Theorem: If \( h \) is CR, then \( h \) is TCR.

**proof sketch:**
Assume \( h \) is not TCR, then given an \( x \), the adversary can find an \( x' \neq x \) such that \( h(x) = h(x') \).
But, then \( x, x' \) form a collision, which is a contradiction since the hypothesis says that \( h \) is CR.

**Remark:** If \( h \) is TCR, then \( h \) is not necessarily CR.

**Example:** \( h: \{0,1\}^n \rightarrow \{0,1\}^m \), if \( x = 0^n \)
\( h: \{0,1\}^n \rightarrow \{0,1\}^m \), if \( x = 1^n \)

Then \( h \) is TCR since given a uniformly random \( x \in \{0,1\}^n \), the probability that we can find an \( x' \) such that \( h(x) = h(x') \) and \( x = x' \) is \( \frac{2^n}{2^m} \) (for \( x = 0^n \) and \( x = 1^n \)).
But, \( h(0^n) = h(1^n) \), so \( h \) is not CR.

**Theorem:** \( h \) is OW \( 

**proof sketch:**
If \( h(x) = x \), then \( h \) is CR, but \( h \) is not OW.
If \( h(x) = \begin{cases} \text{any } f \in \mathcal{F} & \text{if } x = 0^n \\ \text{any } f \in \mathcal{F} & \text{if } x = 1^n \\ f(x) \text{, otherwise} \end{cases} \)

Then \( h \) is OW, but \( h(0^n) = h(1^n) = 0^n \), so \( h \) is not CR.

Why \( h \) is OW?

If \( h \) was not OW, then it would be "feasible" given \( y \in \{0,1\}^m \) such that \( y = h(x) \) and \( x \in \{0,1\}^n \)
to find \( x' \) such that \( h(x) = h(x') \).

But, then \( f \) is not OW, since in most of the inputs we have that \( h(x) = f(x) \).
Exercise 8. Assume \( h: \{0,1\}^{n+1} \to \{0,1\}^n \) and there are exactly two \( x_1, x_2 \) such that \( h(x_1) = h(x_2) \).

If \( h \) is CR, then \( h \) is OW.

**Proof Sketch:**

Assume \( h \) is not OW, then given \( y \) such that \( y = h(x) \) and \( x \neq \{0,1\}^{n+1} \), it is "feasible" to find an \( x' \) such that \( h(x') = h(x) \).

If we prove that with non-negligible probability \( x \neq x' \), then it is "feasible" to find collisions, which is a contradiction (since we assume that \( h \) is CR).

So, \( h \) has to be OW.

What is the probability that \( x \neq x' \)?

From the hypothesis we know that there are exactly two \( x_1, x_2 \) such that \( h(x_1) = h(x_2) = y \). Since, \( x \subseteq \{0,1\}^{n+1} \),

\[
Pr(x = x_1) = Pr(x = x_2) = \frac{1}{2}
\]

So, \( Pr(x \neq x') = Pr(x \neq x'|x = x_1) \cdot Pr(x = x_1) + Pr(x \neq x'|x = x_2) \cdot Pr(x = x_2)
\]

\[
= Pr(x \neq x_1) \cdot \frac{1}{2} + Pr(x \neq x_2) \cdot \frac{1}{2}
\]

\[
= \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}
\]

(since \( x' \) is either \( x_1 \) or \( x_2 \).

**Exercise 8.** Let \( t \) be the number of leaves of a Merkle tree \( M \).

Can we find another Merkle tree with \( t/2 \) leaves that has the same root as \( M \)?

(ex. 5.13. Katzen Lintell)

Yes, let \( (x_1, ..., x_t) \) be the leaves of \( M \), then

if \( h(x_{(i+1)}x_{(i+2)}) \), \( i = 1, ..., t-1 \) are the \( t/2 \) leaves of \( M' \) then \( M \) and \( M' \) have the same root.

Theorem 3.1. Let \( h \) be CR, then \( MTh \) is CR, where \( MTh \) is the root of the Merkle tree that uses \( h \), for a fixed \( t \).

**Proof Sketch:**

If \( MTh \) was not collision resistant, then \( (x_1, ..., x_t) \) such that \( (x_1, ..., x_t) \neq (x_1', ..., x_t') \) such that \( MTh(x_1, ..., x_t) = MTh(x_1', ..., x_t') \).

(ex. 5.13. Katzen Lintell)
So, there would be a level $i$ such that the nodes of level $i$ of the two trees will be equal, but the nodes of level $i+1$ will not be equal. Then this will give a collision for $h$, which is a contradiction.

**Exercise:** Assume $h$ is OW, CR, TCR, PR, non-malleable, ....

Let $H$ be the hash function that we get from the Merkle-Damgard construction using $h$. Is $H$ non-malleable?

No, $H$ is malleable, because given $H(m)$, we can find (without knowing $m$) $H(\text{pad}(m)||c)$, where pad($m$) is the padded message $m$ and $c$ is a string of our choice.

These attacks are known as "extension attacks".

**Exercise:** Let $h$ be a OW function, is $h(h(x)) = h(h(x))$ OW?

No. Let $f(x) = h(y) || 0^n$ where $|x| = |y| = n$.

Then, $f$ is a length-preserving OW function, since if we could "invert", we could "invert" $h$ as well. But, $f(f(x,y)) = f(h(y)||0^n) = h(0^n) || 0^n$, which is not OW.

Why is proving the contrapositive not possible?

Assume $h'$ is not OW, then from $h(h(x))$ we can get $x'$ such that $h(h(x)) = h(h(x'))$.

But to prove that $h$ is not OW, we need to be able to recover an $x'$ from $h(x)$ such that $h(x) = h(x')$.

If given $y = h(x)$, we apply $h$ and "invert" $h(y) = h(h(x))$ then we will get an $x'$ such that $h(h(x)) = h(h(x')) = h(y)$.

But, can we argue that $h(x) = y$? No.