

*Skriv ditt studentnummer tydligt på varje svarsapper. Man får använda räknare i mellanförhöret, men det behövs inte.*

1. **Förklara kort** följande begrepp och förkortningar som ansluter sig till datakommunikation och datasäkerhet (6p)

- a. Distribuerat system
- b. CIA-modellen
- c. Router (väljare)
- d. DNS
- e. CIDR
- f. Socket API

2. **Motivera kort** vilka av följande påståenden är sanna och vilka är inte (poängen kommer från motiveringarna) (6p)

- a. WLAN använder ett åtkomstprotokoll (media access protocol) som bygger på att upptäcka kollisioner
- b. Ett meddelande som krypterats med en bra, modern krypteringsalgoritm är praktiskt tagit omöjligt att bryta
- c. Överföringsfel på fysiska skiktet orsakas nästan alltid av komponenter av dålig kvalitet
- d. Att skriva ett serverprogram är mer utmanande än att skriva ett klientprogram
- e. 196.236.260.1 är en funktionsduglig IP-adress
- f. IP erbjuder tillförlitlig dataöverföring

3. **AJAX & TCP**

- a. Definiera AJAX (i kursens sammanhang). Vad gör man med det? Vilka teknologier använder man i AJAX? (3p)
- b. Hur öppnas en TCP-förbindelse? Hur stängs den? Varför? (3p)

4. **Datasäkerhet**

- a. Du surfar webben och märker att HTTPS-protokollet har använts för att överföra webbsidan. Hur har din webbläsare försäkrat sig om att sidan härstammar från den server vars namn står i webbläsarens adressfält? (4p)
- b. Läs vidstående artikel om datasäkerhet i näthandel. Vilka begrepp blandar journalisten ihop? Hur skulle du kritisera artikeln? (2p)

5. **Protokollstack (6p)**

Nedan finns en bild av en Ethernet-ram. Vilka skikt i TCP/IP-protokollstacken finns pakethuvuden A,B,C och D i? Vilka är de olika skiktens uppgifter och vilken information bör det finnas i huvudet för varje skikt för att skikten skall kunna utföra sina uppgifter?

A	B	C	D	Data	A
---	---	---	---	------	---