

Homework 1 of CS549 Cryptography and Network Security

ASSIGNED: AUGUST 30TH, 2010 DUE DATE: SEPT. 24TH, 2010
EXTENSION DATE (WITH 10% DEDUCTION ON GRADING): PM, 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 .

Solution: We use the extended Euclidean algorithm to find it:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -9 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -15 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 9871 \\ 4321 \end{pmatrix}$$

So

$$\begin{aligned} 1 &= 443 \times 9871 + (-1012) \times 4321 \pmod{9871} \\ &= (-1012) \times 4321 \pmod{9871} \\ &= 8859 \times 4321 \pmod{9871} \end{aligned}$$

So the smallest positive number of the inverse of 4321 modular 9871 is 8859.

2. What is the value of $7^{2010} \pmod{13}$?

Solution: First, please note that, by the Fermat's little theory, we get that $7^{12} = 1 \pmod{13}$. So $7^{2010} = 7^6 \pmod{13}$. $7^2 \pmod{13} = 10$, $7^4 \pmod{13} = 9$, so $7^6 \pmod{13} = 90 \pmod{13} = 12$. So $7^{2010} \pmod{13} = 12$.

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.

Solution: We only need to solve the following equations to get p, q .

$$\begin{cases} n &= p \times q \\ \phi(n) &= (p-1) \times (q-1) \end{cases}$$

We get that $p + q = 4472$. By brute-force, we can get that p and q are equal to 1453 and 3019 respectively.

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.

Solution: Because 101 is a prime number, so 99 and 101 are co-prime. So we can employ the Chinese remainder theorem.

$$13^{-1} = 61 \pmod{99}, 7^{-1} = 29 \pmod{101}.$$

$$e_1 = 101 \times ((101)^{-1} \pmod{99}) = 101 \times 50, e_2 = 99 \times ((99)^{-1} \pmod{101}) = 99 \times 50.$$

$$\text{So the number is } 61 \times 101 \times 50 + 29 \times 99 \times 50 \pmod{(99 \times 101)} = 1645.$$

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 *exactl* 2^k integers $x \in [1, n]$ satisfying that

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

Solution: First, for any prime number $p > 2$, $x^2 = 1 \pmod{p}$ only has exactly two different solutions. When $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$, where p_i 's are different prime numbers larger than 2, we can write $x^2 = 1 \pmod{n}$ as $x^2 = 1 \pmod{(p_1 \cdot p_2 \cdot \dots \cdot p_k)}$.

Now we want to show that (i) $x^2 = 1 \pmod{p_1 \cdot p_2 \cdot \dots \cdot p_k}$ is equivalent to a set of equations (ii):

$$\begin{cases} x^2 &= 1 \pmod{p_1} \\ x^2 &= 1 \pmod{p_2} \\ \dots & \\ x^2 &= 1 \pmod{p_k} \end{cases}$$

First, it is trivial that (i) implies (ii), so we skip this part. Next, we want to show (ii) implies (i). By the Chinese remainder theorem, we know that there is one solution and only one solution of x^2 in the range of $[1, n = p_1 \cdot p_2 \cdot \dots \cdot p_k]$, and we also know that x^2 is a solution of (i), which show that the solution actually is the same both for (i) and (ii). So we have built the equivalence.

For each of the equations in the set there are two different solutions for x , so combine them together we will have exactly 2^k different solutions for x in (i) by solving by Chinese Remainder Theorem.

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 $b^{\frac{p-1}{2}} = 1 \pmod{p}$.

Solution:

\Rightarrow If b is a quadratic residue, then $b = x^2 \pmod{p}$. So $b^{\frac{p-1}{2}} = (x^2)^{\frac{p-1}{2}} = x^{p-1} = 1 \pmod{p}$.

\Leftarrow Let g be a primitive root for p , then $b = g^i$ for some i . If i is even, then we are done since $b = (g^{\frac{i}{2}})^2 \pmod{p}$. Suppose i is odd, then $b = g^{2k+1}$. $b^{\frac{p-1}{2}} = (g^{2k+1})^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} = 1 \pmod{p}$. Since g is a primitive, $g^{\frac{p-1}{2}} \neq 1 \pmod{p}$. So i cannot be odd, which means that b is quadratic residue.

(b) b is a quadratic non-residue of p if and only if $b^{\frac{p-1}{2}} = -1 \pmod{p}$.

Solution:

\Rightarrow If b is a quadratic non-residue, then $b = g^{2k+1}$ where g is some primitive root for p . $b^{\frac{p-1}{2}} = (g^{2k+1})^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} \pmod{p}$. Since $g^{p-1} = 1 \pmod{p}$ and p is prime, so $g^{\frac{p-1}{2}} = -1 \pmod{p}$. Note that since g is a primitive root for p , $g^{\frac{p-1}{2}} \neq 1$. So $b^{\frac{p-1}{2}} = -1 \pmod{p}$.

\Leftarrow If $b^{\frac{p-1}{2}} = -1 \pmod{p}$, $b = g^i$ for some primitive root g , then $(g^i)^{\frac{p-1}{2}} = -1 \pmod{p}$. We prove that i cannot be even, since that otherwise $(g^i)^{\frac{p-1}{2}} = (g^{2k})^{\frac{p-1}{2}} = (g^{p-1})^k = 1 \pmod{p}$, which contradicts with $b^{\frac{p-1}{2}} = -1 \pmod{p}$. So b is quadratic non-residue.

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 $a = x^2 \pmod{p}$.

Solution: First, by the fundamental theorem of algebra, it can have at most 2 roots not congruent for p . Next, we want to show that it cannot have one root, that is it must have at least 2 roots not congruent for p . Thus, we finished the proof.

If there is only one root for the equation $a = x^2 \pmod{p}$, then we know that $x = \pm x_0$ and x_0 is congruent with $-x_0$ under modular p . Thus p divides $2x_0$ ($p \mid 2x_0$), which results that $p \mid x_0 \mid x_0^2 \mid a$. Since a is quadratic residue, so $p \nmid a$, thus we got a contradiction.

So we are done.

(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.

Solution: Since we have proved that there can be and only be two solutions when p is a odd prime. So we only need to prove that the two roots holds for $a = x^2 \pmod{p}$.

$x_1^2 = (a^{\frac{p+1}{4}})^2 = a^{\frac{p+1}{2}} = a^{\frac{p-1}{2}} \cdot a \pmod{p}$, since that a is quadratic residue, thus $a^{\frac{p-1}{2}} = 1 \pmod{p}$. So we got $x_1^2 = a \pmod{p}$, which is correct.

$x_2^2 = (p - x_1)^2 = p^2 - 2px_1 + x_1^2 = x_1^2 = a \pmod{p}$, which is correct.

So we finished the proof.

- (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.

Solution: Still, we only need to prove the correctness.

$x_1^2 = (a^{\frac{p+3}{8}})^2 = a^{\frac{p+3}{4}} = a^{\frac{p-1}{4}} \cdot a \pmod p$, since $a^{\frac{p-1}{4}} = 1 \pmod p$, $x^2 = a \pmod p$, which is correct. $x_2^2 = a$ as shown in above. Thus we finished.

- (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.

Solution: As above, we only need to prove the correctness of x_1 .

$x_1^2 = (2a \cdot (4a)^{\frac{p-5}{8}})^2 = 4a^2 \cdot (4a)^{\frac{p-5}{4}} = a \cdot (4a)^{\frac{p-5}{4}+1} = a \cdot (4a)^{\frac{p-1}{4}} = a \cdot (-1) \cdot 4^{\frac{p-1}{4}} = a \cdot (-1) \cdot 2^{\frac{p-1}{2}} \pmod p$. For that $p = 5 \pmod 8$, by the second supplement of the law of quadratic reciprocity: $(2/p) = (-1)^{\frac{p^2-1}{8}} = -1$. So we know that 2 is a primitive root of p . So $2^{\frac{p-1}{2}} = -1 \pmod p$. Thus $x^2 = a \cdot (-1) \cdot (-1) = a \pmod p$.

So we are done.

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?

Solution: For that this is one-to-one mapping, we need to let the encryption be decrypted, that is $x = k_1^{-1}y - k_2 \pmod{256}$. So we need to make sure $k_1^{-1} \pmod{256}$ exists, that is $GCD(k_1, 256) = 1$. So the choices of k_1 could be $\phi(256)$, k_2 can be chosen any value from 0 to 255. So the total number of choices is $256 \times \phi(256) = 256 \times 128 = 32768$.

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 $n = 2^{345} + 1$.

Solution: I just wrote a short program which used the algorithm introduced in the lecture. We first calculate a series of power of a 's (from $a^{2^0} \pmod n$ to $a^{2^{998}} \pmod n$), and then we time them from left to right step by step on modular n . After run the program with the long integer type wrote by myself, the final result is as follows in binary form:

```
11011111111110000010000110001111111110001010110001010000111
0001111001100000001110111011001110010111110101000101101111
111000001000000010101101111101011111010010101111110100
00000110010011001001011000000101100101110000011111001111001
10001000100110000111101110010100111001010100101110101010001
11100001111010101000010011110110001000010101001
```

Or the decimal form:

```
78380308944664459449169764048415136628132994290978905811703
30514812317792703329182233555759459326431401
```

So the last digit is 1.