Signature Schemes Designs: RSA Full Domain Hash

- **Public Functions** A hash function $H : \{0,1\}^* \to \mathbb{Z}_N^*$
- **Keygen:** Run RSA.Keygen. $pk = (e, N)$, $sk = (d, N)$.
- **Sign**: Input: sk, M. Output $\sigma = \text{RSA.Dec}(sk, H(M)) = H(M)^d \mod N$
- **Verify**: Input: pk, M, σ. If $\text{RSA.Enc}(pk, \sigma) = H(M)$ output accept, else reject
- If $\sigma^e \mod N = H(M)$, output accept, else reject.

Correctness

Suppose $\sigma = \textbf{Sign}(sk, M)$. This implies $\sigma = H(M)^d \mod N$. This implies

$$\sigma^e \mod N = (H(M)^d \mod N)^e \mod N = H(M)^{ed} \mod N$$

. As $ed \equiv 1 \mod \phi(N)$ and H maps to $\mathbb{Z}_N^*$, we have

$$\sigma^e \mod N = H(M) \mod N = H(M)$$

which is the acceptance condition in the verification algorithm.