.

4. (0 points). Page 272, Problem 17 (b) (c) (d).

5. (0 point). Page 273, Problem 24 and 25 (a) (b) (c) (d) (e)

6. (0 point). Page 273, Problem 30. (It is good enough to express the lcm as the product of its prime factors.)

7. (0 point) Find the binary representation of 571.

8. (0 points). This problem illustrates an example of the of RSA public key encryption process.

Pick $p = 103$ and $q = 211$. Then $n = p \cdot q = 103 \cdot 211 = 21733$. Also pick $e = 19$.

Thus $(n, e) = (21733, 19)$ is the public key.

1. We have $(p-1) \cdot (q-1) = 102 \cdot 210 = 21420$.

   Use Euclidean-GCD algorithm to show: $gcd(21420, 19) = 1$

   (You need to write down all intermediate steps. They are needed in the next part.)

2. Find integers d, t such that:

   $$d \cdot e + t \cdot 21420 = d \cdot 19 + t \cdot 21420 = 1 \tag{1}$$

   This can be done by using Extended Euclidean-GCD algorithm. Namely, by reversing the process in part 1.

   Note that from (1), we have:

   $$d \cdot e \equiv 1 \text{ mod } 21420$$

   So $(n, d) = (21733, d)$ is the secrete key.

3. Suppose that Alice has a message $M = 100$. Calculate the encrypted message C, where:

   $$C = M^e \text{ mod } n = 100^{19} \text{ mod } 21733$$

   Note: You should NOT evaluate $M^2 \equiv \text{mod } 21733$, $M^3 \equiv \text{mod } 21733$, $M^4 \equiv \text{mod } 21733$, $\ldots, M^{19} \equiv \text{mod } 21733$. This will take too long! Instead, you should use the *double squaring* method discussed in class.

(The answer should be: $100^{19} \bmod 21733 = 20815$. You should find the solution by yourself. The answer is provided here so that you can proceed to the next step.)

4. Once Bob receives the encrypted message C, he needs to decrypt it by calculating:

$$C^d \equiv \bmod n$$

   Perform this calculation (as in part 3, or write a short program to do this). Verify that this gives the original message $M = 100$.

   This is a long process involving lengthy numerical calculations. You are encouraged to complete the entire calculation, and see the answer is indeed 100. If you don't have enough time, it is acceptable that you carry out the first few steps (so that you can understand what's going on), and wait to see the solution.