

Student ID Number:

--	--	--	--	--	--	--	--

Name: _____

Test II

ICS 6D

Spring 2015

Wed, May 13, 2015

Instructor: Sandy Irani

Wait until instructed to turn over the cover page. Complete all of the following questions. There are a total of 50 points.

Page 1	
Page 2	
Page 3	
Page 4	
Total	

1. (2 points) Give the base 3 representation of $(77777777)_9$. (Hint, start with the base 3 representation of $(7)_9$. Then try $(77)_9$.)
2. (2 points) Give the decimal representation of $(10010110)_2$.
3. (2 points) Give the base 5 representation of 542.
4. (2 points) Give the representation for 171 in hexadecimal notation.
5. (2 points) Give the binary representation of $(A70F)_{16}$.

6. (2 points) Circle the numbers below that are equivalent to $3 \bmod 11$:

-7 11 58 113 -3 -11 -30

7. (8 points) Compute the following quantities:

(a) $-127 \bmod 11$.

(b) $-127 \operatorname{div} 11$.

(c) $(25 - 1700 * 265^2) \bmod 17$.

(d) $(56 - 3 * 34) \bmod 11$.

8. (5 points) Compute $(46)^{39} \bmod 11$

9. (3 points) Compute $7^{36} \bmod 2399$. The following equalities may be useful:

$$7^2 \bmod 2399 = 49$$

$$7^4 \bmod 2399 = 2$$

$$7^8 \bmod 2399 = 4$$

$$7^{16} \bmod 2399 = 16$$

$$7^{32} \bmod 2399 = 256$$

$$7^{64} \bmod 2399 = 512$$

10. (6 points) Use the prime factorizations given below to compute the following expressions:

$$19800 = 2^3 \cdot 3 \cdot 11 \cdot 15^2$$

$$4590 = 2 \cdot 3^2 \cdot 11^2 \cdot 17$$

$$3267 = 3^3 \cdot 11^2$$

(a) Give the prime factorization for $\text{lcm}(19800, 3267)$.

(b) Give the prime factorization for $\text{gcd}(19800, 4590)$.

(c) Give the prime factorization for $4590 \cdot 3267$.

11. (4 points) Consider an RSA cryptosystem with public key (e, N) , where $N = p \cdot q$ and p and q are prime. The private key is d . Alice wishes to send a plaintext message m to Bob.

(a) Give an expression for the cyphertext message that Alice sends as a function of the parameters above.

(b) If Bob receives cyphertext c , give an expression for m , the original plaintext message, as a function of c and the other parameters besides m .

12. (12 points) Consider an RSA cryptosystem with $p = 11$ and $q = 13$. Suppose that the encryption key $e = 83$. Compute the decryption key d . Your answer should be a non-negative number.
- Show all your work as clearly as possible, so you can get partial credit if needed.