Question 4.9

Suppose h_2 is *not* collision resistant then we have $x, x' \in \{0,1\}^{4m}$ such that $x \neq x'$ and $h_2(x) = h_2(x')$.

We write $x = x_1||x_2$ and $x' = x'_1||x'_2$, where $x_1, x_2, x'_1, x'_2 \in \{0,1\}^{2m}$ yielding:

$$h_1(h_1(x_1)||h_1(x_2)) = h_1(h_1(x'_1)||h_1(x'_2))$$

First suppose $A = h_1(x_1)||h_1(x_2) \neq h_1(x'_1)||h_1(x'_2) = B$ then we have $h_1(A) \neq h_1(B)$ where $A \neq B$ which implies that h_1 is *not* collision resistant. A contradiction.

Now suppose $h_1(x_1)||h_1(x_2) = h_1(x'_1)||h_1(x'_2)$ which means $h_1(x_1) = h_1(x'_1)$ where $x_1 \neq x'_1$ implying that h_1 is *not* collision resistant. A contraction.

Collectively this implies that there is no such $x, x' \in \{0,1\}^{4m}$ where $x \neq x'$ and $h_2(x) = h_2(x')$, which means that h_2 is collision resistant as required.$\square$