Homework 5

MARCH 7

Due by the **start of class on THURSDAY, MARCH 16** (differs from the usual date). Start early!

Instructions. Your solutions will be graded on *correctness* and *clarity*. You should only submit work that you believe to be correct; if you cannot solve a problem completely, you will get significantly more partial credit if you clearly identify the gap(s) in your solution. It is good practice to start any long solution with an informal (but accurate) "proof summary" that describes the main idea. For this problem set, a random subset of problems will be graded.

You may collaborate with others on this problem set. However, you must ***write up your own solutions*** and ***list your collaborators*** for each problem.

1. (12 points) Information-theoretical secure MAC and digital signature.
   (a) (6 points) A MAC is *perfectly* secure if the probability that any adversary, possibly unbounded, produces a forgery is 0. Give a formal definition under chosen-message-attacks. Is perfectly secure MAC possible? Justify your answer.
   Note. We may relax the above definition to allow "small" probability of break, and call it information-theoretical secure (IT-secure) MAC. Efficient constructions of IT-secure MACs exist.
   (b) (6 points) Describe analogously informal definitions for perfectly secure and IT-secure digital signatures. Are they possible to exist? Justify your answer.

2. (10 points) "Textbook" RSA signature.
   (a) (5 points) [KL: Exercise 12.3] Forge on arbitrary message with one signing query.
   (b) (5 points) [KL: Exercise 12.4] Uniform unforgeable against no-message attacks.

3. (5 points) [KL: Exercise 12.10] Attack on Lamport's one-time signature.

4. (10 points) Oblivious transfer from trapdoor permutations. Let (G, F, I) be a trapdoor one-way permutation on $\{0,1\}^n$ and $\mathsf{hc} : \{0,1\}^n \to \{0,1\}$ a hard-core predicate of F. Consider the following protocol:

   > Input to Alice: $s_0, s_1 \in \{0,1\}$; input to Bob: choice bit $c \in \{0,1\}$.
   >
   > - $A \to B$: Alice generates $(pk, sk) \leftarrow G(1^n)$. Send pk to Bob.
   > - $B \to A$: Bob samples $x, y \leftarrow \{0,1\}^n$. Let $x_c := x$. Compute $y_c := F_{pk}(x_c)$ and $y_{1-c} := y$. Send (y_0, y_1) to Alice.
   > - $A \to B$: Alice inverts (y_0, y_1) using sk and gets x_0, x_1. Send $(z_0 := \mathsf{hc}(x_0) \oplus s_0, z_1 := \mathsf{hc}(x_1) \oplus s_1)$ to Bob.
   > - Bob computes $s_c := \mathsf{hc}(x_c) \oplus z_c$.

   (a) (2 points) Verify that this is a correct oblivious transfer protocol.
   (b) (3 points) Show that an semi-honest Alice cannot learn c. (Hint: is Alice's view (y_0, y_1) dependent on c?)
   (c) (Bonus 5pts) Show that an semi-honest Bob cannot recover s_{1-c}.