Cryptography: HW6

Due electronically (via TEACH) on **Friday** Mar 11

1. In a DHKA execution (using cyclic group $\mathbb{Z}_p^*$), the eavesdropper observes the following values:

   $p = 6323947392563$ $A = 6233663610066$

   $g = 2$ $B = 4871694980854$

   What will the two parties output as the shared key?

2. (a) Suppose you are given an ElGamal encryption of an unknown plaintext $M \in \mathbb{G}$. Show how to construct a different ciphertext that also decrypts to the same M.

   (b) Suppose you are given two ElGamal encryptions, of unknown plaintexts $M_1, M_2 \in \mathbb{G}$. Show how to construct a ciphertext that decrypts to their product $M_1 \cdot M_2$.

3. (a) Recall Lemma 4.8 of the notes, restated here in slightly different terms: Imagine taking q independent uniform samples $r_1, \ldots, r_q \leftarrow \mathbb{Z}_N$. When $q = \sqrt{2N}$, with probability at least 0.6 there exist $i \neq j$ such that $r_i = r_j$.

   Now consider the following modification: Before sampling, fix a value $x \in \mathbb{Z}_N$ and then proceed as above. Show that when $q = \sqrt{2N}$, with probability at least 0.6 there exist $i \neq j$ with $r_i \equiv_N r_j + x$.

   Note: The proof should be very similar to that of Lemma 4.8, so describe only the reasoning that is different. (And it should be different *somewhere!*)

   (b) Let g be a primitive root of $\mathbb{Z}_p^*$ (for some prime p). Consider the problem of computing the discrete log of $X \in \mathbb{Z}_p^*$ with respect to g — that is, finding x such that $X \equiv_p g^x$. Argue that if one can find integers r and s such that $g^r \equiv_p X \cdot g^s$ then one can compute the discrete log of X.

   (c) Combine the above two observations to describe a $O(\sqrt{p})$-time algorithm for the discrete logarithm problem in $\mathbb{Z}_p^*$.

extra credit A 2-message key-agreement protocol is one in which each user sends a single message before agreeing on a common key. Assume Alice sends the first message.

Show that a 2-message key-agreement protocol exists if and only if CPA-secure public-key encryption exists. In other words, show how to construct a CPA-secure encryption scheme from any 2-message KA protocol, and vice-versa. *Prove the security of your constructions!*

Hint: For the $\Rightarrow$ direction, take inspiration from how ElGamal is related to DHKA (a 2-message protocol). For the $\Leftarrow$ direction, it is not necessary that both users have "influence" over the choice of key. In particular, one user can simply choose the key unilaterally — the only requirement is that the key looks random to an eavesdropper.