**Skrivningskod:** Glöm den inte!

**Om du vill:** Lägg till tre bokstäver.

**KTH Matematik**
B.Ek

| Σ p | G/U | bonus |
|---|---|---|
| | | |

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

**Kontrollskrivning 4, on 25 april 2007, 8.15–9.15,**
**i 5B1118 Diskret matematik för CL2 och CL3**

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), $n = 1, \ldots, 5$.
13–15 poäng ger ett ytterligare bonuspoäng till tentamen.
**Uppgifterna 2)–5) kräver 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)** | **Avståndet** (distansen) mellan orden 1101011 och 1001101 i en binär kod är 3. | | |
| **b)** | Den linjära koden med kontrollmatris $\begin{matrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{matrix}$ har dimension 3. | | |
| **c)** | I ett RSA-system med parametrar $n, m, e, d$ offentliggörs normalt $n, m$ och $e$. | | |
| **d)** | Ett **carmichaeltal** är ett primtal som för minst en bas inte klarar fermattestet. | | |
| **e)** | Med **boolesk algebra** kan man forma om satslogiska sentenser till logiskt ekvivalenta sentenser. | | |
| **f)** | Den booleska funktionen $f(x, y, z, w) = x\overline{y}z + yz\overline{w}$ är given på **disjunktiv normalform**. | | |

| poäng uppg.1 |
|---|
| |

| Namn | poäng uppg.2 |
|---|---|
| | |

**2a)** (1p) Man har en binär kod $\mathcal{C}$ av längd 6.
Hur många ord kan $\mathcal{C}$ högst innehålla, om man säkert kan rätta upp till två uppkomna fel i kodens ord? Man får inte förutsätta att $\mathcal{C}$ är linjär.
Motivera ditt svar.

**b)** (1p) Formulera **Fermats lilla sats**.
Var noga med att inte missa någon förutsättning.

**c)** (1p) Skriv upp värdetabellen för den booleska funktionen

$$f(x, y, z) = (\overline{x\overline{y} + yz})(x + \overline{y}z).$$

| Namn | poäng uppg.3 |
|---|---|
| | |

**3)** En linjär kod definieras av kontrollmatrisen (i boken kallad checkmatrisen)

$$\mathbf{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

**a)** (1p) Vilket eller vilka (om något) av följande är ord i koden?

$$010110, 111010, 111100$$

**b)** (2p) Om man tar emot 101101 och högst ett fel har uppstått, vilket var det sända kodordet?

| Namn | poäng uppg.4 |
|---|---|
| | |

**4)** (3p) I ett (pytte-)RSA-system används en offentlig nyckel för kryptering $(n, e) = (527, 113)$.
Finn talet $d$ som behövs för att dekryptera meddelanden i detta system.
$(527 = 17 \cdot 31)$

| Namn | poäng uppg.5 |
|---|---|
| | |

**5)** Betrakta den booleska funktion $f(x, y, z)$ som ges av värdetabellen

| $x$ | $y$ | $z$ | $f(x, y, z)$ |
|---|---|---|---|
| 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 0 | 0 | 1 |

**a)** (1p) Skriv $f(x, y, z)$ som ett booleskt uttryck (dvs ett uttryck med $x, y, z$ och $+, \cdot, ^-$) på **disjunktiv normalform, dnf**.

**b)** (2p) Uttryck med hjälp av ett **karnaughdiagram** $f(x, y, z)$ som ett **minimalt** disjunktivt uttryck.

*Lösningar kommer att läggas ut på kurssidan efter skrivningen.*