# Foundations of Cryptography

Homework Set No. 7

Date Due: January 8th 2004

Assume one-way functions exist.

1. Show that the last bit/first bit are not necessarily hardcore predicates.

2. Generalization: show that for any fixed function $h : \{0,1\}^* \mapsto \{0,1\}$ there is a one-way function $f : \{0,1\}^* \mapsto \{0,1\}^*$ such that $h$ is *not* a hardcore predicate of $f$.

3. Show a one-way function $f$ such that given $y = f(x)$ each input bit of $x$ can be guessed with probability at least 3/4