# Exercise 11.2

## Task

Simplified Merkle-Damgård construction

## Solution

We are given two input strings $x$ and $x'$.

Let's start with what happens on the last step:

The final step of hashing $x$ is $h(x) = f(z_{n+1})$, while the final step of hashing $x'$ is $h(x') = f(y_{m+1})$. And we assume that we have a collision, i.e. $h(x) = h(x')$. Then:

Case 1: $z_{n+1} \neq y_{m+1}$ → We're done - given a collision of $h$ we can find a collision of $f$ - Giving $z_{n+1}$ and $y_{m+1}$ to $f$ produces a collision.

Case 2: $z_{n+1} = y_{m+1}$. Then we go 1 step back in the hashing algorithm - the previous step for $x$ has value $f(z_n)||x_i$, and for $x'$ it's $f(y_m)||x'_j$. We are in pretty much the same case as what we had when we first looked at these Case 1/2. So we repeat the same process again until we fall into Case 1.

If we go all the way to the start of the hashing chain for $x$ (let's assume $x$ has got a shorter chain than $x'$, it works the same way if we exchange the places of $x$ and $x'$). The first step of the $x$ chain is $z_1 = 0^k||x_i$. But that would mean that at some point in the $x'$ chain we had $f(y_k)$, which produced $0^k$ - Contradiction, with the fact that $f$ is zero-preimage resistant.

Then the only option that's left is that we haven't found two values of $f$, which cause a collision, but $h$ has a collision. This is again a contradiction with the assumption in the problem.

With this we show that if $f$ is collision resistant and zero-preimage resistant, then $h$ is collision resistant.