Skrivningskod: Glöm den inte!

Om du vill: Lägg till tre bokstäver.

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

Kontrollskrivning 4B, onsdagen den 5 december 2007, 13.15–14.15, i SF1610 Diskret matematik för IT2.

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 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)	Avståndet i en 4-felsrättande kod är alltid minst 9.	x	
b)	Ett RSA-krypto kan ha $n = 19$.		x
c)	I en Boolesk algebra gäller allmänt att $a\bar{a} = 0$	x	
d)	Det Booleska uttrycket $x\bar{y}z + x\bar{y}z$ i de tre variablerna x, y och z, är skrivet på minimal disjunktiv form.		x
e)	I ett RSA-krypto med $n = 35$ kan e vara lika med 6.		x
f)	Det finns linjära koder med 31 element.		x

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) En 1-felsrättande kod har kontrollmatrisen (parity check-matrisen)

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Rätta ordet 11111.

SVAR: 11011

b) (1p) Ett RSA-krypto har $n = 143$. Välj lämpliga nycklar e och d.

SVAR: e och d skall uppfylla $e \cdot d \equiv 1 \pmod{10 \cdot 12}$ så t ex $e = 11$ och $d = 11$

c) (1p) Ange antalet Booleska funktioner i de tre variablerna x, y och z.

SVAR: $2^8 = 256$.

Namn	poäng uppg.3

3) (3p) Skriv den Booleska funktionen $xyzw + x\bar{w}$ på en minimal disjunktiv form.

LÖSNING man ritar ett karnaugh diagram och ser då att en minimal disjunktiv form är $xyz + x\bar{w}$.

Namn	poäng uppg.4

4) (3p) I ett RSA-krypto är $n = 15$ och $e = 3$. Dekryptera meddelandet 3, dvs bestäm $D(3)$.

LÖSNING $n = 3 \cdot 5$ ger $m = 2 \cdot 4 = 8$. Då $3 \cdot 3 \equiv 1 \pmod{m}$ har vi att $d = 5$. Så $D(3) = 3^3 = 27 \equiv 12 \pmod{15}$.

Namn	poäng uppg.5

5) (3p) Konstruera en 1-felsrättande kod bestående av 32 ord och med så kort ordlängd som möjligt.

LÖSNING Antalet ord i koden är 2 upphöjt till antalet kolonner i kontrollmatrisen minus antalet rader. Denna skillnad måste vara precis 5 om antalet ord i koden skall vara 32. Och kolonnerna skall vara olika. Med ordlängd 8 skulle antalet rader vara 3 men det finns högst 7 olika kolonner av höjd 3. Men med nio fungerar det. T ex kan vi ha kontrollmatrisen

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