Private key
PR A
Public key
PU A
Plaintext
M
Encryption
E()
Ciphertext
C=E(PR A,M)
Decryption
D()
Plaintext
M=D(PU A,C)