Cryptography ENEE/CMSC/MATH 456: Homework 9

*****Choose 5 out of 8*****

Due by 11:59pm on 5/10/2023.

1. Show that any 2-round key-exchange protocol (that is, where each party sends a single message) can be converted into a CPA-secure public-key encryption scheme.

2. Consider the following variant of El Gamal encryption. Let $p = 2q + 1$, let G be the group of squares modulo p, and let g be a generator of G. The private key is (G, g, q, x) and the public key is $G, g, q, h)$, where $h = g^x$ and $x \in Z_q$ is chosen uniformly. To encrypt a message $m \in Z_q$, choose a uniform $r \in Z_q$, compute $c_1 := g^r modp$ and $c_2 := h^r + mmodp$, and let the ciphertext be $\langle c_1, c_2 \rangle$. Is this scheme CPA-secure? Prove your answer.

3. In class we showed an attack on the plain RSA signature scheme in which an attacker forges a signature on an arbitrary message using two signing queries. Show how an attacker can forge a signature on an arbitrary message using a single signing query.

4. Prove that LWE with secret s chosen from the noise distribution χ is as hard as LWE with secret s chosen uniformly at random from $\mathbb{Z}_p$.

   Specifically, given $(A_1, u_1 = A_1 s + e_1 \mod p)$ and $(A_2, u_2 = A_2 s + e_2 \mod p)$, where A_1 is invertible, show how to construct an instance $(A_3, u_3 = A_3 e_1 + e_3 \mod p)$, where e_1 becomes the LWE secret.

   Hint: Consider setting $A_3 = -A_2 A_1^{-1}$.

5. Prove that Decision-LWE is as hard as Search-LWE. Specifically, show a "divide-and-conquer" attack, where given an adversary who solves Decision-LWE, it is possible to guess the entries of s one by one. Recall that the modulus p is polynomial in the security parameter.

   Hint: Consider guessing the value of the first entry of s, denoted $s_1 \in \mathbb{Z}_q$ and choosing a column vector $a' \in \mathbb{Z}_p^m$ uniformly at random. Given an LWE instance (A, u), update the instance to $(A', u + s_1 \cdot a' \mod p)$, where A' is the matrix A with column vector a' added to its first column. What is the distribution of $(A', u + s_1 \cdot a' \mod p)$ in case the guess for s_1 is correct or incorrect?

6. Two bases $B_1, B_2 \in \mathbb{Z}^{n \times n}$ define the same lattice (i.e. $\Lambda(B_1) = \Lambda(B_2)$) if and only if $B_1 = B_2 \cdot U$, where U is a *unimodular* matrix.
   Using the above fact, construct three distinct bases $B1, B2, B3$ for the lattice $\mathbb{Z}^3$.

7. Show that given an algorithm that solves the SIS problem, one can obtain an algorithm for solving the Decision-LWE problem.

   Hint: Given an input (A, u), where either $u = As + e \mod p$ or u is uniform random in $\mathbb{Z}_p^m$, consider using SIS to find a short, non-zero vector $z \in \{0, 1\}^m$ such that $zA = 0^n \mod p$. What happens in either case when you compute the inner product $\langle z, u \rangle$?

8. Show that given an algorithm that solves the SVP problem, one can obtain an algorithm for solving the SIS problem. Specifically, given $A \leftarrow \mathbb{Z}_p^{n \times m}$, define a basis B and a lattice $\Lambda(B)$ such that the shortest non-zero vector of $\Lambda(B)$ is equal to the shortest non-zero vector $z \in \mathbb{Z}_p^m$ such that $Az = 0^n \mod p$. You may assume that A is full-rank.