OPERATIVSYSTEM 2008, RÄKNEÖVNING 5, v. 42
UPPGIFT 5 lämnas in senast måndag 20.10. OBS Uppgift 5 måste besvaras!

1. Oftast visas asterisker istället för bokstäver i det fält man matar in lösenord. Alternativet är att inte skriva ut något alls (för då vet en potentiell hacker som ser inmatningen inte hur långt lösenord som används). Om vi antar att lösenord består av endast gemener (’a’ till ’z’) samt är 5 till 8 tecken långa, hur mycket säkrare är det att inte visat något på skärmen? (2p)

2. Vi antar att det idag tar en timme att bryta krypteringssystem med nyckellängd på 56 bitar. Vilket år kan vi bryta ett system med 2048-bitars nyckellängd på en timme, om vi antar att processeringskapaciteten fördubblas varje halvår? (2p)

3. Beskriv stegvis vilka datastrukturer och datablock måste accesseras för att läsa första blocket i en namngiven fil, om vi antar att inget finns i cache-minnet., samt att filen finns i root-katalogen i filsystemet
    a. För ett FAT-baserat system
    b. För ett i-nod-baserat system

4. I ett filsystem där blockadministrationen sker via en filallokeringstabell (FAT) övervägs blockstorleken. Vilken skall blockstorleken vara, för att det utrymme som går förlorat vid intern fragmentering är mindre än filallokeringstabellen, då skivan är full? Vi antar att medelfilstorleken är 8 kB, samt att FAT-tabellelementen är 32 bit (2p)

5. Skriv i ditt favoritprogrammeringsspråk en implementation av hissalgoritmen, som för en given sekvens av läsningar från cylindrar skedulerar läsningarna, och beräknar totala antalet diskarmrörelser. Visa resultaten för sekvensen {12 44,89,33,51,22,73,28}.