1 Fun with the Blum TDP

The Blum trapdoor permutation works as follows:

- **Key generation:** On input the security parameter $1^k$, produce modulus $N = pq$, where $p$ and $q$ are both random $k$-bit primes such that $p \equiv q \equiv 3 \pmod{4}$. Let the keys be $pk = N$ and $sk = \{p, q\}$.

- **Sampling the domain:** The domain of this permutation consists of the squares mod $N$. To sample from the domain, pick a random $z \leftarrow \mathbb{Z}_N^*$ and output $x = z^2 \pmod{N}$. We denote this domain by $\text{QR}_N$, for “quadratic residues.”

- **Computing the permutation:** The permutation itself is simply squaring; that is, $f_N(x) = x^2 \pmod{N}$.

In this problem, you will analyze the Blum TDP.

a. Prove that for all $N$, $f_N$ is a permutation over $\text{QR}_N$. Here is a suggested outline (however, you are free to do it in any method you prefer):

   (1) Show that for a prime $p$, $x^{(p-1)/2} \equiv 1 \pmod{p}$ if and only if $x$ is a square mod $p$.
   (2) Show that for a prime $p \equiv 3 \pmod{4}$, $-1$ is not a square mod $p$.
   (3) Infer that if $x$ is a square mod $p$ and $p \equiv 3 \pmod{4}$, then $x$ has a unique square root mod $p$ that is itself a square.
   (4) Use the Chinese remainder theorem to show that it follows that $f_N$ is a permutation.

b. Prove the following lemma: If $p = 4m + 3$ is prime and $a$ is a quadratic residue mod $p$, then $a^{m+1}$ is a square root of $a$ mod $p$.

c. Give an algorithm for computing $f_N^{-1}$ given the trapdoor $\{p, q\}$.

   **Hint:** Use what you just proved and the Chinese remainder theorem.

d. Suppose we are given $x$ and $y$ where $x \neq \pm y \pmod{N}$ and $x^2 \equiv y^2 \pmod{N}$. What can you infer about the value $x - y \pmod{N}$? Show how to use this value to factor $N$. 

Homework 4
e. Suppose we have a polynomial-time adversary $A$ that breaks the Blum TDP. We wish to show that this implies a polynomial-time algorithm for factoring the corresponding modulus. Consider the following reduction $B$: On input $N$, set $x \leftarrow \mathbb{Z}_N^*$ and run $A(N, x^2 \pmod{N})$ to obtain some $y$. If $y \neq \pm x \pmod{N}$, then use part (d) above to factor $N$.

Analyze this reduction.

2 One-Way Functions Under XOR

Let $f_1$ and $f_2$ be one-way functions with the same size output. That is, if $|x_1| = |x_2|$, then $|f(x_1)| = |f(x_2)|$. Now consider $f(x) = f_1(x_1) \oplus f_2(x_2)$, where $x = x_1 \circ x_2$ such that $|x_1| = \left\lceil \frac{|x|}{2} \right\rceil$ and $|x_2| = \left\lfloor \frac{|x|}{2} \right\rfloor$. When XORing strings of unequal length, you can pretend that blank characters at the ends of the shorter strings are 0’s.

a. Assuming that length-preserving one-way functions exist, give an example of OWFs $f_1$ and $f_2$ such that $f$ is a OWF. Prove that $f_1$, $f_2$, and $f$ are OWFs.

b. Assuming that length-preserving one-way functions exist, give an example of OWFs $f_1$ and $f_2$ such that $f$ is not a OWF. Prove that $f_1$ and $f_2$ are OWFs, and that $f$ is not a OWF.