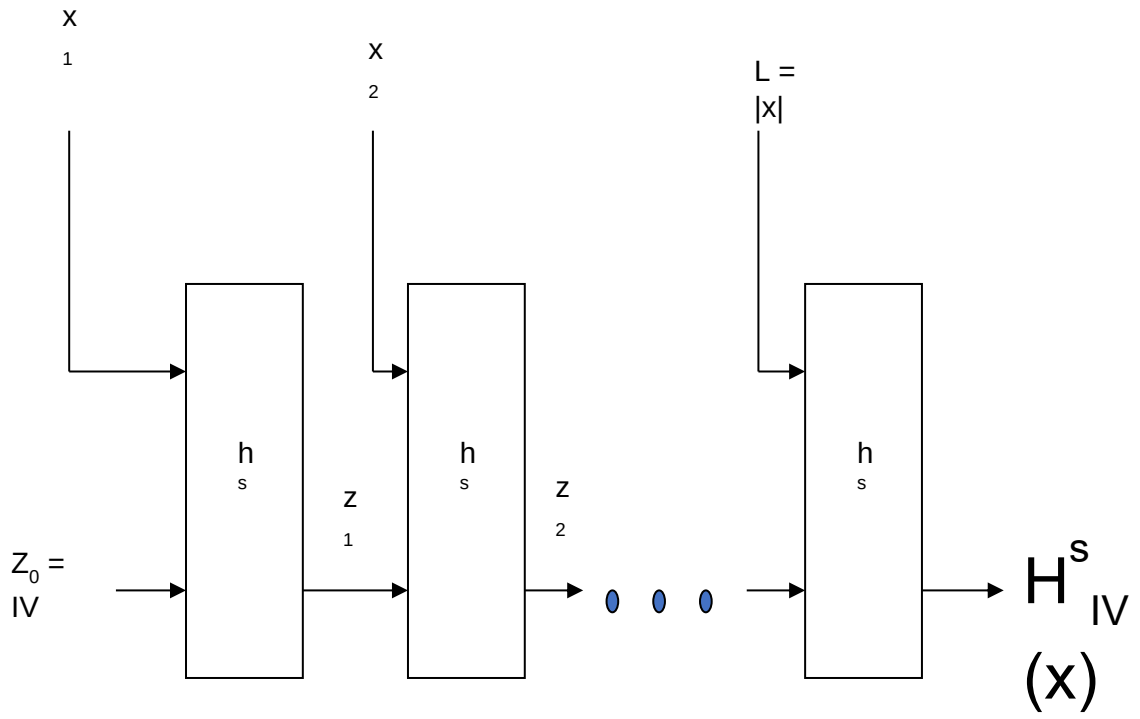
Merkle Damgard Transformation

MD Transformation is used to construct hash functions $H^s(x)$ from fixed length hash functions h^s having input length 2n and output length n.



The Merkle Damgard Transform takes the Message m in the blocks of size n and an initialization vector of size n. The length of the message is taken as the last block.

If h^s is fixed lengt collision resistant hash function, then $H^s_{IV}(x)$ is collision resistant hash function.