

Skrivningskod:   
Glöm den inte!

Om du vill:   
Lägg till tre bokstäver.

KTH Matematik  
Olof Heden

| $\Sigma$ p | G/U | bonus |
|------------|-----|-------|
|            |     |       |

| Efternamn | förnamn | pnr | årskurs |
|-----------|---------|-----|---------|
|           |         |     |         |

**Kontrollskrivning 4B, torsdagen den 3 maj 2007, 10.15–11.15,  
i 5B1118 Diskret matematik för Media1**

Inga hjälpmedel tillåtna.

Minst 8 poäng ger godkänt.

Godkänd ks  $n$  medför godkänd uppgift  $n$  vid tentor till (men inte med) nästa ordinarie tenta (högst ett år),  $n = 1, \dots, 5$ .

13–15 poäng ger ett ytterligare bonuspoäng till tentamen.

**Uppgifterna 3)–5) kräver väl motiverade lösningar för full poäng.**

Uppgifterna står inte säkert i svårighetsordning.

**Spara alltid återlämnade skrivningar till slutet av kursen!**

Skriv dina lösningar och svar på samma blad som uppgifterna, använd baksidan om det behövs.

1) (För varje delfråga ger rätt svar  $\frac{1}{2}$ p, inget svar 0p, fel svar  $-\frac{1}{2}$ p.)  
Totalpoängen på uppgiften rundas av uppåt till närmaste icke-negativa heltal.)  
**Kryssa för** om påståendena **a)–f)** är sanna eller falska (eller avstå!)

|  | sant | falskt |
|--|------|--------|
| a) Ett RSA-krypto kan ha de offentliga nycklarna $n = 36$ och $e = 5$ .  |      | x      |
| b) I ett RSA-krypto kan den hemliga parametern $m$ var lika med 15.  |      | x      |
| c) 000 och 111 bildar orden i en 1-felsrättande kod av längd 3.  | x    |        |
| d) En linjär binär kod innehåller alltid $2^n$ stycken ord för något heltal $n$ .  | x    |        |
| e) Antalet olika Booleska funktioner i tre variabler $x, y, z$ är $2^8$ .  | x    |        |
| f) Uttrycket $xyz + \bar{x}\bar{y}\bar{z} + yz$ är en disjunktiv normalform för någon Boolesk funktion i variablerna $x, y, z$ . |      | x      |

|                 |
|-----------------|
| poäng<br>uppg.1 |
|                 |

| Namn | poäng<br>uppg.2 |
|------|-----------------|
|      |                 |

**2a)** (1p) En kod  $C$  har kontrollmatrisen (parity-check matrisen)

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Du tar emot ordet 111000 som inte tillhör koden. Rätta detta ord till ett kodord på avstånd ett från detta ord.

**Svar:** 1110100

**(Lösning:**

$$H \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix},$$

vilket är kontrollmatrisens femte kolonn. Så felet var i femte positionen.)

**b)** (1p) Låt  $C$  vara som ovan. Ange tre olika kodord.

**Svar:** Text 0000000, 1111111, 1110100.

**c)** (1p) Ett RSA-krypto har de offentliga nycklarna  $n = 21$  och  $e = 5$ . Ange  $d$ .

**Svar:**  $d = 5$ .

**(Lösning**  $m = 2 \cdot 6 = 12$  och söker  $d$  sådant att  $e \cdot d \equiv 1 \pmod{m}$ ), varvid vi gissar att  $d = 5$  vilket är en bra gissning eftersom  $5 \cdot 5 = 2 \cdot 12 + 1$ .)

|      |                 |
|------|-----------------|
| Namn | poäng<br>uppg.3 |
|      |                 |

**3)** (3p) Skriv det Booleska uttrycket  $yu + \bar{y}u$  i de fyra variablerna  $x, y, z, u$

a) på en disjunktiv normalform.

b) på en minimal disjunktiv form.

a) **Svar:** Vi de rutor som motsvarar uttrycket i ett Karnaughdiagram (alternativt multiplicerar uttrycket med  $(x + \bar{x})(z + \bar{z})$ ) och får då 8 markerade rutor vilket motsvarar den disjunktiva normalformen

$$yuxz + yux\bar{z} + yu\bar{x}z + yu\bar{x}\bar{z} + \bar{y}uxz + \bar{y}ux\bar{z} + \bar{y}u\bar{x}z + \bar{y}u\bar{x}\bar{z}.$$

b) **Svar:** Ur Karnaughdiagrammet (eller av att  $yu + \bar{y}u = (y + \bar{y})u = u$ ) får vi den minimala formen  $u$ .

| Namn | poäng<br>uppg.4 |
|------|-----------------|
|      |                 |

4) (3p) Givet är ett RSA-krypto med de offentliga nycklarna  $n = 33$  och  $e = 3$ . Dekryptera det krypterade meddelandet 2.

**Lösning:**  $n = 33 = 3 \cdot 11$  ger att  $m = (3 - 1)(11 - 1) = 20$ . Söker  $d$  sådant att  $3 \cdot d \equiv 1 \pmod{20}$  varvid vi ser att  $d = 7$  duger bra.

Dekrypteringen av 2 är då

$$2^7 \pmod{33} = 128 \pmod{33} = 29.$$

**Svar:** 29.

|      |                 |
|------|-----------------|
| Namn | poäng<br>uppg.5 |
|      |                 |

5) (3p) Låt  $C$  bestå av de ord  $c_1c_2c_3c_4c_5$  sådana att

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Bestäm antalet binära ord som ligger på avståndet ett från ord i koden.

**Lösning:** Antal ord i koden är

$$2^{\text{antal kolonner} - \text{antal rader}} = 2^2 = 4$$

Till varje ord av längd 5 finns precis fem ord på avståndet 1, nämligen man har precis fem olika möjligheter att göra ett fel i ett kodord. Inget ord ligger på avstånd ett från två olika kodord. Totalt ligger alltså precis

$$4 \cdot 5 = 20$$

ord på avståndet ett från något kodord.