Homework 10: Public key crypto review

Total of 120 points

(Most of this exercise is a review exercise on some of the notions we have encountered before.)

1. (25 points) Suppose that there exists an efficient algorithm A that on input m and $a \in \mathbb{Z}_m^*$ outputs the smallest number r such that $a^r = 1(\mod m)$. Prove that under this assumption there is an efficient (probabilistic) algorithm B that on input $m = pq$ with $q(\mod 4) = p(\mod 4) = 3$, outputs p and q. You can follow the outline of the lecture notes, or see the footnote for hint on another approach[1]

2. (50 points) Consider the following proof system for Alice to prove to Bob that a graph is 3 colorable:

- **Common input:** Graph $G = (V, E)$ on n vertices.
- **Alice (Prover) private input:** A function $f : V \rightarrow \{1, 2, 3\}$ such that $f(i) \neq f(j)$ for every $\{i, j\} \in E$.
- **Step 1: Alice <- Bob:** Bob selects $z, z' \leftarrow_R \{0,1\}^{10n}$ and sends z, z' to Alice.
- **Step 2: Alice -> Bob:** Alice selects π to be a random permutation over $\{1, 2, 3\}$ and defines the functions $f' : V \rightarrow \{1, 2, 3\}$ as $f'(i) = \pi(f(i))$. For $i = 1..n$, Alice chooses $w_i \leftarrow_R \{0,1\}^n$ and sends to Bob $y_i = PRG(w_i) + f'(i)z + (f'(i) \mod 3)z'(\mod 2)$ where $PRG : \{0,1\}^n \rightarrow \{0,1\}^{10n}$ is a pseudorandom generator and vector addition and vector/scalar multiplication are defined as usual.
- **Step 3: Bob <- Alice:** Bob selects a random edge $\{i, j\} \in E$ and sends i and j to Alice.

[1] For starters, you can assume for partial credit the following claim: with probability at least 1/100, if we pick a random $a \in \mathbb{Z}_m^*$ then a will have an even order and $a^{r/2} \neq -1(\mod m)$. Using the claim you can reduce factoring to order finding in a similar way to how we reduced factoring to finding square roots. For full credit, prove the claim by first proving using the chinese remainder theorem that for every a, the order of a modulo m is the least common multiple of the order of a modulo P and the order of a modulo q, and then use the fact that for every group G, if $G' \neq G$ is a subgroup of G then $|G|/|G'| \geq 2$.

- **Step 4: Alice -> Bob:** Alice checks that $\{i, j\} \in E$ (otherwise she aborts) and if so sends the strings w_i, w_j and the values $f'(i), f'(j)$.
- **Bob's decision:** Bob accepts the proof iff $f'(i), f'(j)$ as sent by Alice are two distinct numbers in $\{1, 2, 3\}$ and the strings she sent satisfy the equations $y_i = PRG(w_i) + f'(i)z + (f'(i) \mod 3)z' (\mod 2)$ and $y_j = PRG(w_j) + f'(j)z + (f'(j) \mod 3)z' (\mod 2)$

Prove that this system is a zero knowledge proof system for the 3 coloring problem by showing the following:

a. (Completeness, 10 points): Prove that if Alice and Bob are given inputs as above and both follow the protocol then Bob will accept the proof with probability 1.

b. (Soundness, 15 points): Prove that if there exists no 3-coloring for G (i.e., for every coloring of G's vertices in $\{1, 2, 3\}$ there is some edge $\{i, j\}$ such that both i and j receive the same color), then with probability at least $1/(10n^2)$ Bob will reject the proof. (This probability can be amplified to more than $1 - 2^{-k}$ by $100kn^2$ repetitions).

c. (Zero knowledge, 25 points) Prove that for every polynomial-time strategy B^* used by Bob, there exists an efficient algorithm S^*, so that for every 3-colorable graph G and coloring f, the output of $S^*(G)$ is computationally indistinguishabl from the transcript B^* observes after interacting with the honest strategy of Alice on public input G and private input x. (For partial credit of 15 points, prove only *honest verifier zero knowledge* : that the above holds when B^* is the honest strategy of Bob.)

3. KL 11.17 (20 points)
4. KL 12.14 (10 points)
5. KL 13.17 (15 points)