Homework 4

FEBRUARY 21

Due by the **start of class on TUESDAY, MARCH 07**. 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. Number theory

   (a) (6 points) [KL: Exercise 8.9] Let p, N be integers with $p|N$.

      i) Prove that for any integer X, $[[X \bmod N] \bmod p] = [X \bmod p]$.

      ii) Show that, in contrast, $[[X \bmod p] \bmod N]$ need not equal $[X \bmod N]$.

   (b) (6 points) Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time. (Hint: derive a quadratic equation over the integers in the unknown p.)

   (c) (Bonus 5 points) [KL: Exercise 8.14]

2. Key-exchange

   (a) (4 points) [KL: Exercise 10.3] Describe a man-in-the-middle attack on the Diffie-Hellman protocol where the adversary shares a key k_A with Alice and a different key k_B with Bob, and Alice and Bob cannot detect anything is wrong.

   (b) (6 points) [KL: Exercise 10.4]

3. PKC

   (a) (5 points) [KL: Exercise 11.4] Show that any two-round key-exchange protocol (i.e., each party sends a single message) satisfying Definition 10.1 can be converted into a CPA-secure public-key encryption scheme.

   (b) (5 points) Show that the El Gamal scheme ([KL: Construction 11.16]) has the following property: given a public key pk, and two ciphertexts $c_1 \leftarrow E(pk, m1)$ and $c_2 \leftarrow E(pk, m2)$, it is possible to create a new ciphertext c which is an encryption of $m_1 \cdot m_2$. This property is called a *multiplicative homomorphism*.

   (c) (6 points) [KL: Exercise 11.6]

4. CCA

   (a) (5 points) Let $\Pi = (G, E, D)$ be an public-key encryption scheme for single-bit messages. Consider a new scheme $\Pi' = (G, E', D')$ that has message space $\{0,1\}^*$ and $E'_{pk}(m) := E'_{pk}(m_1), \ldots, E'_{pk}(m_\ell)$ where $m = m_1 \ldots m_\ell$. D' is done in the natural way. Suppose Π is CCA-secure, is Π' CCA-secure? Justify your answer.

   (b) (Bonus 5 points) [KL: Exercise 11.17]