7.1 The Merkle-Damgård Construction

a) An easy collision is given by \( x = 0 \) and \( y = (0, 0) \). To see this note that \( \hat{x} = \hat{y} = (0, \ldots, 0) \in \{0,1\}^m \) and thus \( h(x) = f(0, \ldots, 0) = h(y) \).

b) The winner of the collision-finding game for \( h \) outputs two messages \( x \neq y \) such that \( h(x) = h(y) \). From this collision of \( h \) we need to compute a collision of \( f \). Let \( d_x \) and \( d_y \) be the numbers of 0’s that have to be appended to \( x \) and \( y \), respectively, in order that we get strings that are multiples of \( m \) bits long. So, \( d_x = -|x| \mod m \) and \( d_y = -|y| \mod m \). This allows us to write

\[
\hat{x} = x \parallel (0, \ldots, 0) \parallel \langle d_x \rangle \quad \text{and} \quad \hat{y} = y \parallel (0, \ldots, 0) \parallel \langle d_y \rangle.
\]

Moreover, let \( h^x_k, 1 \leq k \leq s = \frac{|x|+d_x}{m} + 1 \), and \( h^y_k, 1 \leq k \leq t = \frac{|y|+d_y}{m} + 1 \), be the outputs of \( f \) in the iterative evaluation of \( h(x) \) and \( h(y) \). We can assume without loss of generality that \( t \geq s \). Note that, by definition,

\[
h^x_s = h(x) = h(y) = h^y_t.
\]

If there exists a \( k \in \{1, \ldots, s-1\} \) with \( h^x_{s-k} \neq h^y_{t-k} \) and \( k \) is the smallest such number, then

\[
f(h^x_{s-k} \parallel 1 \parallel \langle d_x \rangle) = h^x_{s-(k-1)} = h^y_{t-(k-1)} = f(h^y_{t-k} \parallel 1 \parallel \langle d_y \rangle),
\]

which gives a collision of \( f \). Therefore we can assume in the remainder of the proof that \( h^x_{s-k} = h^y_{t-k} \) for all \( 0 \leq k \leq s-1 \). We proceed by considering three cases. First suppose that \( |x| \neq |y| \mod m \) \( \Leftrightarrow d_x \neq d_y \). Then the last compression stages in the evaluations of \( h(x) \) and \( h(y) \) already give a collision of \( f \). Concretely,

\[
f(h^x_{s-1} \parallel 1 \parallel \langle d_x \rangle) = h^x_1 = h(x) = h(y) = h^y_t = f(h^y_{t-1} \parallel 1 \parallel \langle d_y \rangle)
\]

with \( x' \neq y' \) as \( d_x \neq d_y \). Next we turn to the case where \( |x| \equiv |y| \mod m \) but \( |x| \neq |y| \). Here it follows that \( t > s \) and, with \( k = s-1 \),

\[
f((0, \ldots, 0) \parallel \hat{x}_1) = h^x_1 = h^x_{s-k} = h^y_{t-k} = h^y_{t-(s-1)} = f(h^y_{t-s} \parallel 1 \parallel \hat{y}_{t-(s-1)}),
\]

which again gives a collision of \( f \). Finally, suppose \( |x| = |y| \). In this case there is a \( 1 \leq k \leq t = s \) such that \( \hat{x}_k \neq \hat{y}_k \). From this we get the collision

\[
f((0, \ldots, 0) \parallel \hat{x}_1) = h^x_1 = h^y_1 = f((0, \ldots, 0) \parallel \hat{y}_1)
\]

if \( k = 1 \) or else the collision

\[
f(h^x_{k-1} \parallel 1 \parallel \hat{x}_k) = h^x_k = h^y_k = f(h^y_{k-1} \parallel 1 \parallel \hat{y}_k).
\]
7.2 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.
7.3 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

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

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

\[
\text{indep. } \leq \frac{1}{2} \sum_{y \in Y} \sum_{x \in \mathcal{X}} \Pr^{A}[A(x) = y] \cdot \Pr_X(x) - \sum_{x \in \mathcal{X}} \Pr^{A}[A(x) = y] \cdot \Pr_{X'}(x)
\]

\[
\leq \frac{1}{2} \sum_{y \in Y} \sum_{x \in \mathcal{X}} \Pr^{A}[A(x) = y] \cdot \Pr_X(x) - \Pr_{X'}(x)
\]

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

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

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:

\[
\delta(X, Y) = \frac{1}{2} \sum_{x \in I} |\Pr_X(x) - \Pr_Y(x)|
\]

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

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

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

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

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