Sample Problem

Problem: Let H be a compressing, collision resistant hash function. Construct another function that is compressing, pre-image resistant but not collision resistant.

Solution: Let $H : \{0,1\}^* \rightarrow \{0,1\}^n$ be a compressing collision resistant hash function. We define another function $H' : \{0,1\}^* \rightarrow \{0,1\}^n$ as follows:

$$H'(x) = \begin{cases} 0^n, & \text{if } x \in 1^*. \\ H(x), & \text{otherwise.} \end{cases}$$

Clearly, H' is not collision-resistant. From the definition of H', $H'(1) = H'(11) = 0^n$. Hence, it is trivial to find a collision in H.
It is also easy to see that if H is a compressing function, H' is also a compressing function.
All we need to prove now is that H' is pre-image resistant.

Claim 1. *H' is pre-image resistant, if H is pre-image resistant.*

Proof. Let us assume for the sake of contradiction that H' is not pre-image resistant. Then there exists an adversary $\mathcal{A}$ who when given a random $x \in \{0,1\}^k$, can find another $x' \in \{0,1\}^k$, where $x \neq x'$ such that $H'(x) = H'(x')$ with a non-negligible probability. We will now construct another adversary $\mathcal{B}$ who can break the pre-image resistance of H. This adversary $\mathcal{B}$ internally runs $\mathcal{A}$. Given a random $x \in \{0,1\}^k$, $\mathcal{B}$ does the following:

- If $x \in 1^k$, it returns $\perp$. (This only happens with a negligible probability.)
- If $x \notin 1^*$, it forwards x to $\mathcal{A}$. With a non-negligible probability, $\mathcal{A}$ responds with $x' \in \{0,1\}^k$, such that $H'(x) = H'(x')$. $\mathcal{B}$ returns x'.

Since $\mathcal{A}$ finds a correct x' with non-negligible probability, $\mathcal{B}$ can break the pre-image resistance of H with non-negligible probability. But since H is collision resistant, it is also pre-image resistant and such an adversary cannot exist. Hence our assumption was wrong and H' is pre-image resistant. □