

## Solution to Homework

*Lecturer: Shouhuai Xu*

**Due: March 8, in class**

1. Consider the following sub-problems.

(a) Compute  $3^{64} \bmod 79$ . (Show work.)

**Solution:**

$$\begin{aligned} 3^2 &= 9 \bmod 79 \\ 3^4 &= 9^2 = 2 \bmod 79 \\ 3^8 &= 2^2 = 4 \bmod 79 \\ 3^{16} &= 4^2 = 16 \bmod 79 \\ 3^{32} &= 16^2 = 19 \bmod 79 \\ 3^{64} &= 19^2 = 45 \bmod 79. \end{aligned}$$

(b) Compute  $3^{76} \bmod 79$ . (Show work; try to use some of the intermediate results from the previous part.)

**Solution:**  $3^{76} = 3^{64+8+4} = 45 \cdot 4 \cdot 2 = 90 \cdot 4 = 11 \cdot 4 = 44 \bmod 79$ .

(c) Describe an efficient algorithm to compute  $a^b \bmod c$  for positive integers  $a, b, c$ .

The square-multiplication algorithm (see the exponentiation algorithm, Lecture 10-13: Language of Cryptography IV, pp 10).

2. Consider the group  $\mathbb{Z}_{35}^*$  (of course  $35 = 5 \times 7$ ). Answer the following questions about this group:

(a) How many elements are in this group?

**Solution:**  $\phi(35) = \phi(5) \cdot \phi(7) = 4 \cdot 6 = 24$ .

(b) List the elements of this group?

**Solution:**  $\mathbb{Z}_{35}^* = \{1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34\}$ .  
As you can see, exactly 24 elements.

- (c) What does  $\phi(35)$  mean?
3. Consider the following sub-problems.
- (a) Let  $m = m_1m_2$  such that  $\gcd(m_1, m_2) = 1$ , and  $y \in \mathbb{Z}_m$ . Given  $a_1 = y \pmod{m_1}$  and  $a_2 = y \pmod{m_2}$ , prove the Chinese Remainder Theorem in this specific case.  
**Solution:** This is simply a specific case of the proof shown in the lecture (Lecture 10-13, Language of Cryptography IV, pp 12).
- (b) Compute  $101^{4,800,000,023} \pmod{35}$  without using a calculator. Show all work. (Hint: use Chinese Remainder Theorem, among other tricks.)  
**Solution:** Let  $d = 4,800,000,023$ . Note that  $35 = 5 \cdot 7$ . So

$$101 = 1 \pmod{5} \Rightarrow 101^d = 1 \pmod{5}.$$

Also, for any  $a \in \mathbb{Z}_7^*$  we have  $a^6 = 1 \pmod{7}$ . So

$$101^d = 3^d = 3^{d \pmod{6}} = 3^5 = 5 \pmod{7}.$$

Using CRT, we can get

$$x = 7 \cdot 3 \cdot 1 + 5 \cdot 3 \cdot 5 = 26 \pmod{35}.$$

4. Let  $p$  be a prime,  $x_1$  and  $x_2$  be quadratic residues in  $\mathbb{Z}_p^*$ , and  $y$  be a quadratic non-residue in  $\mathbb{Z}_p^*$ .
- (a) Prove that  $x_1x_2$  is a quadratic residue.  
**Solution:** Since  $x_1, x_2$  are quadratic residues, we know there exist  $y_1, y_2$  such that  $y_1^2 = x_1 \pmod{p}$  and  $y_2^2 = x_2 \pmod{p}$ . So we have  $(y_1y_2)^2 = x_1x_2 \pmod{p}$ , which means  $x_1x_2$  is a quadratic residue.
- (b) Prove that  $x_1^{-1} \pmod{p}$  is a quadratic residue.  
**Solution:** We have  $(y_1^{-1})^2 = (y_1^2)^{-1} = x_1^{-1} \pmod{p}$ , which means  $x_1^{-1}$  is a quadratic residue.
- (c) Prove that  $x_1y$  is *not* a quadratic residue.  
**Solution:** Suppose  $x_1y$  is a quadratic residue. Then there exists  $y_3$  such that  $y_3^2 = x_1y \pmod{p}$ . But then  $(y_3y_1^{-1})^2 = y_3^2(y_1^{-1})^2 = x_1y x_1^{-1} = y \pmod{p}$ , so  $y$  is a quadratic residue. We reach a contradiction.

5. Let  $p$  be a prime such that  $p = 3 \pmod{4}$ . Let  $x \in \mathbb{Z}_p$  be a quadratic residue.

(a) Show that  $x^{(p+1)/4} \pmod{p}$  can be computed in time  $O(\text{poly}(|p|))$ .

**Solution:** Since  $p = 3 \pmod{4}$  we may write  $p = 4k + 3$  for some integer  $k$ . Then  $(p + 1)/4 = k + 1$ , an integer. Since  $x \in \mathbb{Z}_p$ , we know that  $x^{(p+1)/4} \pmod{p}$  can be computed in time  $\text{poly}(|p|)$ .

(b) Show that  $x^{(p+1)/4}$  gives a square root of  $x$ . (Hint: use the fact that  $y^{p-1} = 1 \pmod{p}$  for any  $y \in \mathbb{Z}_p$  and the fact that  $x$  is a quadratic residue.)

**Solution:** We need to show that  $(x^{(p+1)/4})^2 = x$ . Since  $x$  is a quadratic residue, we know that  $x = y^2 \pmod{p}$  for some  $y \in \mathbb{Z}_p$ . So,

$$\begin{aligned} (x^{(p+1)/4})^2 &= x^{(p+1)/2} \\ &= y^{p+1} \\ &= y^{p-1}y^2 \\ &= y^2 \\ &= x. \end{aligned}$$

(c) How would you find both square roots of  $x$ ?

**Solution:** Compute  $z = x^{(p+1)/4}$ , which is one square root of  $x$ . The other square root of  $x$  is  $-z \pmod{p}$ .

6. Show that given  $n$  and  $\phi(n) = (p-1)(q-1)$ , one can factor  $n$  in polynomial-time.

**Solution:**  $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$ , so  $p = n - \phi(n) - q + 1$ , so  $n = pq = (n - \phi(n) - q + 1)q$ , so  $q^2 + (\phi(n) - n - 1)q + n = 0$ . This is a quadratic equation in  $\mathbb{Z}$ . So we can solve it to get  $q$  and therefore  $p$ .

**Alternative Solution:**  $\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$  and  $p = \frac{n}{q}$  (in  $\mathbb{Z}$ ). So we have  $\phi(n) = n - \frac{n}{q} - q + 1$ , so  $q^2 + (\phi(n) - n - 1)q + n = 0$ . This is a quadratic equation in  $\mathbb{Z}$ . So we can solve it to get  $q$  and therefore  $p$ .

7. Suppose  $F: \{0, 1\}^\kappa \times \{0, 1\}^\kappa \rightarrow \{0, 1\}^\kappa$  is a family of pseudorandom functions. That is, in terms of our lectures we have  $\mathbb{K} = \mathbb{D} = \mathbb{R} = \{0, 1\}^\kappa$ . Define  $G_k(x) = F_k(x) || F_k(\bar{x})$ , where  $\bar{x}$  denotes the bitwise negation of  $x$  (e.g.,  $\overline{101} = 010$ ). Is  $G$  a PRF? If yes, prove it; if not, disprove it.

**Solution:** No. Because we can compute  $G_k(\bar{x}) = F_k(\bar{x}) || F_k(x)$  from  $G_k(x) = F_k(x) || F_k(\bar{x})$ . For random functions, this happens with probability  $1/2^{-2\kappa}$ . So the advantage is  $1 - 1/2^{-2\kappa}$ .

8. As we covered in the lecture the “birthday paradox” in terms of balls-and-bins. Suppose  $C(N, q)$  is the probability of at least one collision when we throw  $q \geq 1$  balls into  $q \leq N$  bins. Suppose  $1 \leq q^2 \leq 2N$ .

(a) State the inequality you need to finish your proof.

**Solution:** For any real number  $x \in [0, 1]$ , we have the following:

$$\left(1 - \frac{1}{e}\right) \cdot x \leq 1 - e^{-x} \leq x.$$

(b) Prove (note:  $1 - \frac{1}{e} \geq 0.6$ )

$$0.3 \cdot \frac{q(q-1)}{N} \leq C(N, q) \leq 0.5 \cdot \frac{q(q-1)}{N}.$$

**Solution:** The proof is in Lecture 4-7: Language of Cryptography II, pp 14.