Cryptography Foundations

Solution Exercise 7

7.1 Search Problems

a) We have two random variables $X$ and $A$, where $X$ corresponds to the instance of the problem and is distributed according to $P_X$, and $A$ is a random variable over deterministic algorithms. We denote the output of $A$ on input $x$ by $A(x)$ (which is a random variable over $W$). Then, the success probability of $A$ is given by

$$
\Pr[Q(X, A(X)) = 1].
$$

b) Since the success probability of an algorithm $A$ is defined as the average success probability of $A$ over all instances $x \in X$, weighted according to $P_X$, $A$ may perform much below its average success probability on some of the instances. Consider a computational problem with two instances $x_0$ and $x_1$ such that $A$ always finds a witness given $x_0$ but never finds one given $x_1$. If we have $P_X(x_0) = \alpha$ and $P_X(x_1) = 1 - \alpha$, the success probability of $A$ is $\alpha$. In this case, the success probability of $A'$ is also $\alpha$. Obviously, the success probability of $A'$ is at least as high as the one of $A$. Hence, the best lower bound on the success probability of $A'$ is $\alpha$.

c) Let $G = \langle g \rangle$, $|G| = q$ be the group for which $A$ can solve the discrete logarithm problem with probability $\alpha$. Algorithm $A'$ works as follows: Let $c > 1$ be some constant. On input $h = g^x \in G$, the algorithm $A'$ chooses $r \in \mathbb{Z}_q$ uniformly at random and invokes $A$ on $h \cdot g^r = g^{x+r}$. Given the output $y$ of $A$, it computes $y' := y - r \mod q$. If $g^{y'} = h$, $A'$ outputs $y'$. Otherwise, it repeats the procedure with a freshly chosen $r \in \mathbb{Z}_q$ if the number of repetitions so far (including the first iteration) is less than $c$. If the number of repetitions equals $c$, $A'$ outputs $y'$.

Note that if solver $A$ succeeds on $h \cdot g^r$, then $A'$ outputs a correct solution $y'$ with $g^{y'} = h$. Since $h \cdot g^r$ is a uniform random element of $G$, this happens with probability $\alpha$. Hence, the success probability of $A'$ is

$$
1 - (1 - \alpha)^c > \alpha
$$

for $c > 1$.

d) The crucial property of algorithm $A'$ in subtask c) is that it invokes $A$ each time on a uniformly random instance. In general, a problem instance cannot be transformed to a random instance such that a solution to the random instance can be transformed to a solution to the original instance. Problems that allow this are called random self-reducible.

7.2 Reductions Related to Discrete Logarithms

Let $G' := \langle G \setminus \{1\}; * \rangle$ with $g^a * g^b := g^{ab}$. Note that $|G'| = 2^k$ and $G' \cong \mathbb{Z}_q^*$ via the group isomorphism $\mathbb{Z}_q^* \to G', x \mapsto g^x$. Let $r \in \mathbb{Z}_q^*$ be the generator of $\mathbb{Z}_q^*$ that is assumed to be known.\(^1\) Then, $g^r$ generates $G'$ because isomorphisms map generators to generators.

\(^1\)One can in fact efficiently find such generator but this beyond the scope of this exercise.
We now describe the algorithm that computes the discrete logarithm of a given element \( h \in \mathbb{G} \). If \( h = 1 \), the algorithm outputs 0. Otherwise, it computes the discrete logarithm of \( h \) in \( \mathbb{G}' \) to the base \( g' \), i.e., an element \( z \in \mathbb{Z}_q^* \) such that

\[
h = g'^r \ldots g'^r = g'^(xz).
\]  

(1)

Since \( |\mathbb{G}'| = 2^k \) and the group operation \( \ast \) in \( \mathbb{G}' \) can be computed using the computational Diffie-Hellman oracle, the value \( z \) can be found efficiently using the algorithm from Exercise 3.3 d). Finally, our algorithm computes \( x := r^z \in \mathbb{Z}_q^* \) and outputs \( x \). Equation (1) implies that \( x \) is the discrete logarithm of \( h \) to base \( g \) and hence the algorithm is correct.

7.3 Properties of the Statistical Distance

a) Using the independence of \( A \) and \( X \) and the one of \( A \) and \( X' \), and the triangle inequality for the absolute value, we obtain

\[
\delta(A(X), A(Y)) = \frac{1}{2} \sum_{y \in \mathcal{Y}} \left| \Pr^A[X(A) = y] - \Pr^A[X'(A') = y] \right|
\]

\[
= \frac{1}{2} \sum_{y \in \mathcal{Y}} \left| \sum_{x \in \mathcal{X}} \Pr^A[X(x) = y \land X = x] - \sum_{x \in \mathcal{X}} \Pr^A[X(x) = y \land X' = x] \right|
\]

\[
= \frac{1}{2} \sum_{y \in \mathcal{Y}} \left| \sum_{x \in \mathcal{X}} \Pr^A[X(x) = y] \cdot P_X(x) - \sum_{x \in \mathcal{X}} \Pr^A[X(x) = y] \cdot P_{X'}(x) \right|
\]

\[
\leq \frac{1}{2} \sum_{y \in \mathcal{Y}} \sum_{x \in \mathcal{X}} \Pr^A[X(x) = y] \cdot \left| P_X(x) - P_{X'}(x) \right|
\]

\[
= \frac{1}{2} \sum_{x \in \mathcal{X}} \left( \left| P_X(x) - P_{X'}(x) \right| \cdot \sum_{y \in \mathcal{Y}} \Pr^A[X(x) = y] \right)
\]

\[
= \delta(X, X').
\]

b) The claim follows from the following calculation using the definition of the statistical distance and basic properties of the uniform distribution over a finite set:

\[
\delta(X, Y) = \frac{1}{2} \sum_{x \in \mathcal{I}} \left| P_X(x) - P_Y(x) \right|
\]

\[
= \frac{1}{2} \sum_{x \in \mathcal{J}} \left| \frac{1}{|\mathcal{J}|} - \frac{1}{|\mathcal{J}|} \right| + \frac{1}{2} \sum_{x \in \mathcal{I} \setminus \mathcal{J}} \left| \frac{1}{|\mathcal{I}|} - 0 \right|
\]

\[
= \frac{1}{2} \sum_{x \in \mathcal{J}} \left( \frac{1}{|\mathcal{J}|} - \frac{1}{|\mathcal{I}|} \right) + \frac{1}{2} \sum_{x \in \mathcal{I} \setminus \mathcal{J}} \frac{1}{|\mathcal{I}|}
\]

\[
= \frac{1}{2} \left( \frac{|\mathcal{J}|}{|\mathcal{I}|} - \frac{|\mathcal{J}|}{|\mathcal{I}|} + \frac{|\mathcal{I}| - |\mathcal{J}|}{|\mathcal{I}|} \right)
\]

\[
= 1 - \frac{|\mathcal{J}|}{|\mathcal{I}|}.
\]