

# Homework 1 of CS549 Cryptography and Network Security

ASSIGNED: AUGUST 30TH, 2010 DUE DATE: SEPT. 24TH, 2010  
EXTENSION DATE (WITH 10% DEDUCTION ON GRADING): 5PM, OCT 1ST, 2010  
FALL 2010, CS DEPARTMENT, IIT

1. Is there an integer  $x$  such that  $x \cdot 4321 = 1 \pmod{9871}$ . If so, find the smallest such positive integer  $x$ .
2. What is the value of  $7^{2010} \pmod{13}$ ?
3. Suppose that  $n = p \cdot q$  where  $p$  and  $q$  are different prime numbers. Suppose also that  $n = 4,386,607$  and  $\phi(n) = 4,382,136$ . Find the values of the integers  $p, q$ . You need show the details of your methods.
4. Find the smallest integer  $x > 0$  such that  $13 \cdot x = 1 \pmod{99}$  and  $7 \cdot x = 1 \pmod{101}$  are satisfied simultaneously.
5. Given an integer  $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$ , where  $p_1, p_2, p_3, \dots$ , and  $p_k$  are different prime numbers larger than 2, prove that there are *exactly*  $2^k$  integers  $x \in [1, n]$  satisfying that

$$x^2 = 1 \pmod{n}.$$

6. Let integer  $p$  be an odd prime number and  $p$  does not divide  $b$ . Then prove the following statements
  - (a)  $b$  is a quadratic residue of  $p$  if and only if  $b^{\frac{p-1}{2}} = 1 \pmod{p}$ .
  - (b)  $b$  is a quadratic non-residue of  $p$  if and only if  $b^{\frac{p-1}{2}} = -1 \pmod{p}$ .
7. This question is about solving the quadratic congruence. Assume that  $p > 2$  is a prime number and the positive integer  $a = x^2 \pmod{p}$  for some unknown integer  $x \in [1, p-1]$ . Prove the following statements
  - (a) (5 points) There are only two solutions (i.e., two integers in  $[1, p-1]$ ) for equation  $a = x^2 \pmod{p}$ .
  - (b) (5 points) If  $p = 3 \pmod{4}$ , then  $x_1 = a^{\frac{p+1}{4}} \pmod{p}$ , and  $x_2 = p - x_1$  are the only two solutions.
  - (c) (5 points) If  $p = 5 \pmod{8}$  and  $a^{\frac{p-1}{4}} = 1 \pmod{p}$ , then  $x_1 = a^{\frac{p+3}{8}} \pmod{p}$ , and  $x_2 = p - x_1$  are the only two solutions.
  - (d) (5 points) If  $p = 5 \pmod{8}$  and  $a^{\frac{p-1}{4}} = -1 \pmod{p}$ , then  $x_1 = 2a \cdot (4a)^{\frac{p-5}{8}} \pmod{p}$ , and  $x_2 = p - x_1$  are the only two solutions.

Hint: (1) notice that  $a^{\frac{p-1}{2}} = 1 \pmod{p}$ ; (2) notice that 2 is a quadratic non-residue modulo  $p$ , if  $p = 5 \pmod{8}$ , i.e., there is no integer  $t$  such that  $t^2 = 2 \pmod{p}$  if  $p = 5 \pmod{8}$ ; (3) an integer  $b$  is a quadratic residue modulo  $p$  iff  $b^{\frac{p-1}{2}} = 1 \pmod{p}$ .

8. An affine cipher encrypts a plaintext  $x \in [0, 255]$  as  $y = k_1x + k_2 \pmod{256}$ . A key  $(k_1, k_2)$  with  $0 \leq k_1, k_2 \leq 255$  is valid for an affine cipher if the function  $k_1x + k_2 \pmod{256}$  is an one-to-one mapping. How many different valid keys for this affine cipher?
9. Write a code to compute  $a^b \pmod{n}$ , when given integer  $a > 0, b > 0$ , and  $n > 0$ .

Here the input integers could be up to 1000 bits. So your code should be able to take care of big integers.

Use your code to find what is the last digit of the following number  $a^b \pmod{n}$ , when  $a = 2^{123} - 1$ ,  $b = 2^{999} - 1$ , and  $n = 2^{345} + 1$ .