Merkle-Damgard transform to obtain a provable secure collision resistant hash function:

The Merkle-Damgård transform is a way of extending a fixed-length collision-resistant hash function into a general one that takes inputs of arbitrary length messages. This method works for any fixed-length collision-resistant hash function, even one that reduces the length of its input by just a single bit.

This transform reduces the problem of designing a collision-resistant hash function to the problem of designing a fixed-length collision-resistant function that compresses its input by any length(even a single bit).

Construction:

Let (Gen_h, h) be a fixed-length hash function with input length $2\ell(n)$ and output length $\ell(n)$. Construct a variable-length hash function (Gen, H) as follows:

- $\mathsf{Gen}(1^n)$: upon input 1^n, run the key-generation algorithm Gen_h of the fixed-length hash function and output the key. That is, output $s \leftarrow \mathsf{Gen}_h$.
- $H^s(x)$: Upon input key s and message $x \in \{0,1\}^*$ of length at most $2^{\ell(n)} - 1$, compute as follows:
  1. Let $L = |x|$ (the length of x) and let $B = \lceil \frac{L}{\ell} \rceil$ (i.e., the number of blocks in x). Pad x with zeroes so that its length is an exact multiple of ℓ.
  2. Define $z_0 := 0^\ell$ and then for every $i = 1, \ldots, B$, compute $z_i := h^s(z_{i-1} \| x_i)$, where h^s is the given fixed-length hash function.
  3. Output $z = H^s(z_B \| L)$

Theorem:

If (Gen_h, h) is a collision resistant hash function then (Gen, H) is also a collision-resistant hash function.

Proof:

We first show that for any s collision in H^s yields a collision in h^s.

Let x, y are two different strings of lengths L, L' such that a collision occurs $(H(x) = H(y))$. Let's divide the x into blocks $x_1, x_2, \ldots\ldots x_B$ and y into $y_1, y_2, \ldots\ldots y_{B'}$. There are two cases to consider

1. $L \neq L'$: In this case since the hash is same means $h^s(z_B \parallel L) = h^s(z_{B'} \parallel L')$,but $L \neq L'$, it means $h_B \parallel L \; and \; h_{B'} \parallel L'$ are two different strings that collide for h^s.
2. $L = L'$: In this case Let's assume z_i , $z_{i'}$ are two intermediate hash values of $x \; and \; y$. Since $x \neq y$ and both are having same length, there must be an index $i \; (1 \leq 1 \leq B)$ such that $x_i \neq y_i$. Let i^* be the highest index for which it holds $z_{i^*-1} \parallel x_{i^*} \neq z'_{i^*-1} \parallel y_{i^*}$. Here if $i^* = B$ (Means last block) then $z_{i^*-1} \parallel x_{i^*} \; and \; z'_{i^*-1} \parallel y_{i^*}$ gives collision because we know that $H^s(x) = H^s(y)$and $L = L'$ which means $z_B = z_{B'}$. If $i^* < B$ (Means not last block) implies $z_{i^*} = z'_{i^*}$, means $z_{i^*-1} \parallel x_{i^*} \; and \; z_{i^*-1} \parallel y_{i^*}$ gives collision.

In two cases, we got $z_{i^*-1} \parallel x_{i^*} \neq z_{i^*-1} \parallel y_{i^*}$ but $h^s(z_{i^*-1} \parallel x_{i^*}) = h^s(z_{i^*-1} \parallel y_{i^*})$ means **there is a collision in** h^s

But h^s is a collision resistant so function. So, there is no collision in H^s also. It means H^s is a collision resistant hash function.

Properties of secure hash function:

Generally, three levels of security are considered

1. Collision resistance : Given two messages $m_1 \; and \; m_2$, It should be hard to find a hash such that $H^s(m_1) = H^s(m_2)$, where s is the hash key.

2. Second preimage resistance: For given s and x it is hard for a probabilistic polynomial-time adversary to find x' such that $H^s(x) = H^s(x')$.
3. Preimage resistance: For given s and some y it is hard for probabilistic polynomial-time adversary to find a value x' such that $H^s(x') = y$.

We have already proved that the Merkle-damgard transform is a collision resistant hash function.

To prove second preimage resistant adversary needs to find x' such that $H^s(x) = H^s(x')$ but it is collision-resistant hash function. So, it is second preimage resistant. (Any collision resistant hash function is second preimage resistant).

Any hash function that is second preimage resistant is also preimage resistant. To prove preimage resistance adversary needs to find x' for given y such that $H^s(x') = y$ . . Suppose If Adversary can find x' then he can take x and can compute $H(x) = y$ and invert it again gives x', But the domain of hash function is infinite, it follows that $x' \neq x$ with good probability. So that inversion is not successful means it is preimage resistance.

So Merkle-damgard transform is a secure collision resistant hash function.