

Homework*Lecturer: Shouhuai Xu***Due: March 8, in class**

Note: You are allowed to discuss with anyone else, but you **MUST** write your own solutions independently. Scientific honesty is fundamental to us, so you **MUST** sign on your cover page something like this:

I hereby certify that I independently wrote my solutions.

If possible, print your solutions.

1. (15 points) Consider the following sub-problems.
 - (a) Compute $3^{64} \bmod 79$. (Show work.)
 - (b) Compute $3^{76} \bmod 79$. (Show work; try to use some of the intermediate results from the previous part.)
 - (c) Describe an efficient algorithm to compute $a^b \bmod c$ for positive integers a, b, c .
2. (10 points) 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?
 - (b) List the elements of this group?
 - (c) What does $\phi(35)$ mean?
3. (15 points) Consider the following sub-problems.
 - (a) Let $m = m_1 m_2$ such that $\gcd(m_1, m_2) = 1$, and $y \in \mathbb{Z}_m$. Given $a_1 = y \bmod m_1$ and $a_2 = y \bmod m_2$, prove the Chinese Remainder Theorem in this specific case.
 - (b) Compute $101^{4,800,000,023} \bmod 35$ without using a calculator. Show all work. (Hint: use CRT etc.)

4. (10 points) 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^* .
- Prove that x_1x_2 is a quadratic residue.
 - Prove that $x_1^{-1} \bmod p$ is a quadratic residue.
 - Prove that x_1y is *not* a quadratic residue.
5. (15 points) Let p be a prime such that $p = 3 \bmod 4$. Let $x \in \mathbb{Z}_p^*$ be a quadratic residue.
- Show that $x^{(p+1)/4} \bmod p$ can be computed in time $O(\text{poly}(|p|))$.
 - Show that $x^{(p+1)/4}$ gives a square root of x . (Hint: use the fact that $y^{p-1} = 1 \bmod p$ for any $y \in \mathbb{Z}_p^*$ and the fact that x is a quadratic residue.)
 - How would you find both square roots of x ?
6. (10 points) Show that given n and $\phi(n) = (p-1)(q-1)$, one can factor n in polynomial-time.
7. (10 points) 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 $G_k(x) = F_k(x) \parallel F_k(\bar{x})$, 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.
8. (15 points) As we covered in the lecture the “birthday paradox” in terms of balls-and-bins, suppose $C(N, q)$ is the probability that there are at least one collision when we throw $q \geq 1$ balls into $q \leq N$ bins, where $1 \leq q^2 \leq 2N$.
- State the inequality you need to finish your proof.
 - Prove

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