

Homework #2

Due date & time: 10:30am on February 16, 2012. Hand in at the beginning of class (preferred), or email to the TA (jiang97@purdue.edu) by the due time.

Late Policy: You have three extra days in total for all your homeworks. Any portion of a day used counts as one day; that is, you have to use integer number of late days each time. If you emailed your homework to the TA by 10:30am the day after it was due, then you have used one extra day. If you exhaust your three late days, any late homework won't be graded.

Additional Instructions: The submitted homework must be typed. Using Latex is recommended, but not required.

Problem 1 (12 pts) Number theory exercises. Write out the intermediate steps to show that you understand the algorithm. Do not include just the final answer.

- Use the Extended Euclidean Algorithm to compute the multiplicative inverse: (a) $17^{-1} \pmod{113}$, (b) $271^{-1} \pmod{1009}$.
- Compute $\gcd(57, 93)$ and find integers s and t such that $57s + 93t = \gcd(57, 93)$.
- Solve the linear congruence equation $19x \equiv 8 \pmod{97}$.
- Solve the linear congruence equation $20x \equiv 8 \pmod{96}$.
- Solve the linear congruence equation $20x \equiv 8 \pmod{95}$.

Problem 2 (6 pts) An integer a is called square-free if it is not divisible by the square of any integer greater than 1. Show that:

- (a) A number a is square-free if and only if $a = \pm p_1 \cdots p_r$, where the p_i 's are distinct primes;
- (b) Every positive integer n can be expressed uniquely as $n = ab^2$, where a and b are positive integers, and a is square-free.

Hint. The Fundamental Theorem of Arithmetic may be helpful.

Problem 3 (6 pts) Prove that if $k \leftarrow \{0, 1\}^n$ is drawn at uniform random, then for any probability distribution D over $\{0, 1\}^n$, when x is drawn from the distribution, both $(k + x \pmod{2^n})$ and $k \oplus x$, where \oplus denotes bit-by-bit XOR, have uniform random distribution. That is, you need to show that for any $v \in \{0, 1\}^n$, we have $\Pr[(k + x \pmod{2^n}) = v] = \frac{1}{2^n}$ and $\Pr[k \oplus x = v] = \frac{1}{2^n}$

Problem 4 (10 pts) (Katz and Lindell. Page 106. Exercise 3.1.)

Problem 5 (5 pts) (Katz and Lindell. Page 106. Exercise 3.2.)

Problem 6 (5 pts) (Katz and Lindell. Page 106. Exercise 3.4.)

Problem 7 (6 pts) (Katz and Lindell. Page 106. Exercise 3.6. With slight modifications.)

Let G be a pseudorandom generator where $|G(s)| > 4 \cdot |s|$.

- (a) Define $G'(s) \stackrel{\text{def}}{=} G(s0^{|s|})$. That is $G'(s)$ invokes G with a concatenation of s and a string of 0's of the same length as s . Is G' necessarily a pseudorandom generator?
- (b) Define $G'(s) \stackrel{\text{def}}{=} G(s_1 \cdots s_{n/2})$, where $s = s_1 \cdots s_n$. Is G' necessarily a pseudorandom generator?

Problem 8 (10 pts) (Katz and Lindell. Page 107. Exercise 3.9.)

Problem 9 (12 pts) (Katz and Lindell. Page 107. Exercise 3.15.)

Problem 10 (13 pts) Let p be a 128-bit prime and let \mathbb{Z}_p be the set of integers $\{0, \dots, p-1\}$. Consider the following encryption scheme. The secret key is a pair of integers $a, b \in \mathbb{Z}_p$ where $a \neq 0$. To encrypt a message $m \in \mathbb{Z}_p$, one chooses $r \leftarrow \mathbb{Z}_p$ uniformly at random and compute:

$$\text{Enc}_{a,b}[M] = \langle r, (ar + b + m) \bmod p \rangle$$

- (5 pts)** Show that when this scheme is used to encrypt a single message $m \in \mathbb{Z}_p$ the system has perfect secrecy.
- (8 pts)** Show that the system is insecure when encrypting multiple messages, i.e., it *does not* have indistinguishable *multiple encryptions*. That is, give an algorithm \mathcal{A} that can win the $\text{PrivK}^{\text{mult}}$ experiment with non-negligible probability.

Problem 11 (15 pts) Conduct an analysis of the security of RC4 and write a summary. The summary should include: (a) the currently most effective attacks against RC4 (how much time and how many messages are needed, the basic ideas); (b) the recommendation on how to use RC4 for encrypting multiple messages. One starting point is the wikipedia page for RC4.