



Attacker

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

Observes: operations at target

Aim: find PR_B