

# Mask Generation Function (a pseudorandom function)

8 bytes 00 00 00 00 00 00 00 00

00 00 ... 00 01

$M, E(PR_a, EM)$

MSB 비트가 1이면  
강제로 0으로 설정한다

~~$M, E(PR_a, H(M))$~~

pseudorandom  
number

hexadecimal  
value BC

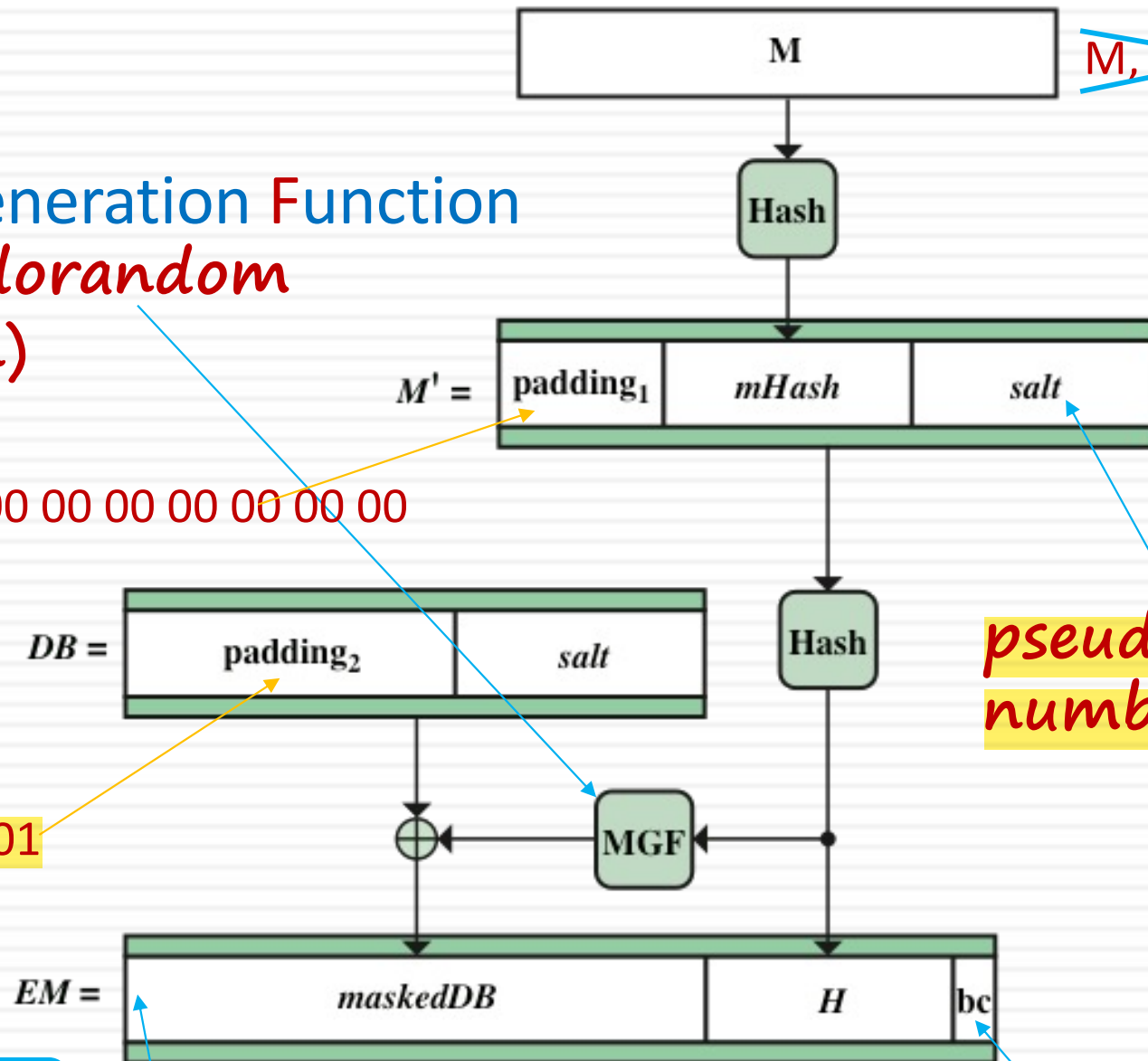


Figure 13.7 RSA-PSS Encoding