UCInetID:

Name (written clearly):_____

Test II

Version A

ICS 6D
Winter 2017
February 17, 2017
Instructor: Sandy Irani

Instructions

- Wait until instructed to turn over the cover page.
- The total number of points on the test is 45.
- **Important:** Except for the last page, there are questions on both sides of the page.

1. *(8 points)* Bob publishes his public key $(e, N) = (31, 161)$ Use the fact that $N = 7 \cdot 23$, to determine Bob's private key d.

2. *(2 points)* Give the binary representation of $(3A7E3)_{16}$.

3. *(5 points)* Compute $(24)^{42} \mod 11$.

4. *(8 points)* Compute the following quantities:

   (a) $-72 \bmod 11$

   (b) $-72 \text{ div } 11$

   (c) $72 \bmod 11$

   (d) $72 \text{ div } 11$

   (e) $(260 \cdot 2378 + 41 \cdot 29) \bmod 13$

   (f) $((131)^{37} + 12 \cdot (-10)) \bmod 13$

5. *(4 points)* Bob uses the RSA cryptosystem to allow people to send him encrypted messages. He selects the parameters:

$$p = 3, \quad q = 11, \quad e = 3, \quad d = 7$$

   (a) What are the numbers that Bob publishes as the public key?

   (b) Alice wants to send the message $m = 5$ to Bob. Use the public key for this cryptosystem to compute the cyphertext that she sends.

6. *(2 points)* The prime factorizations for $2,395,575$ and $1,497,375$ are given below:

   - $2,395,575 = 3^4 \cdot 5^2 \cdot 7 \cdot 13^2$
   - $1,497,375 = 3^2 \cdot 5^3 \cdot 11^3$

   (a) Give the prime factorization for the **gcd** of $2,395,575$ and $1,497,375$.

   (b) Give the prime factorization for the **lcm** of $2,395,575$ and $1,497,375$.

7. *(2 points)* Use the fact that $(33233344)_6 = 1000000$ to determine the decimal value for $(3323334402)_6$

8. *(2 points)* Give the base 9 representation of $(2121212121212121)_3$. *Hint: there is a quick way and a slow way to do this problem.*

9. *(6 points)* Give the decimal representation for the following numbers:

   (a) $(257)_8$.

   (b) $(101101)_2$

   (c) $(A05)_{16}$

10. *(6 points)* A number is given below in decimal format. Compute the representation of the number in the indicated base.

    (a) 146, base 5

    (b) 52, binary

This area is for scratch work.