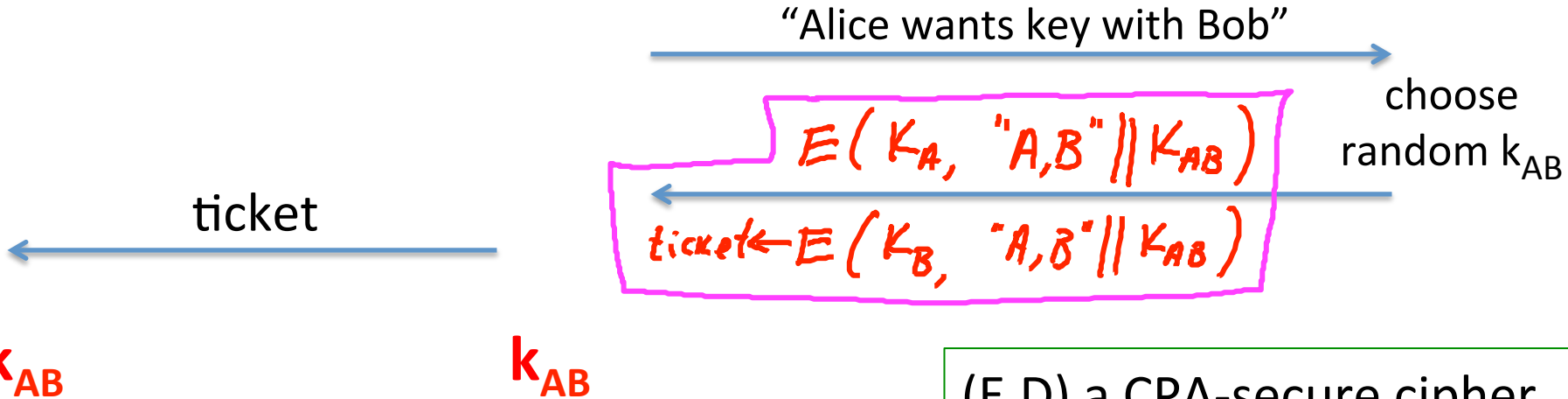


Alice wants a shared key with Bob. Eavesdropping security only.

Bob (k_B)

Alice (k_A)

TTP



(E,D) a CPA-secure cipher