

## Lösningförslag 2D1522, 2001-05-28

***Skriv gärna mer utförliga svar än nedan!***

1. Databas
2. Databas
3. Databas
4. Se föreläsningssanteckningar
5. a) Till nätverket  
b) Till endast 177.165.2.15  
c) Till 177.165.2.1 - 177.165.2.255
6. En fil på klientdatorn där varje server har rätt att skriva in en liten mängd data. Detta data skickas sedan över vid varje request. Det är användbart för att på servern hålla reda på ett visst "tillstånd", alltså sessionshantering
7. a) Vid POST skickas data i själva meddelandekroppen på request-meddelandet. GET har ingen meddelandekropp utan där skickas data URL-kodat i själva URLen. GET-requests går därför att lagra som bokmärken till skillnad från POST.  
b) POST eftersom det annars blir en oerhört lång URL.
8. T.ex. HTTP\_USER\_AGENT som innehåller vilken klient som ansluter (typ Mozilla eller Explorer), och QUERY\_STRING som innehåller variabler satta i t.ex. ett formulär.
9. Tre typer av användare per fil; Ägaren, Gruppen och Övriga. För var och en av dessa tre kan rättigheterna Read, Write och Execute sättas.
10. Ingen Python ingår 2002
11. Ingen Python ingår 2002
12. bv
13. a)  $n=q*p = 3*11 = 33$   
 $c=m^e \text{ mod } n$   
 $c= 2^7 \text{ mod } 33 = 128 \text{ mod } 33 = \mathbf{29}$   
b)  $d*e \text{ mod } (n-1)*(q-1) = 1$   
 $d*7 \text{ mod } 2*10 = 1$   
 $7d \text{ mod } 20 = 1$   
Test ger att  $d=\mathbf{3}$  uppfyller villkoret dvs  $21 \text{ mod } 20 = 1$   
 $m=c^d \text{ mod } n$   
 $m=10^3 \text{ mod } 33$   
 $m=1000 \text{ mod } 33 = \mathbf{10}$   
( $30*33 = 990$ ;  $1000 - 990 = 10$ )