Homework 3

Due date: Thursday, November 2nd 9:00 AM

Question 1 (20 points)

Given root $\stackrel{\text{def}}{=} \mathcal{MT}(x_1, ..., x_n)$ where $\mathcal{MT}(\cdot)$ is the Merkle Tree Hash, it is easy to prove that $x \in \{x_1, ..., x_n\}$. However, it's not clear how to efficiently prove that $x \notin \{x_1, ..., x_n\}$. Propose a solution to prove non-membership of some x using Merkle Tree Hash. Your solutions should still allow for efficient proofs of membership, and it should take time $O(n \log n)$ to construct the (modified) Merkle Tree given inputs $x_1, \ldots, x_n$. **Hint:** What famous algorithm runs in time $O(n \log n)$?

Question 2 (20 points)

Let f be a one-way function. Are the following functions necessarily a one-way function. Prove your answer

1. $g(x) = f(f(x))$
2. $g(x) = f(x)||f(f(x))$

Question 3 (20 points)

Let $x \in \{0,1\}^n$ and denote $x_1, \ldots, x_n$ as the bits of x. Prove that if there exists a one-way function, then there exists a one-way function f such that for every i there is an algorithm $A_i(f(x))$, which successfully predicts the i^{th} bit x_i of x with probability

$$\Pr_{x \leftarrow \{0,1\}^n}\left[A_i(f(x)) = x_i\right] \geq \frac{1}{2} + \frac{1}{2n} .$$

Question 4 (15 points)

- Compute $3^{302} \mod 385$ (by hand) **Hint:** Use the Chinese Remainder Theorem and the fact that $385 = 5 \times 7 \times 11$.
- Use extended Euclidean algorithm to compute: $\mathsf{gcd}(1234, 4321)$.
- Show that if $N = p \cdot q$ for distinct primes $p > q > 1$ and $ed = 1 \mod (p-1)(q-1)$ then for all $x \in Z_N^*$ we have $(x^e)^d = x \mod N$

Question 5 (25 points)

Fix $N \in \mathbb{N}$ such that $N, e \geq 1$ and $\texttt{gcd}(e, \phi(N)) = 1$. Assume that there is an adversary $\mathcal{A}$ running in time t such that

$$\Pr\left[\mathcal{A}\left(\left[x^e \mod N\right]\right) = x\right] \geq 0.01$$

where the probability is taken over the uniform choice of $x \in \mathbb{Z}_N^*$. Show how to construct an adversary $\mathcal{A}'$ with running time $t' = O\left(poly\left(t, \log_2 N\right)\right)$ such that

$$\Pr\left[\mathcal{A}'\left(\left[x^e \mod N\right]\right) = x\right] \geq 0.99\ .$$

Hint: Use the fact that $y^{1/e} \cdot r = \left(y \cdot r^e\right)^{1/e} \mod N$. Here, $y^{1/e} = y^d \in \mathbb{Z}_N^*$ where d is a (secret) number such that $ed \equiv 1 \mod \phi(N)$. Also use the fact that, given $r \in \mathbb{Z}_N^*$, we can find a number r^{-1} such that $rr^{-1} = 1 \mod N$.