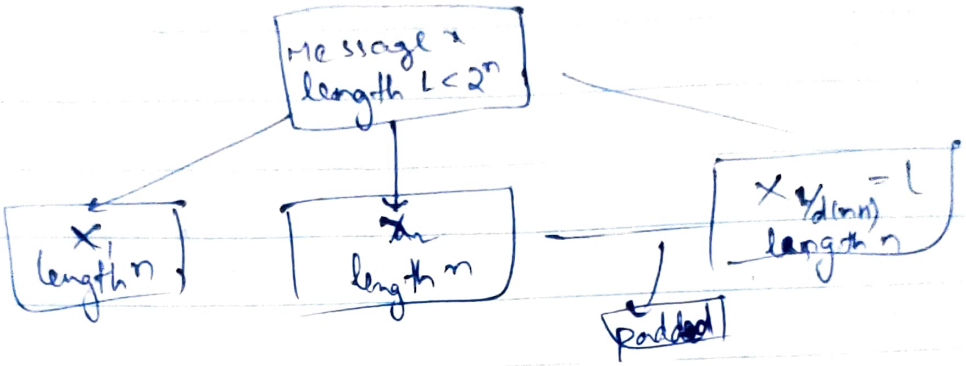
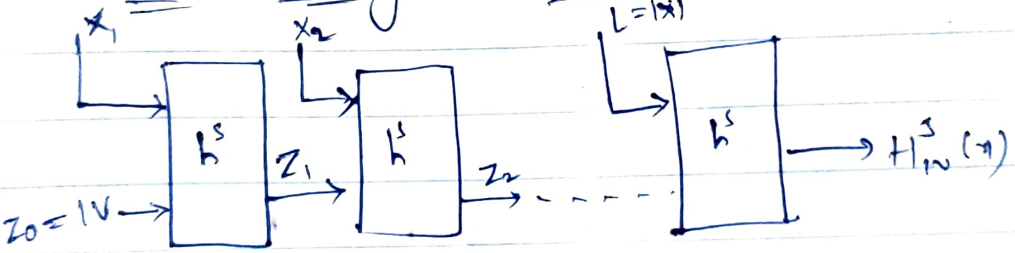
Merkle Damgard Transform :

→ Constructing hash-functions $H^s(x)$ from fixed length hash functions (h^s) with inputs of length 2n and output of length n.



Merkle Damgard Transform :



Theorem: If (Gen, h) is a fixed length collision resistant hash function, then (Gen, H) is a collision resistant hash function.

Construction: Let (Gen, h) be a fixed-length collision-resistant hash function for inputs of length 2l(n) and with output length l(n). Construct a variable length hash function (Gen, H) :-

- Gen : remains unchanged.
- H : on input key s and a string $x \in \{0,1\}^*$ of length $L < 2^{l(n)}$ do the following (set l = l(n)) :-

1) Set $B := \lceil \frac{L}{l} \rceil$ (i.e., the no. of blocks in x). Pad x with zeroes so its length is a multiple of l. Parse the padded result as the

sequence of ℓ-bit blocks $x_1, \ldots, x_B$. set $x_{B+1} := L$, where L is encoded as using exactly ℓ bits.

2. set $z_0 := 0^\ell$
3. for $i = 1, \ldots, B+1$, compute $z_i = h^s(z_{i-1} \| x_i)$
4. Output z_{B+1}

Proving this is secure:

1) Case 1: if $L \neq L'$. In this case, the last step of the computation of $H^s(x)$ is $z_{B+1} := h^s(z_B \| L)$ and the last step of the computation of $H^s(x')$ is $z'_{B+1} := h^s(z'_B \| L')$. Since $H^s(x) = H^s(x')$ it follows that $h^s(z_B \| L) = h^s(z'_B \| L')$. However $L \neq L'$ and $z_B \| L$, $z'_B \| L'$ are 2 different strings that collide for h^s.

2) Case 2: $L = L'$. Note this means that $B = B'$ and $x_{B+1} = x'_{B+1}$. Let z_i, z'_i be the intermediate hash values of x and x' during the computation of $H^s(x)$, $H^s(x')$ resp. Since $x \neq x'$ but $|x| = |x'|$ there must exist at least one index i (with $1 \leq i \leq B$) such that $x_i \neq x'_i$. Let $i^* \leq B+1$ be the highest index for which it holds that $z_{i^*-1} \| x_{i^*} \neq z'_{i^*-1} \| x'_{i^*}$. If $i^* = B+1$ then $z_B \| x_{B+1}$ and $z'_B \| x'_{B+1}$ are 2 different strings that collide for h^s because

$$h^s(z_B \| x_{B+1}) = z_{B+1} = H^s(x) = H^s(x') = z'_{B+1} = h^s(z'_B \| x'_{B+1})$$

If $i^* \leq B$, then maximality of i^* implies $z_{i^*} = z'_{i^*}$. Thus, once again $z_{i^*-1} \| x_{i^*}$, $z'_{i^*-1} \| x'_{i^*}$ are 2 different strings that collide for h^s.