

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 Jonathan Katz's Lecture 7 from his Fall 2002 course: <http://www.cs.umd.edu/~jkatz/crypto/lectures/lecture7.pdf>, especially the material on the Legendre symbol \mathcal{L}_p , the Jacobi symbol \mathcal{J}_N , and Section 3.1 on making Rabin's function a permutation.

1. Suppose p is a prime.

(a) Show that for $x, y \in Z_p^*$, $\mathcal{L}_p(xy) = \mathcal{L}_p(x) \cdot \mathcal{L}_p(y)$.

(b) Let g be a generator of Z_p^* . Show that for $x \in Z_p^*$, $\mathcal{L}_p(x) = 1$ iff $x = g^{2i}$ for some integer i .

2. Recall from problem 0 above that Rabin's function becomes a permutation mapping QR_N to QR_N , if $N = pq$ where p, q are distinct primes that are each congruent to 3 mod 4. Adapt the proof given in class, to show that this permutation is one-way iff factoring is hard.

3. Read Problem Set 2 from Jonathan Katz's Fall 2002 course and its solutions, available at

<http://www.cs.umd.edu/~jkatz/crypto/handouts.html>, and problems 3 and 4 there in particular. This is to strengthen your understanding of PRGs.

Now suppose $G : \{0, 1\}^k \rightarrow \{0, 1\}^{k+1}$ is a PRG. Let A be the event that when a string x is chosen uniformly at random from $\{0, 1\}^k$, then the string $G(x)$ has at least $\lceil 2 \log_2 k \rceil$ consecutive zeroes in it. Show that the probability of event A *cannot* be negligible. (**Hint:** Suppose a string y is chosen uniformly at random from $\{0, 1\}^{k+1}$. What is the probability that the first $\lceil 2 \log_2 k \rceil$ bits of y are all zero?)

G1. (**For graduate students only.**) Show that in problem 3, the probability of event A must tend to zero as $k \rightarrow \infty$.

Hint: Let " \vee " denote the "or" symbol as usual. Then, for any events B_1, B_2, \dots, B_t ,

$$\Pr[B_1 \vee B_2 \vee \dots \vee B_t] \leq \sum_{i=1}^t \Pr[B_i].$$