Public key
PU B
Private key
PR B
Plaintext
M
Encryption
E()
Ciphertext
C=E(PU B,M)
Decryption
D()
Plaintext
M=D(PR B,C)
Attacker
Knows: C, PU B, E(), D()
Aim: find M, PR B