TEKNISKA HÖGSKOLAN I STOCKHOLM
NUMERISK ANALYS OCH DATALOGI
Inge Frick

TENTAMEN
2D1522, Datorteknik och kommunikation
2D2051, Databasteknik och Datorkommunikation

Torsdagen 26 Maj 2005, kl. 8.00 – 13.00 i sal Q31, Q32, Q33

Totala poängantalet är 60 poäng + 2 bonuspoäng., ungefärliga poänggränser är 30 (betyg 3), 40 (betyg 4) och 50 (betyg 5). Poängtalet på varje uppgift ges inom parenteser i början på uppgiften.

Hjälpmedel: Utdelade databashäften. Anteckningar i häftet får endast finnas om de är strikt relaterade till kursdelen om databaser.

De olika frågorna på tentamen rättas separat. Därför är det **viktigt** att varje problem löses på ett separat (eller flera separata) papper. Deluppgifter får lösas på samma papper.

Lös EJ flera problem på samma papper!

Läs igenom frågetexten ordentligt innan du formulerar ditt svar. Kontrollera att du svarat på rätt sak.

Lämna inget underförstått! Den som rättar ska ej behöva lägga tid på att räkna ut vad du egentligen menat. Skriv läsligt och med korrekt språk. Undermåligt formulerade svar kan medföra poängavdrag.

1.-3. Se senare sidor.

4. Vilka nivåer i OSI-modellen skulle du placera in följande (motivera):
a) (*1p*) http
b) (*1p*) tcp
c) (*1p*) ip
d) (*1p*) ethernet
e) (*1p*) ssl (som används för exempelvis krypterad webb-förbindelse)
f) (*1p*) ftp

5. (*5p*) Vad är kretskopplade resp. paketkopplade nät. Förklara skillnaden och diskutera för- och nackdelar med resp. metod.

6. Kommandot 'grep kaka fil' skrivera alla rader i filen 'fil' som innehåller strängen 'kaka'. Vad skriver följande kommandon ut?
a) (*1p*) grep ^kaka$ fil
b) (*1p*) grep ^.*kaka.*$ fil
c) (*1p*) grep kak.a$ fil
d) (*1p*) grep kak*a fil
e) (*1p*) grep ^kak.a$ fil

7. (*5p*) Skriv en rimlig DTD som beskriver följande XML-kod:

```
<bookcollection>
  <book>
    <title year='1885'>Tom Sawyer</title>
    <author>Mark Twain</author>
  </book>
  <book>
    <title year='1920'>Winnie the Pooh</title>
    <author>Milne</author>
  </book>
</bookcollection>
```

8. Antag följande: Du vill kryptera ett meddelande med RSA-algoritmen. Du har valt två primtal: p=3 och q=5. Du väljer sedan krypteringsnyckeln e=7. Lös nu följande uppgifter (visa givetvis hur du går tillväga):

a) (*3p*) Räkna ut den andra delen av den publika nyckeln, dvs n och kryptera meddelandet `2`

b) (*3p*) Räkna ut dekrypteringsnyckeln d och dekryptera meddelandet `3`

9. (*5p*) Vad är ett blankettchiffer? Om man på rätt sätt använder en bra nyckel så är ett blankettchiffer oknäckbart. Varför? Förklara vilken egenskap nyckeln skall ha och hur den skall användas. Finns det något problem med blankettchiffer?

10.

a) (*2p*) Vad är det för skillnad på hur data överförs om man använder GET och POST i t.ex. ett webformulär?

b) (*2p*) Vilken metod bör man använda om man har stora datamängder som ska överföras, och varför?

11. (*4p*) HTTP-protokollet är ju tillståndslöst. Detta innebär att webbservertillämpningar måste ta till olika tekniker för att komma ihåg vem klienten är. Redogör för två sådana tekniker, hur de fungerar och vilka problem som finns.