CS355: Topics in cryptography **Fall 2002**

Assignment 0.5: Warm-Up Questions

The purpose of these exercises is to illustrate the definitions that we learned in the class. Make sure that you understand the question, know the right answer, and can give an explanation (either a proof or a counterexample). If you need help, come during the office hours to Dan Boneh or Ilya Mironov.

1. Let $g \in \mathbb{Z}_q$ be an element of order p and x be an integer between 1 and p. Numbers p and q are prime, $p > 2^{160}$ and $q > 2^{1024}$. We define two functions $s_g(y) = g^y \colon \mathbb{Z}_p \mapsto \langle g \rangle$ and $t_x(h) = h^x \colon \langle g \rangle \mapsto \langle g \rangle$. Are $s_g(\cdot)$ and $t_x(\cdot)$ one-way? Are they pseudo-random?

2. DES is a secure block cipher with block length 64 bits and key length 56 bits. How would you construct a one-way function from DES? A pseudo-random number generator? A pseudo-random function? Try to estimate security of your constructions in the (t, ε, q) notation.

3. Your company has licensed a one-way permutation $F : \{0,1\}^{160} \mapsto \{0,1\}^{160}$ with a guarantee that the 80 least significant bits of the input are simultaneously hardcore. Having taken the CS355 course, you suggested to apply the Blum-Micali construction that outputs 80 bits at a time to construct an efficient pseudo-random number generator based on F. This suggestion was enthusiastically approved by your boss, it was built into the main product and you got a raise in salary. All of a sudden, an attack on F is published that, given any $F(x)$, correctly determines 10 independent linear combinations of bits from the lower half of x (say, the xor of all 80 lower half of the bits of x, the xor of every other bit from the 80 lower half of x, etc.). A rumor floated that the generator is no longer secure. How do you fix the generator?