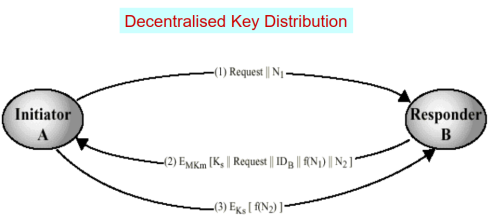
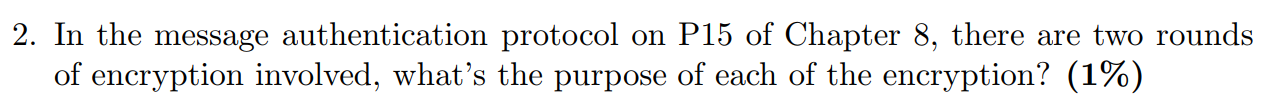
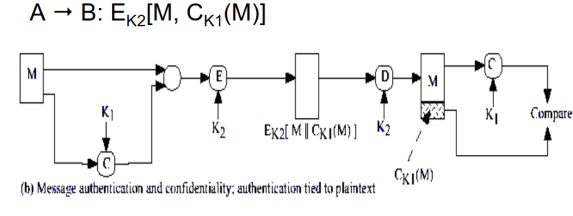
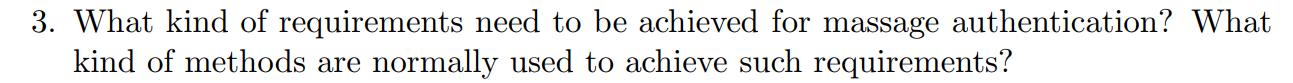


1. Encrypt the request with EMKm[request || N1]
2. The master key needs to be distributed via “secure” channel amongst A and B before it can carried out

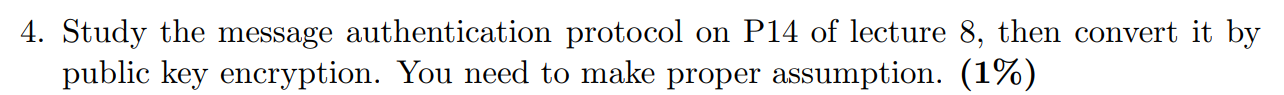


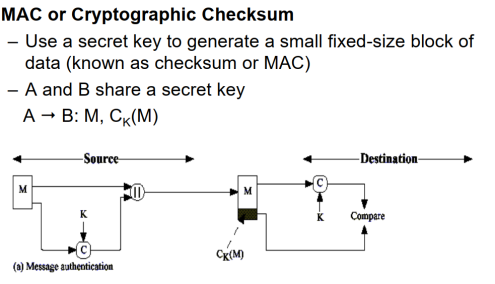


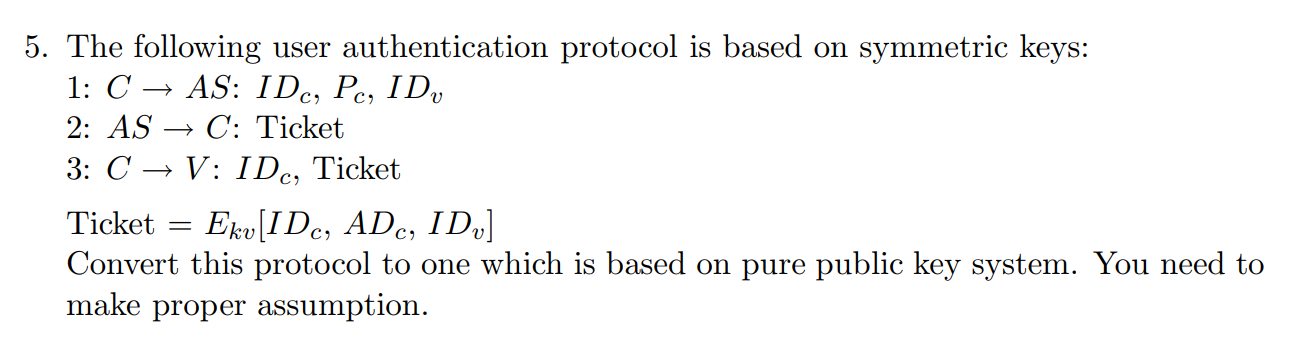
1. K1 - function of the message CK1(M); which is used for authenticity; this is concatenated with the original message [other user can apply the same function on the message to determine its origin]
2. K2 - The concatenated message Ek2[M || F(M)] is then encrypted for confidentiality [hidden from a potential attacker]



The requirement is that the receiver can guarantee authenticity with or without the use of confidentiality. There are many methods which can be used [both symmetric and asymmetric] for example by using symmetric private keys, asymmetric keys, functions or hash functions [applied to the message].



  
Instead of using the shared key, we use A’s Private Key.   
A->B M, EKra[M]  
We assume that B has been sent A’s public Key via some secure method, and B then applies public key of A to decrypt it.

  
  
  
  
  
  
  
  
  
  
Encrypt ticket with Ekra[private key of AS] – Ekra[IDc, ADc, IDv] – Assume AS has a pair of KUas & Kras, Kuas has been distributed to V