

$$m = decrypt(sk_A, c_A)$$









Alice (sk_A, pk_A)



Bob (sk_B, pk_B)