Skrivningskod: Glöm den inte!

Om du vill: Lägg till tre bokstäver.

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

Lösning till kontrollskrivning 4B, 9 oktober 2009, 10.45–11.45, i SF1610 Diskret matematik för CINTE.

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)	Ett RSA-krypto kan ha parametrarna $n = 81$, $e = 5$.		x
b)	Ett RSA-krypto kan ha $e = 3$ och $d = 4$.		x
c)	I varje Boolesk algebra gäller $b\bar{b} = 0$.	x	
d)	I varje Boolesk algebra är $ab + b = b$.	x	
e)	En kod med ett jämnt minimiavstånd kan aldrig rätta några fel.		x
f)	Om minavståndet i en kod C är 7 så är C en 3-felsrättande kod	x	

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Betrakta en felkorrigerande kod C med kontrollmatrisen

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

Rätta ordet 0111110.

Lösnng:

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

vilket är kontrollmatrisens sjätte kolonn. Fel i position sex och alltså

SVAR: 011110

b) (1p) Ett RSA-krypto har $n = 55$. Vilka värden på parametern e kan man välja om e skall ligga i intervallet $10 \leq e \leq 15$.

Lösnng: Då $n = 55 = 5 \cdot 11$ så $m = 4 \cdot 10 = 40$. Krav på e är att $\gcd(e, 40) = 1$. I intervallet 10 till 15 är det de udda talen som uppfyller detta krav så

SVAR: Möjliga värden på parametern e är 11 och 13.

c) (1p) Hur många Booleska funktioner $f(x, y, z)$ i tre variabler uppfyller

$$f(0,1,0) = 1, \quad f(1,0,0) = 0, \quad f(0,1,1) = 1, \quad f(1,0,1) = 0, \quad f(1,1,0) = 1.$$

Lösnng: Vi kan fritt välja värden 0 eller 1 till $f(0,0,1)$, $f(0,0,0)$ och $f(1,1,1)$. Funktiones värden i de övriga punkterna är givna. Så

SVAR: 2^3 dvs 8.

Namn	poäng uppg.3

3) (3p) Ett RSA-krypto har $n = 85$ och $e = 13$. Dekryptera meddelandet 2, dvs bestäm $D(2)$.

Lösnng: Då $n = 85 = 5 \cdot 17$ så $m = 4 \cdot 16 = 64$. Krav på d är att $e \cdot d \equiv 1 \pmod{m}$. Vi minns att $13 \cdot 5 = 65 \equiv_{64} 1$ så $d = 5$.

Vidare gäller ju allmänt att $D(a) = a^d \pmod{n}$, och vi får

SVAR: $2^5 \pmod{85} = 32$.

Namn	poäng uppg.4

4) (3p) Skriv på en minimal disjunktiv form följande booleska uttryck

$$\bar{y}\bar{w} + xy\bar{z}\bar{w} + \bar{x}\bar{y}w.$$

Lösnng: Motsvarande Karnaughdiagram ser ut som följer

	xy	$x\bar{y}$	$\bar{x}\bar{y}$	$\bar{x}y$
zw	0	0	1	0
$z\bar{w}$	0	1	1	0
$\bar{z}\bar{w}$	1	1	1	0
$\bar{z}w$	0	0	1	0

Vi sammanför till så stora rektanglar av formatet 1 ruta, två, fyra eller åtta rutor som möjligt och finner då att disjunktionen av konjunktionerna $\bar{y}\bar{w}$, $\bar{x}\bar{y}$ och $x\bar{z}\bar{w}$ minimerar antalet konkunktioner och antalet literaler i konjunktionerna, så

SVAR: $\bar{y}\bar{w} + \bar{x}\bar{y} + x\bar{z}\bar{w}$

Namn	poäng uppg.5

5) (3p) Bestäm kontrollmatrisen till en 1-felsrättande kod som innehåller bland annat orden 11100000 och 10011100 och som totalt består av 16 olika ord.

Lösnng: Söker en matris H med $k = 8$ kolonner, (eftersom orden har längd 8), och $r = 4$ rader eftersom då blir antalet ord som den sökta koden C innehåller lika med

$$|C| = 2^{k-r} = 2^4 = 16.$$

Att de givan orden tillhör koden innebär att summan av de tre första kolonnerna i H skall bli nollkolonnen och att summan av kolonnerna 1, 4, och 6 skall bli nollkolonnen. En systematisk uppställning av H ger då

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

som ger att summan av de tre första kolonnerna blir noll oberoende av de övriga kolonnerna. Nu kompletterar vi så att nästa krav blir uppfyllt

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

sen kan vi välja de två övriga kolonnerna hur vi vill, bara de inte är nollkolonnen eller lik någon av de redan givna kolonnerna, så

SVAR: T ex

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