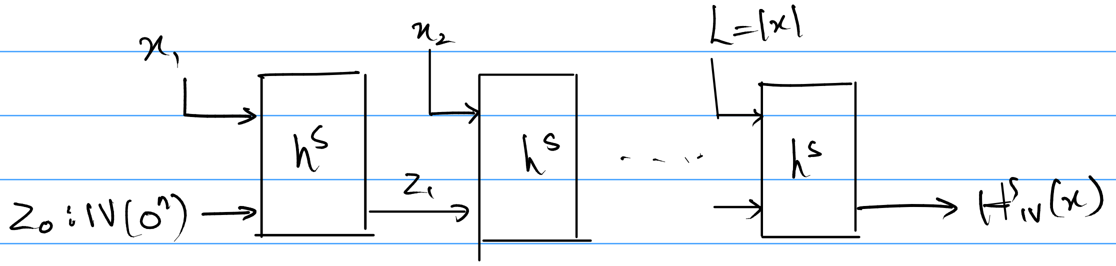
Merkle Damgard Transform

The Merkle Damgard Transform allows the conversion of a fixed length hashing func to a variable length hashing func.
The algorithm is as follows,

```
Gen($1^n$) : Return key $s \leftarrow Gen_h$
$H^s(x)$ : key s & message x.
        1. Pad x with zeros st. x is a exact multiple of block size.
        2. $z_0 = 0^l$ (IV)
            for i = 1 to B (Block size)
                $z_i = h^s(z_{i-1} \| x_i)$   $h^s$ is fixed length hash function.
        3. $z = H^s(z_B \| L)$
```

To visualize,



Since each fixed length hash function is valid, the Merkle-Damgard transform gives a valid variable length hash func.