



Attacker

Knows: $C, PU_B, E(), D(), M$

Aim: find PR_B