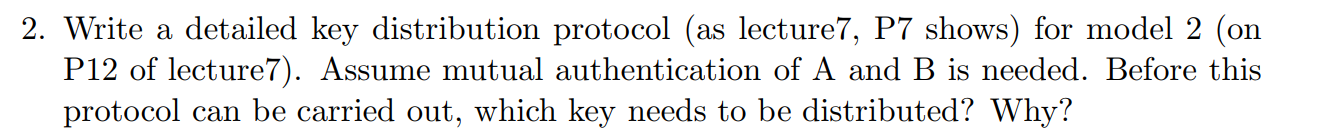
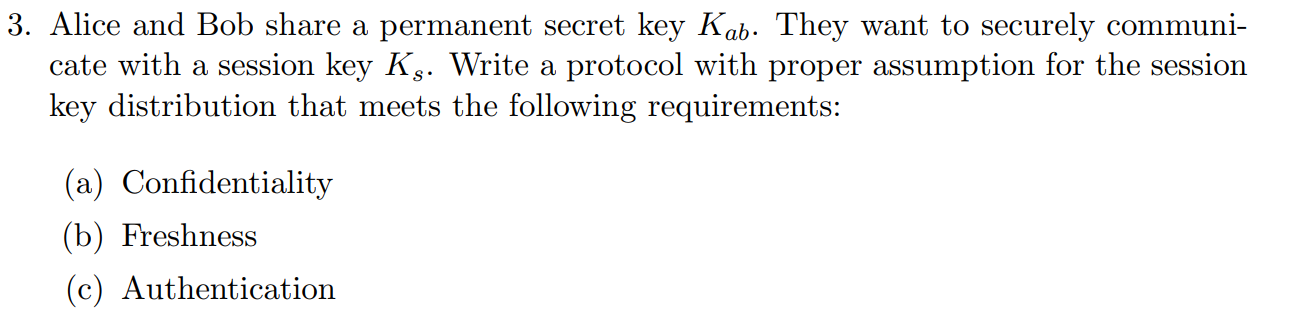
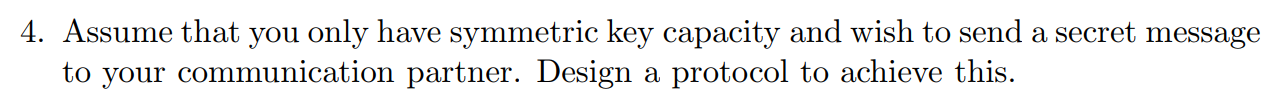
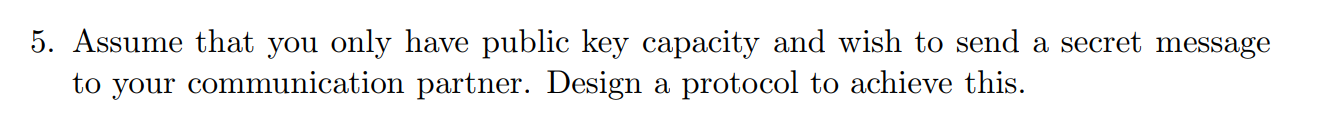
  
A public key certificate is a mechanism in which a public key authority holds the public keys of its recipients; instead of communicating continuously with the KDC; the client can register their key with the PKA and then get a certificate which contains, the public key of A, Identity of A and Timestamp; and send this certificate the individuals they want to communicate with.   
  
  
Both the master keys Ka and Kb need to be distributed beforehand because they are needed for the secure communication. Also the authentication function H needs to be agreed by both A and B.  
  
A→KDC: RequestA, N1  
KDC→A: Eka[Ks, RequestA, N1]  
B→KDC: RequestB, N2  
KDC→B: Ekb[Ks, RequestB, N2]  
A→B: Eks[N3]  
B→A: Eks[H(N3)]  
  
  
They agree on a hash function.

A→B: Ekab[RequestA, N1]  
B→A: Ekab[Ks, RequestA, N2]  
A→B: Eks[N3]  
B→A: Eks[H(N3)]  
A→B: Eks[M, F(M)]  
  


A -> B: EK2[M] || CK1(EK2[M])  
  
  
  
A🡪B: EKUb[EKRa[M]]