Rawan Alzowaid
CSCI-3753
Problem set 5

Q1:

a) Using a FAT file system:
   - 2000*4 =8000 bytes
b) Using a UNIX-style file system:
   - 1st level index blocks= 12*4 = 48 bytes
   - Single indirect blocks= 15*4 = 60 bytes
   - 2nd indirect blocks= 13*4 + 15*4*2 =172 bytes
   - 3rd indirect blocks= 13*4 + 13*4*2 + 15*4*4 = 396 bytes
   - Total= 48+60+172+396=676 bytes
c) 1099
d) 4th level down to the search

Q2:

a) Using bitmap:
   - 1024 pages * 1 bit =1024 bits = 128 bytes
b) Using a linked list:
   - (1024-1) *2+2 = 2048 bytes (includes 1023 pointers from the page and one to head to the pages)
   -
c) Linked list will me more memory efficient than bitmap when there are only few free space blocks.

Q3:

a) FCFS scheduling:
   - (97-84) +(155-84) + (155-103) + (103-96) + (197-96) =244
b) SCAN scheduling:
   - (103-97) +(155-103) + (197-155) + (199-197) + (199-96) + (96-84) =217
c) LOOK scheduling:
   - (103-97) + (155-103) + (197-155) + (197-96) + (96-84)=213

Q4:

The server first sends N, where N=p*q, to the user, the user stores N, and then sends N back to the server. Server verifies the N with p&q. User randomly generates encrypted message K with pre-stored N, and send it to the server, server then uses K for AES. Then the SSH session is now encrypted with K.

A symmetric key K encrypts it, because only the server knows the private key, and can solve that to decrypt the symmetric key K. If the hack is fake, it will receive an encrypted message K, the server will decrypt that and send back to user some non-sense characters because the user can't decrypt the message