

T-110.2100 Introduktion till datakommunikation (suomenkielinen tentti paperin toisella puolen)
Mellanförhör 1 8.3.2011

Skriv ditt studentnummer *tydligt* på varje svarpapper.

- 1 Förklara **kort** följande begrepp och förkortningar som ansluter sig till datakommunikation och datasäkerhet (6p)
 - a) Protokollstack
 - b) SSL
 - c) Port
 - d) Router (väljare)
 - e) Jämlike (peer)
 - f) Tillgänglighet

- 2 **Motivera** kort vilka av följande påståenden är sanna och vilka är inte (poängen kommer från motiveringarna) (6p)
 - a) Vid symmetrisk kryptering kan inte meddelandets integritet skyddas lika väl som i asymmetrisk.
 - b) IP skapar en virtuell krets mellan sändare och mottagare.
 - c) När du får ett certifikat från en webbserver vet du vem du har kontakt med.
 - d) Ett sekvensnummer visar vilket i ordningen ett datapaket är.
 - e) Maximistorleken på ett Ethernet-nät kommer från elektricitetens fart i ledningen.
 - f) Host-fältet tillsattes i version 1.1 av HTTP, för att man bara kunde ha en tjänst (t.ex. www.aalto.fi-webbplatsen) per IPv4-adress med version 1.0.

- 3
 - a) Du implementerar TCP/IP-protokollet på en liten och långsam mobil apparat som kallas agentklocka. Vilken av TCP:s egenskaper kan du använda för att garantera att din lilla terminals buffert inte överfylls, då du ber om klart mera hemlig agentdata från servern än det ryms i din agentklockas lilla buffert? Beskriv grundprincipen för hur egenskapen fungerar. (2p)
 - b) Beskriv två användningar för ICMP-protokollet. (2p)
 - c) Varför har IP-adresser en nätdel och en värddel? (2p)

- 4
 - a) Bedöm en nätbanks datasäkerhetsbehov enligt CIA-modellen. Vad finns det för data att skydda i banksystemet? Vilken egenskap är viktigast för varje datatyp och på vilken egenskaps bekostnad kunde den förbättras? (3p)
 - b) Beskriv hur du krypterar och signerar ett meddelande med hybridkryptering. (3p)

- 5 Det finns en TCP-förbindelse mellan två maskiner. En av maskinerna på paketens rutt har stockning och dess buffert är full för ett ögonblick.
 - a) Vad händer i routern? (1p)
 - b) Hur upptäcker maskinerna detta och reagerar på det ovannämnda? (3p)
 - c) Vad finns det för risk om routerns buffert är full längre än en kort stund? Hur garderar sig TCP mot detta? (2p)