Final Exam Info and Sample Questions

The BU CAS CS 538 final exam will be held Monday, December 17, 12:30-2:30 PM in our usual classroom. **Please do not be late. The exam will end promptly at 2:30 pm.** Recall that the exam counts for 30% of your grade.

You are allowed to bring two double-sided letter-size ($8\frac{1}{2} \times 11$ inches) sheets of paper with whatever information you want on them, subject to the following restriction: these sheets must be *handwritten by you personally.* Photocopied, typewritten, computer printed, etc., sheets are not allowed. The reason for this requirement is simple: the benefit derived from these sheets of paper comes primarily not from the help they provide you during the exam, but from the help they provide you during their preparation, forcing you to systematically go over the class and pick out the most important topics.

I will be checking that this condition is adhered to, but will not check the contents of these sheets otherwise. It's entirely up to you what to put on them. You are allowed to use these sheets and nothing else during the exam—no books, no lecture notes, etc. Oh, and please bring two pens/pencils that work.

Everything we studied during the semester (including homeworks and solutions) is fair game for the exam. However, naturally, the focus will be on fundamental concepts and constructions. Questions will be mostly short-answer with justification (no lengthy proofs, but proof outlines or "complete this proof" are fair game).

Below are some questions of the type that may appear on the exam. Note that the actual exam will contain more that four such questions, and they will cover a broader range of topics.

Problem 1. Consider the following attempt at constructing a signature scheme.

- G generates two primes, p_1 and p_2, as the secret key, and $n = p_1 p_2$ as the public key.
- S can only sign messages m that are squares modulo n. When input p_1, p_2 and m, S outputs σ such that $\sigma^2 \equiv m \pmod{n}$.
- V, on input n, m, σ, checks if $\sigma^2 \equiv m \pmod{n}$.

Show that this scheme is insecure in the following sense: an attacker carrying out an adaptive chosen-message attack can recover the secret key with high probability.

Problem 2. WeEncrypt, Inc., has designed the following public-key cryptosystem. Take any trapdoor permutation family $\{f_i : D_i \to D_i\}$. The public key is a permutation index i selected at random from the family, and the secret key is the information t needed to invert it. To encrypt a message $m \in D_i$, simply compute $c = f_i(m)$. Is this a secure cryptosystem? Justify your answer.

Problem 3. Let a public key for the Blum-Goldwasser cryptosystem be $n = p_1 p_2$, where p_1 and p_2 are k-bit primes. How many possible ciphertexts are there for a given plaintext m of length l?

Problem 4. Let f be a one-way permutation. Let B be a hardcore predicate for it. Consider the following function g: $g(x) = f(x) \circ B(x)$. Is g necessarily one-way? Justify your answer.