

# Theoretical Foundations of Cryptography

close-book midterm exam

May 20, 2003

## Instructions

- Cheating will be most seriously punished. Any dishonest attempt from any person in this exam immediately implies an "F" as his/her final grade.
- This is designed to be a 2.5-hour exam. So, you should be able to answer each problem in roughly 30 minutes. You may answer the problems in any order.

### Problem 1 (20 points)

- (5 points) Explain what is a strongly one-way function.
- (5 points) Explain why  $\mathbf{NP} = \mathbf{P}$  implies that there is no strongly one-way function.
- (10 points) Suppose that  $f$  is a function with  $|f(x)| \leq \log_2 |x|$ . (So,  $f$  is not length-preserving.) Explain why  $f$  is definitely not a strongly one-way function (under the assumption that  $\mathbf{NP} \neq \mathbf{P}$ ).

### Problem 2 (20 points)

- (5 points) Explain what is a hard-core predicate.
- (15 points) Let  $G_\ell$  be a pseudorandom generator with extension factor  $\ell(n) = n + 1$ . (That is, we have  $|G_\ell(x)| = |x| + 1$ .) You are asked to *explicitly* give two functions  $h$  and  $f$ , based upon  $G_\ell$ , such that  $h$  is a hard-core predicate of  $f$ . You are welcome to directly use any results that we proved in the class as subroutines of your answer. If you use anything else, please provide its proof.

### Problem 3 (20 points)

Let  $X = \{X_n\}_{n \in \mathbb{N}}$  be a probabilistic ensemble.

- (5 points) What do we mean by “ $X$  is pseudorandom”? (Well, you might also have to explain the concept of “indistinguishability” for this problem.)
- (5 points) What do we mean by “ $X$  is unpredictable”?
- (10 points) Prove that “ $X$  is pseudorandom” implies “ $X$  is unpredictable”.

### Problem 4 (20 points)

Let  $G_\ell$  be a pseudorandom generator with extension factor  $\ell(n) = n + 1$ . Prove that  $H_r$  with  $H_r(x) = G_\ell(G_\ell(x))$  is a pseudorandom generator with extension factor  $r(n) = n + 2$ .

### Problem 5 (20 points)

1. (10 points) What is an interactive proof system?
2. (10 points) Give an interactive proof system for the GRAPH ISOMORPHISM problem. Justify your answer.