SEGURIDAD

EJ 4:

A -> B: KpubA

B -> A: KpubB

A -> B: EpubB(KAB)

A -> B: EprivA(Ekab(M))

EJ 5:

A -> B: KpubA

B -> A: KpubB

A -> B: EpubB(KAB)

A -> B: Ekab(M), EprivA(H(M))