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, 5 oktober 2010, 15.45–16.45, 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)	I varje RSA-krypto med parametrarna n, e och d gäller det att $ed \equiv 1 \pmod{n-1}$.		x
b)	I varje Boolesk algebra är $\overline{(x+y)} = xy$.		x
c)	Minimiavståndet i en 1-felsrättande kod är 2.		x
d)	Ett RSA-krypto kan ha $n = 60$.		x
e)	En kontrollmatris till en 1-felsrättande kod kan ha 3 rader och 8 kolonner.		x
f)	I varje Boolesk algebra gäller att om $a + b = 0$ så är $a = 0$ och $b = 0$.	x	

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Ett RSA-krypto har $n = 33$ och $e = 7$. Ange $D(2)$, dvs det tal man får när man dekrypterar talet 2.

SVAR MED LÖSNING: $n = 3 \cdot 11$ medför att $m = (3-1)(11-1) = 20$. Vidare skall ju $e \cdot d \equiv 1 \pmod{m}$ och då $7 \cdot 3 = 21 \equiv 1 \pmod{20}$ så $d = 3$. Alltså

SVAR: $D(2) = 2^d \pmod{n} = 2^3 \pmod{33} = 8$

b) (1p) Låt den Booleska funktionen $f(x, y, z)$ i de tre variablerna x, y och z definieras genom

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

Bestäm $f(0, 1, 0)$.

SVAR MED LÖSNING: Med räkningar i en Boolesk algebra får vi

$$f(0, 0, 1) = 0 \cdot 1 \cdot 0 + \bar{0}(1 + 0) + \overline{(\bar{1} + 0)} = 0 + 1 \cdot 1 + 1 \cdot 1 = 0 + 1 + 1 = 1 \, .$$

c) (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 1101010.

SVAR MED LÖSNING:

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

vilket är kontrollmatrisens första kolonn så fel i position 1.

SVAR: 0101010.

Namn	poäng uppg.3

3) (3p) Bestäm en minimal disjunktiv form till den Booleska funktionen

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

LÖSNING: Ritar upp motsvarande Karnaughdiagram

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

Enligt Karnaughts metod bildar vi rektanglar av formatet 1, 2, 4, eller 8 som bara innehåller ettor, och redovisar de Booleska utryck som dessa rektanglar motsvarar, och med så få ”ingredienser” som möjligt. Vi får då

SVAR: Till exempel $f(x,y,z) = yz + \bar{y}\bar{z} + \bar{x}y$.

Namn	poäng uppg.4

4) (3p) Bestäm ett RSA-krypto, dvs bestäm de tre parametrarna n, e och d, med kravet på parametrarna n och e att $45 < n < 55$ och $2 < e < 9$.

LÖSNING: Tag t ex $n = 51$ som är produkten av de skilda primtalen 3 och 17. Detta ger m värdet $m = (3-1)(17-1) = 32$ och vi kan t ex låta $e = 3$, ty sgd$(3, 32) = 1$. Emedan $3 \cdot 11 = 33 \equiv 1 \pmod{32}$ blir då $d = 11$. Så t ex

SVAR: $(n, e, d) = (51, 3, 11)$.

Namn	poäng uppg.5

5) (3p) Bestäm kontrollmatrisen till en 1-felsrättande kod C vars ord har längden 9 och antalet kodord är 64, dvs $|C| = 64$, och som rättar ordet 101111001 till ordet $101011001 \in C$.

LÖSNING: Om ordet $\bar{c} = 101011001$ tillhör C så kommer alla ord på avstånd ett att rättas till detta ord med hjälp av kontrollmatrisen, och eftersom det givna ordet $\bar{x} = 101111001$ ligger på avstånd ett från $\bar{c}$ så rättas $\bar{x}$ just till detta ord. Vi behöver alltså] endast tänka på att skapa en kod med föreskrivna specifikationer och som innehåller ordet $\bar{c}$.

Antalet ord skall vara 32 och ordlängden är uppenbarligen 9 eftersom ordet $\bar{c}$ har denna längd. Om nu r betecknar antalet rader i en kontrollmatris H till C, och eftersom antalet kolonner i H skall vara 9 får vi sambandet

$$32 = 2^{9-r} \ ,$$

vilket ger att $r = 4$. det enda återstående kravet att uppfylla är att ordet $\bar{c}$ skall tillhöra C, men så blir fallet om summan av kolonnerna nummer 1, 5, 6 och 9 blir nollkolonnen (de positioner i vilka det finns ettor i ordet $\bar{c}$. Vi fixar nu detta

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

Ytterligare krav på kontrollmatrisen är att kolonnerna är sinsemellan olika ock skilda från nollkolonnen. Vi fixar nu detta:

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