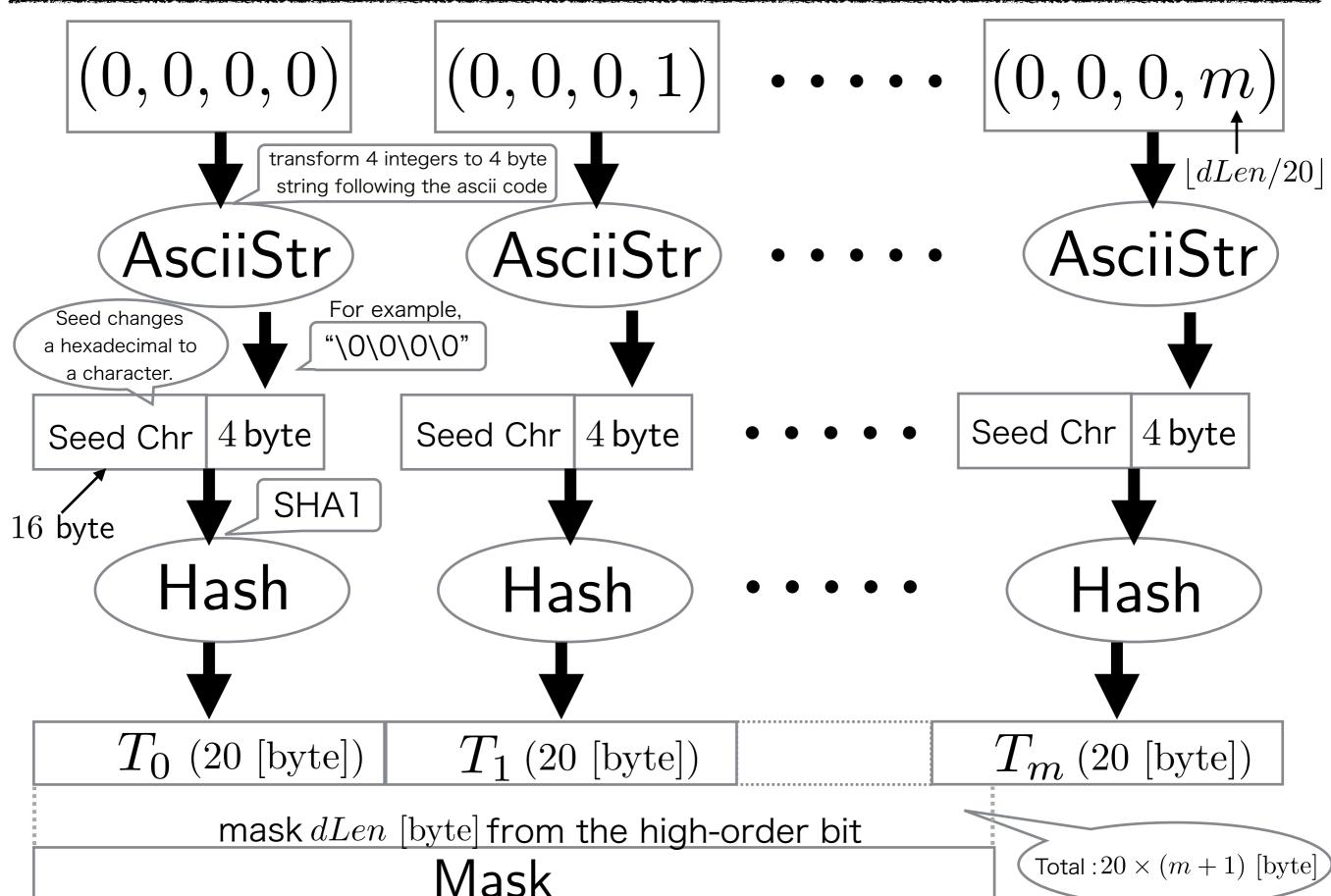
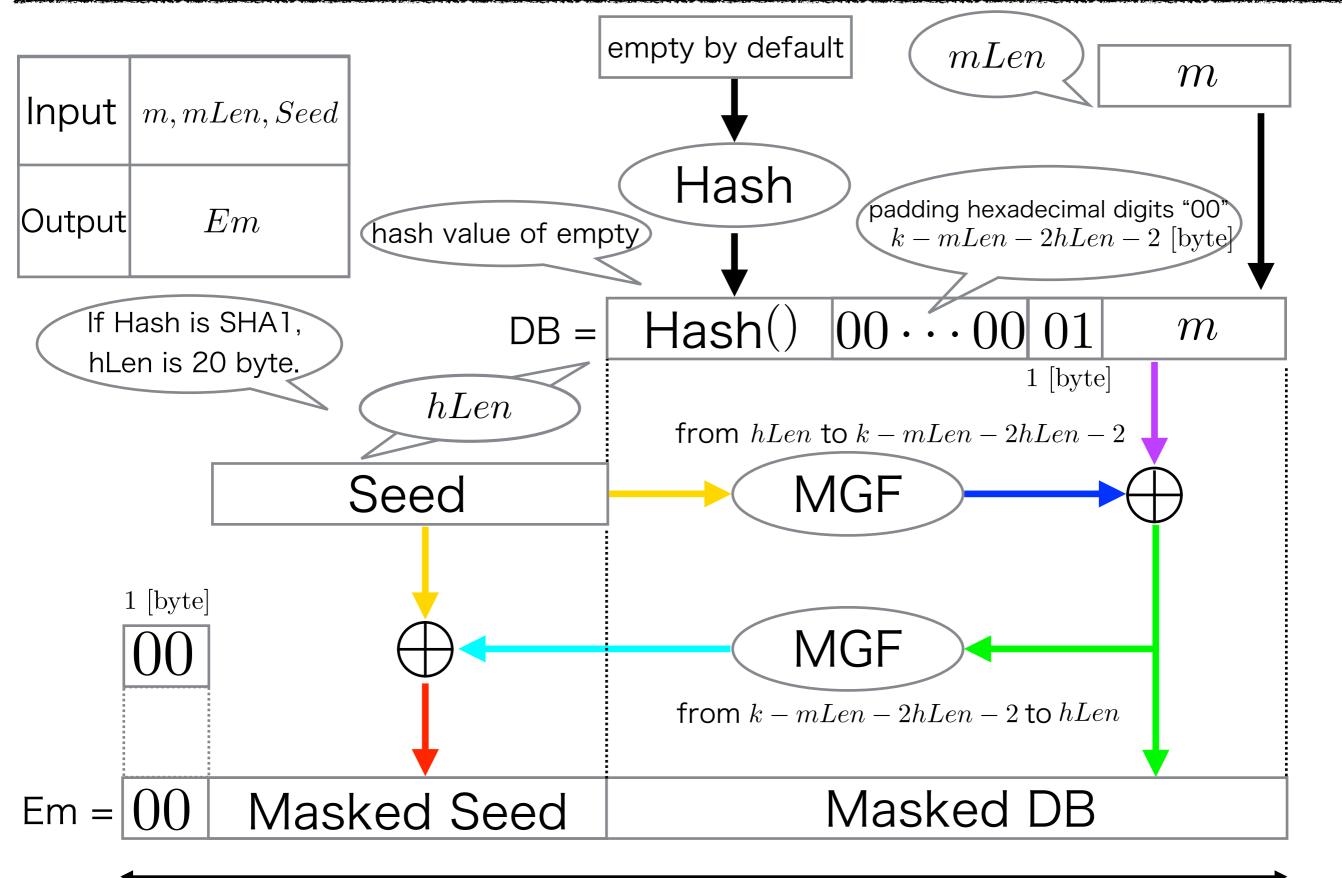
MGF(Masked Generation Function) (Input : Seed, dLen → Output : Mask)





Padding of RSA-OAEP Encoding

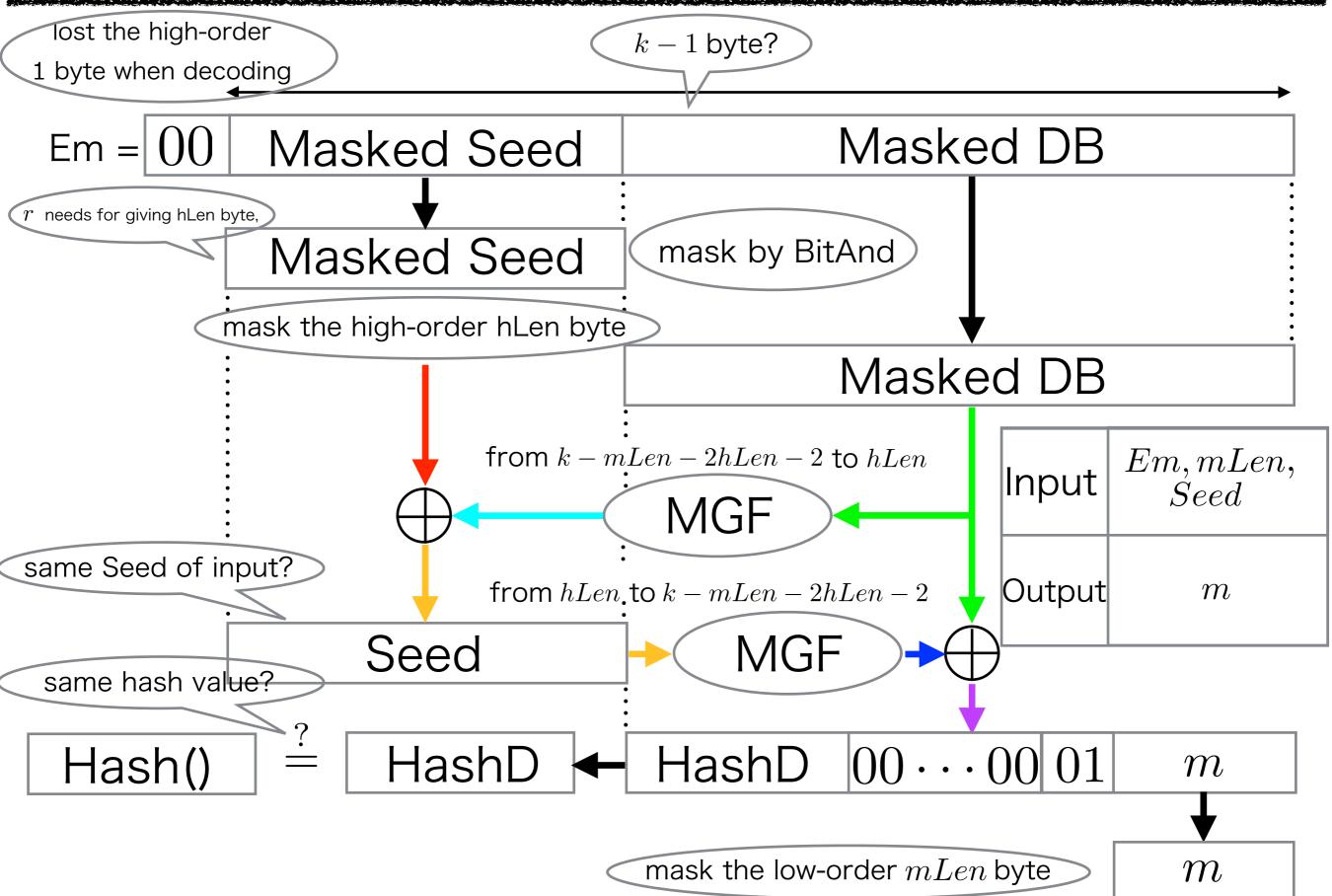




$$k = \lceil \text{bitlen}(pq)/8 \rceil \lceil \text{byte} \rceil$$

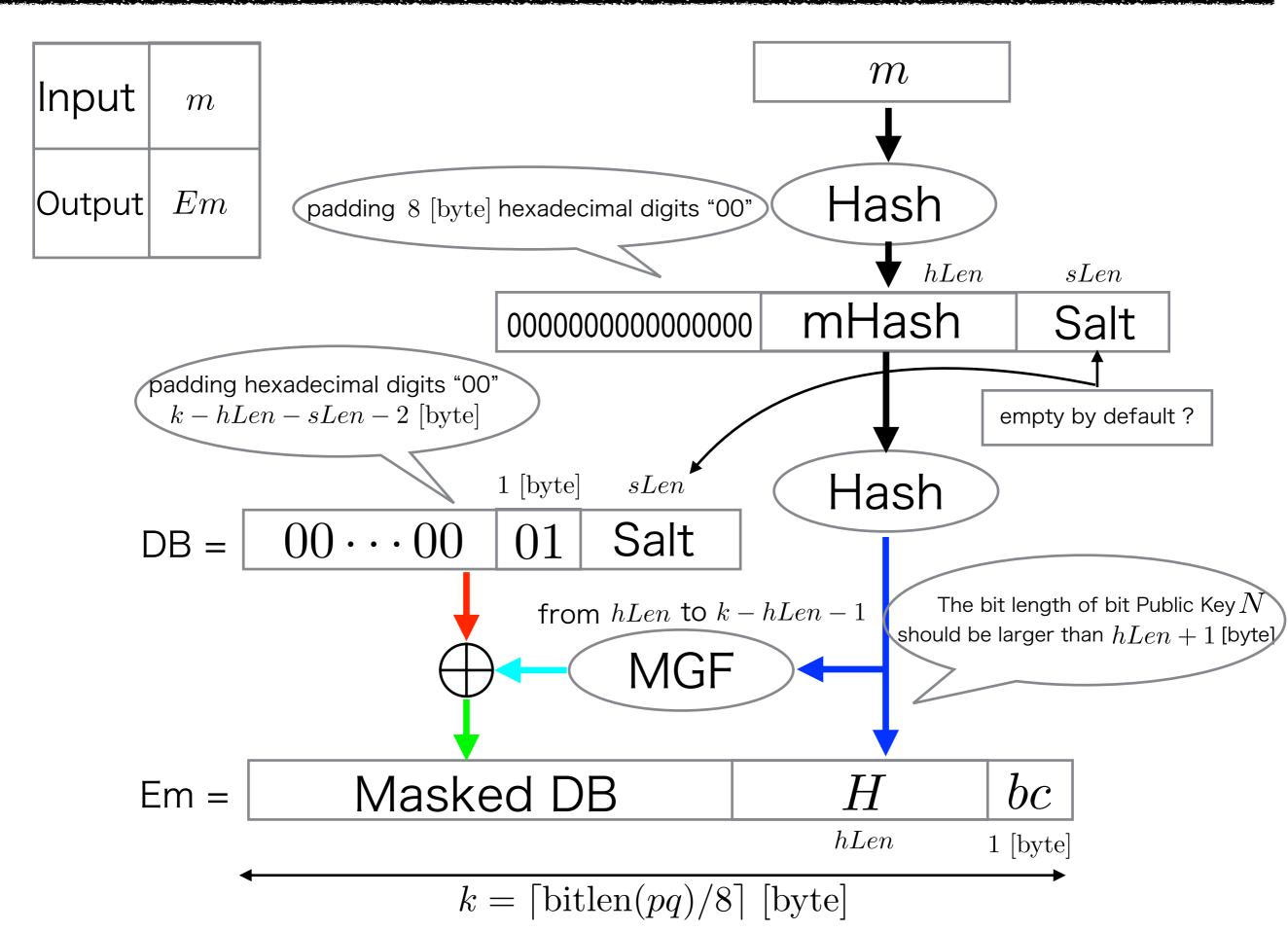
Reverse Padding of RSA-OAEP Decoding





Padding of RSA-PSS Signature Generation





Reverse Padding of RSA-PSS Signature Verification



