**PA3 Requirements**

Part A

1. Read the message from the user file:  
     
   m
2. Create a message digest using SHA1:  
     
   H(m)
3. Create an initialization vector?
4. Encrypt the message digest using Alice's private key:  
     
   K-A(H(m))
5. Append the encrypted message digest to the end of the message:  
     
   (m, K-A(H(m)))
6. Generate a symmetric key using 3DES:  
     
   KS
7. Encrypt the signed message using the symmetric key:  
     
   KS(m, K-A(H(m)))
8. Encrypted the symmetric key using Bob's public key:  
     
   K+B(KS)
9. Prepend the symmetric key to the encrypted message (since it is a fixed size of 128 bits, Bob can get it by reading the first 128 bits of the cipher text):  
     
   (K+B(KS), KS(m, K-A(H(m))))
10. Send to Bob.