

Homework is due at the *start of class*, on the date listed above. **Problems numbered G# need only be completed by graduate students.**

0. *This problem is a reading exercise, and will not be graded.* Read Section 5.3 of Stinson (pages 167–171), “The RSA Cryptosystem”.
1. This problem suggests a concrete approach to generating large primes. Let  $k$  be a large integer, and suppose we try to generate a random  $k$ -bit prime  $p$  as follows. (i) Generate a random integer  $p$  in the range  $[2^{k-1}, 2^k - 1]$ . (ii) Use a deterministic primality test to check if  $p$  is prime; if  $p$  is not a prime, then reject  $p$ .  
Suppose we repeat the above  $k^3$  times. Show that the probability that we always rejected the number chosen, is very small. (**Hints:** Let  $\pi(t)$  denote the number of primes in the range  $\{1, 2, \dots, t\}$ , as usual. Use the approximation  $\pi(t) \sim t/\ln t$  for large  $t$ ; in particular, assume  $\pi(t) = t/\ln t$ . Also use the fact that  $1 - x \leq e^{-x}$ .)
2. Let  $p, q$  be distinct odd primes, and let  $N = pq$ ; let  $\mathcal{J}_N(y)$  denote the Jacobi symbol of an element  $y$  of  $Z_N^*$ .
  - (a) Show that for  $x, y \in Z_N^*$ ,  $\mathcal{J}_N(xy) = \mathcal{J}_N(x) \cdot \mathcal{J}_N(y)$ .
  - (b) Suppose  $p$  and  $q$  are known. Give a randomized polynomial-time algorithm to generate a quadratic non-residue  $y \in Z_N^*$ , such that  $\mathcal{J}_N(y) = 1$ . (The algorithm is allowed to “give up” with some small probability; with high probability, it should do the given task in polynomial time.)
  - (c) Read the three-step encryption scheme based on the hardness of quadratic residuosity, from page 2 of Jonathan Katz’s lecture 29; we also covered this in class. Prove rigorously that in step 2 (which describes the encryption),  $C$  is indeed a random quadratic residue or a random quadratic non-residue with Jacobi symbol  $+1$ , in the respective cases of encrypting 0 and 1. (When we say “random” here, it is meant in the rigorous sense of “chosen uniformly at random”).
3. Stinson, problem 5.14, page 221.
- G1. (**For graduate students only.**) Stinson, problem 5.15 (both parts (a) and (b)), pages 221–222.