HW 1 (Due before Feb. 18, 3.45pm)

Exercise 1. *Random Self-Reducibility*

The notion of *random self-reducibility* states that, if there exists an efficient algorithm solving a problem for a non-negligible fraction of its inputs, then there exists an efficient algorithm efficiently solving the problem for any input.

1. Show that the Discrete Logarithm Problem is random self-reducible. More precisely, given a cyclic group $\mathbb{G}$ of known prime order p and public generator g, assume that there exists an efficient deterministic algorithm $\mathcal{A}$ that solves the Discrete Logarithm Problem (it takes as input $h \in \mathbb{G}$ and outputs the smallest $k \in [1, p]$ such that $g^k = h$) for a fraction $1/\mathsf{poly}(\lambda)$ of its inputs. Prove that there exists an efficient probabilistic algorithm $\mathcal{A}'$ that solves the DLP for any input $x \in \mathbb{G}$. *Hint: What is the distribution of g^B for $B \hookleftarrow U([0, p-1])$?*

2. Show that the search version of Learning with Errors is random self-reducible. More precisely, given parameters $q, m, n, B \in \mathbb{N}$ and $\mathbf{s} \in \mathbb{Z}_q^n$, the $\mathsf{sLWE}_{q,n,m,B}(\mathbf{s})$ problem is the following:

   - Find $\mathbf{s}$, given $(\mathbf{A}, \mathbf{As} + \mathbf{e})$ where $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$ and $\mathbf{e} \hookleftarrow U\left((-B, B]^m\right)$.

   Assume that there exists an efficient algorithm $\mathcal{A}$ that solves $\mathsf{sLWE}_{q,n,m,B}(\mathbf{s})$ for a fraction $1/\mathsf{poly}(\lambda)$ of $\mathbf{s}$.

   Design an efficient algorithm that solves $\mathsf{sLWE}_{q,n,m,B}(\mathbf{s})$ for any $\mathbf{s} \in \mathbb{Z}_q^n$.

3. In the tutorial we defined LWE with small secret: instead of sampling $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, we sampled and restricted our choice of secrets to $\mathbf{s} \hookleftarrow U\left((-B, B]^n\right)$. Show that if we have an adversary that distinguishes with non-negligible probability between the distribution $(\mathbf{A}, \mathbf{As} + \mathbf{e})$ for $\mathbf{A} \hookleftarrow U(\mathbb{Z}_q^{m\times n})$, $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$ and $\mathbf{e} \hookleftarrow U((-B, B]^m)$ and the uniform distribution over $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, then we can distinguish between $(\mathbf{A}, \mathbf{As} + \mathbf{e})$ where $\mathbf{A}$ and $\mathbf{e}$ are sampled as before but $s \hookleftarrow U((-B, B]^n)$ and the uniform distribution over $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$.

Exercise 2. *Security of CTR*

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF. To encrypt a message $M \in \{0,1\}^{d\cdot n}$, CTR proceeds as follows:

- Write $M = M_0 \| M_1 \| \ldots \| M_{d-1}$ with each $M_i \in \{0,1\}^n$.
- Sample IV uniformly in $\{0,1\}^n$.
- Return $IV \| C_0 \| C_1 \| \ldots \| C_{d-1}$ with $C_i = M_i \oplus F(k, IV + i \bmod 2^n)$ for all i.

The goal of this exercise is to prove the security of the CTR encryption mode against chosen plaintext attacks, when the PRF F is secure.

1. Recall the definition of security of an encryption scheme against chosen plaintext attacks.

2. Assume an attacker makes Q encryption queries. Let $IV_1, \ldots, IV_Q$ be the corresponding IV's. Let `Twice` denote the event "there exist $i, j \leq Q$ and $k_i, k_j < d$ such that $IV_i + k_i = IV_j + k_j \bmod 2^n$ and $i \neq j$." Show that the probability of `Twice` is bounded from above by $Q^2 d / 2^{n-1}$.

3. Assume the PRF F is replaced by a uniformly chosen function $f : \{0,1\}^n \to \{0,1\}^n$. Give an upper bound on the distinguishing advantage of an adversary $\mathcal{A}$ against this idealized version of CTR, as a function of d, n and the number of encryption queries Q.

4. Show that if there exists a probabilistic polynomial-time adversary $\mathcal{A}$ against CTR based on PRF F, then there exists a probabilistic polynomial-time adversary $\mathcal{B}$ against the PRF F. Give a lower bound on the advantage degradation of the reduction.