# Public Key Requirements

2. $C = E(PU_b, M)$

3. $M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$

6. $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$

A mask generation function (MGF) is a cryptographic primitive similar to a cryptographic hash function except that while a hash function's output is a fixed size, a MGF supports output of a variable length.

Mask generation functions are completely deterministic: for any given input and desired output length the output is always the same.