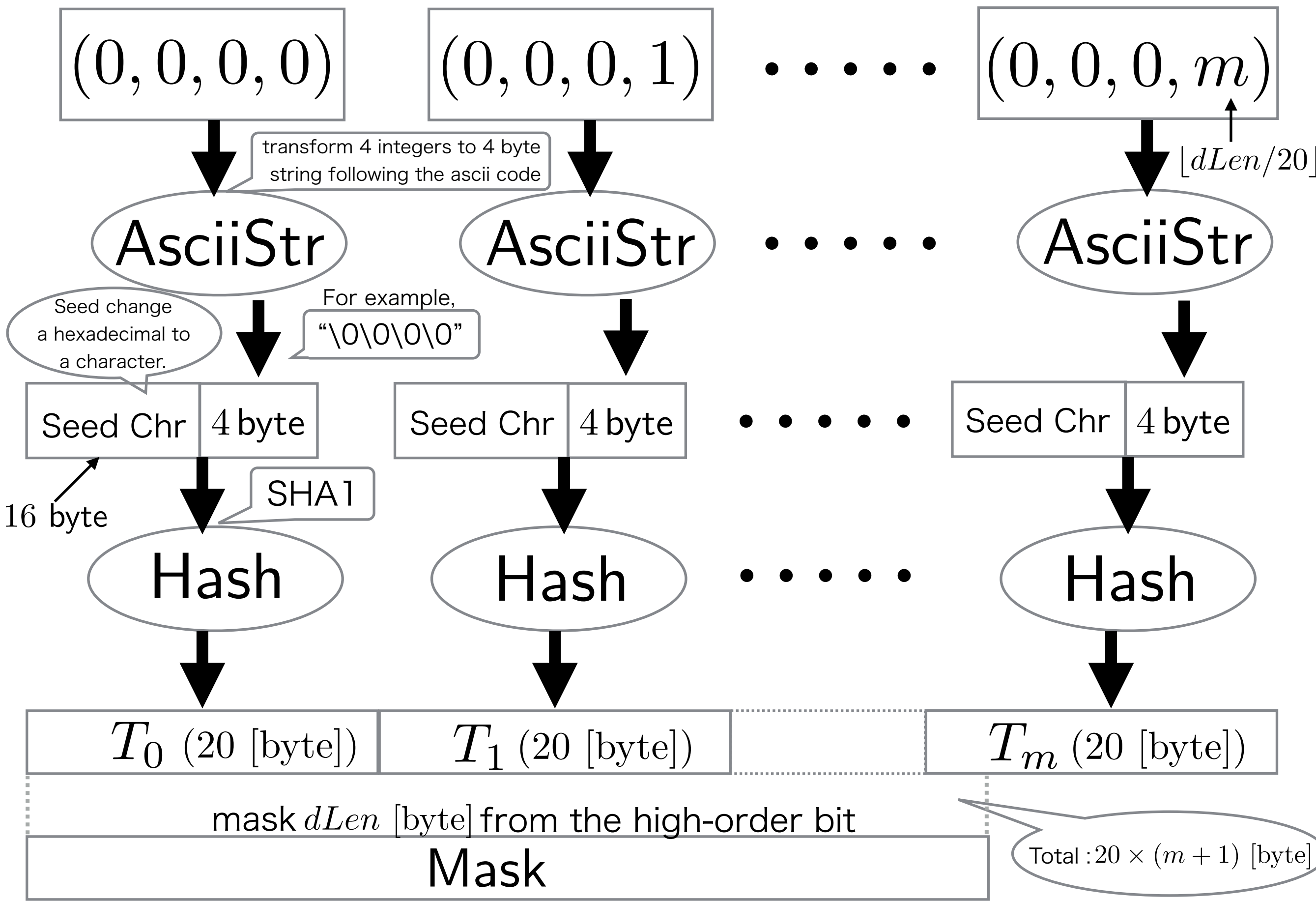
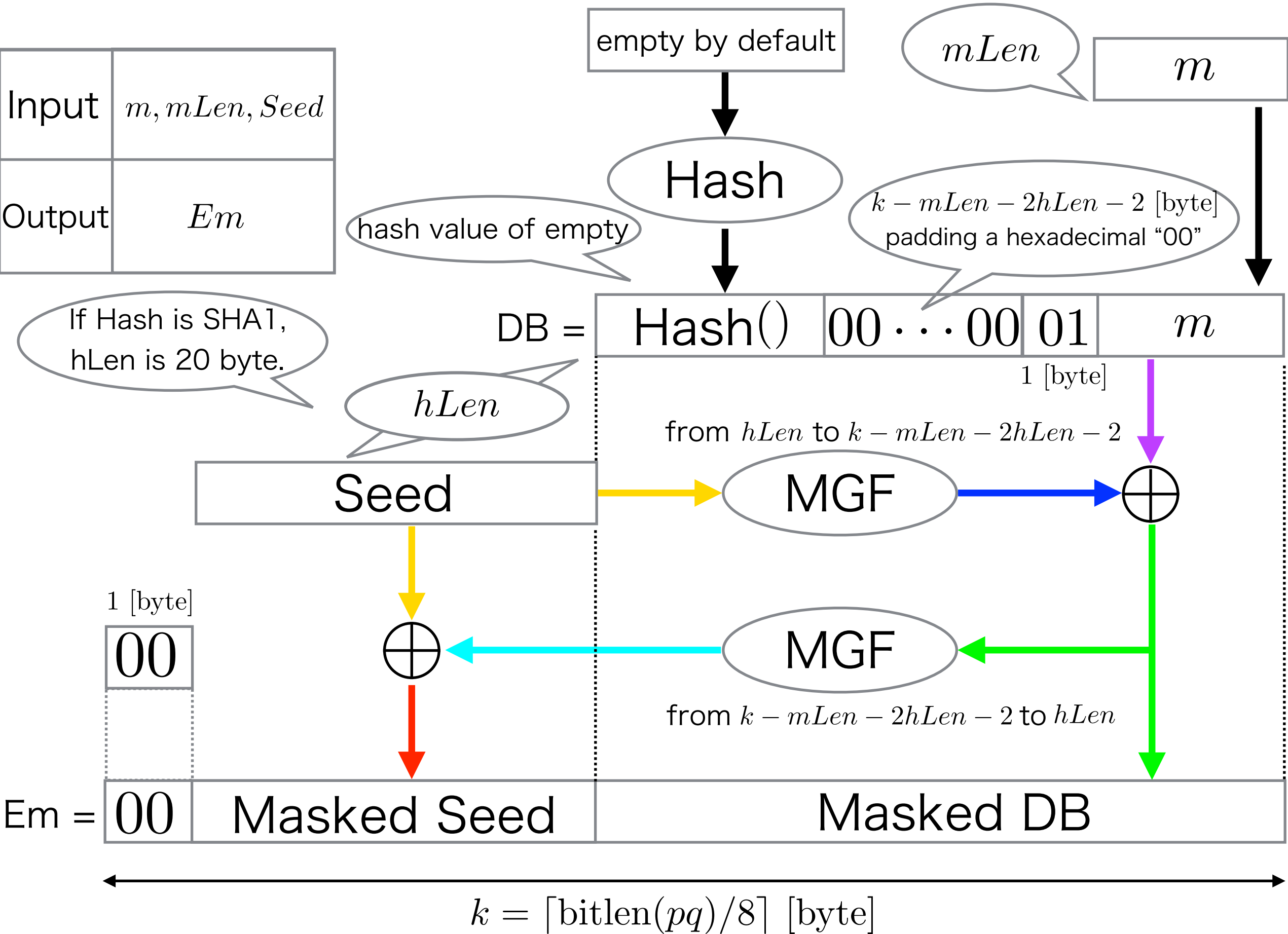


MGF(Masked Generation Function) (Input : Seed, dLen → Output : Mask)



Padding of RSA-OAEP Encode

Input	$m, mLen, Seed$
Output	Em



Reverse Padding of RSA-OAEP Decode

