We can construct an arbitrary length hash function $H^s(x)$ from a fixed length hash function $h^s(x)$ with inputs of length 2n and output of length n. If (Gen, h) is a fixed length collision resistant hash function, then (Gen, H) is also a collision resistant hash function.

Let (Gen, h) be a fixed length collision resistant hash function for input of length 2l(n) and output of length l(n). We can set l(n) = l. On input a key s and a string x of any length L such that $L < 2^{l(n)}$, a variable length hash function (Gen, H) can be constructed as follows using Merkle-Demgard transform:

- Set the length L = length of the string x. Let there be B = ⌈L/l⌉ blocks. Pad x with zeros so that its length is a multiple of l. Parse the result as the sequence of l-bit blocks x1…xB. Set x_{B+1} = L where L is encoded using exactly l bits.
- Set $z_0 = 0^l$ as initialising vector
- For i=1 to B+1, compute $z_i = h^s(z_{i-1} || x_i)$
- Output z_{B+1}