Task 3



Two parties - Alice and the Lotto Server can establish a session key or keys using the Diffie-Hellman Key Exchange method.

This can provide the basis of a secure connection between her and the Server.

• Alice cannot modify any part of the ticket after purchase.   
  
This is a function of the software running in the Lotto Server. Once the ticket is bought, the Server must ensure that the details are read only as far as Alice is concerned.   
  
• Alice does not have public and private key pair.   
  
If a key exchange mechanism is used as in the DHKE method earlier on, then this can produce transient keys that can be symmetric or a public/private pair, which are valid only for the one connection session between them. If either party forgets the agreed keys, then the whole negotiation has to be repeated.   
  
• Lotto server cannot deny Alice’s purchase and the corresponding draws.    
  
The Lotto Server should send an email confirmation of the purchase to Alice. This will be equivalent to buying a printed ticket in an outlet that provides a service for the lottery.   
  
I hope this helps.