Recall the definitions:

**Definition 1** A function \( f : \mathbb{N} \to \mathbb{R}^+ \) is negligible if for all large enough \( n \) we have \( f(n) < 1/n^c \). (By “for all large enough \( n \)...” we mean “for any any \( c > 0 \) there exists an \( n_c \) such that for all \( n > n_c \)...”.)

**Definition 2** A function \( f : \{0,1\}^* \to \{0,1\}^* \) is one way if for any feasible adversary \( \{A_n\}_{n \in \mathbb{N}} \) and for all large enough \( n \in \mathbb{N} \) we have

\[
\text{Prob}[x \leftarrow R \{0,1\}^n; x' \leftarrow A(1^n, f(x)) : f(x') = f(x)] < \nu(n)
\]

where \( \nu() \) is a negligible function.

**Definition 3** A function \( f : \{0,1\}^* \to \{0,1\}^* \) is weakly one way if there exists a constant \( c > 0 \) such that for any \( \{A_n\}_{n \in \mathbb{N}} \) and for all large enough \( n \in \mathbb{N} \) we have

\[
\text{Prob}[x \leftarrow R \{0,1\}^n; x' \leftarrow A(1^n, f(x)) : f(x') = f(x)] < 1 - n^{-c}.
\]

**Question 1 (25%)**: Show that if \( f \) is a one way function with respect to deterministic feasible adversaries then it is one way also against randomized feasible adversaries.

Hint: Show that for any \( n \) and any randomized adversary \( A_n \) there exists a specific set of random choices for \( A_n \) that maximizes the success probability of \( A_n \).

(Remark: The standard term for what we called in class “feasible adversary” is “non-uniform polynomial time algorithm”. The term “non-uniform” comes from the fact that for any \( n \) the algorithm \( A_n \) is different, and there isn’t necessarily a uniform way to represent the \( A_n \)’s for all \( n \in \mathbb{N} \).)

**Question 2 (25%)**: Learning Parity with Noise (LPN) is another example of a hard problem that people have been using in cryptography. The problem comes from learning theory. Specifically, the **LPN assumption** states that for any feasible (i.e., non-uniform polytime) adversary \( \{A_n\}_{n \in \mathbb{N}} \) and for all large enough \( n \in \mathbb{N} \) we have:

\[
\text{Prob}[s \leftarrow R \{0,1\}^n; r_1...r_m \leftarrow R \{0,1\}^n) \mu; d_1...d_m \leftarrow R D; s \leftarrow A(r_1, <r_1, s> + d_1, ..., r_m, <r_m, s> + d_m)] < \nu(n)
\]

where \( \nu() \) is a negligible function, \( m = n^2 \), and \( D \) is a distribution over \( \{0,1\}^n \) where the probability of 1 is 1/\( \sqrt{n} \). Here \( s \) is thought of as the ”secret”, and \( <r, s> \) denotes the inner product between \( s \) and \( r \). That is, let \( s = \sigma_1...\sigma_n \) and \( r = \rho_1...\rho_n \) where the \( \sigma_i \)’s and \( \rho_i \)’s are bits. Then, \( <s, r> = \sum_{i=1}^n \sigma_i \cdot \rho_i \mod 2 \).

The values \( d_1...d_m \) represent “noise”, or errors. (Note that if the \( d_i \)’s are all 0’s then the problem would be easy (why?) and if the \( d_i \)’s are distributed uniformly in \( \{0,1\} \) then there are so many solutions that the problem becomes easy again. Consequently, we are interested in the case where the \( d_i \)’s are 1 with some small but non-zero probability.

Write a function \( f \) and prove that \( f \) is one way if and only if the LPN assumption holds.

**Question 3 (40%)**: Let \( P = \{(p_n; g_n)\}_{n \in \mathbb{N}} \) be such that \( 2^n < p_n < 2^{n+1} \) is a prime and \( g_n \) is a generator of the group \( Z_{p_n}^* \). Further, assume that \( p_n \) and \( g_n \) can be computed in polynomial time from \( 1^n \). The exponentiation function \( EXP : Z_{p_n}^* \to Z_{p_n}^* \) is defined as \( EXP(x) = g_n^x \mod p_n \), where \( n = |x| \). Prove that \( EXP \) is one way iff it is weakly one-way.

Hint: Us the algebraic properties of the modular exponentiation function to boost the success probability of any adversary that succeeds with some non-negligible probability.

**Question 4 (20%)**: Show that if there exist one way functions then there exist one way functions that are length preserving.
Question 5 (20 %): Show that if there exist one way functions then there exist one way functions where the first half of the bits of the input are copied to the output. That is, a function $f : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is first-half-preserving if for any $x = x_1, x_2$ where $|x_1| = |x_2|$ we have that $f(x) = y_1, y_2$ where $y_1 = x_1$. Then, show that if there exist one way functions then there exist one way functions that are first-half-preserving.

Note that the overall number of points is 130. This means that you have a built in 30 points bonus if you solve all questions.