Skrivningskod: Glöm den inte!		**Om du vill:** Lägg till tre bokstäver.	

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

Lösningar till kontrollskrivning 4A, onsdagen den 8 oktober 2008, 09.15–10.15, i SF1610 Diskret matematik för IT2.

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 ett RSA-krypto med $n = p \cdot q$ måste p och q vara olika primtal.	x	
b)	Koden $C = \{00000, 11111\}$ är 2-felsrättande.	x	
c)	I varje Boolesk algebra gäller det alltid att $ab + c = (a + c)(b + c)$	x	
d)	Det Booleska uttrycket $x + \bar{y}z$ i de tre variablerna x, y och z, är skrivet på minimal disjunktiv form.	x	
e)	I ett RSA-krypto med $n = p \cdot q$ kan e aldrig vara lika med $p - 1$.	x	
f)	Om en kontrollmatris H har 7 rader och 3 kolonner kan samtliga ord av längd 7 rättas.	x	(x)

poäng uppg.1

Namn	poäng uppg.2

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

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

Rätta ordet 111101.

SVAR: 111100 (ty matrisen multiplicerad med givna ordet ger den sista kolonnen och därför, om bara ett fel uppstått vid informationsöverföringen, så var felet i den sista positionen.

b) (1p) Ett RSA-krypto har $n = 35$. Varför kan man inte ha nyckeln $e = 16$ i kryptot?

SVAR: $n = 35 = 5 \cdot 7$ ger att $m = 4 \cdot 6 = 24$ men elementet 16 är inte inverterbart i ringen Z_{24} eftersom $sgd(24, 16) \neq 1$.

c) (1p) Förenkla uttrycket $x + xy$.

SVAR: $x + xy = x(1 + y) = x \cdot 1 = x$.

Namn	poäng uppg.3

3) (3p) I ett RSA-krypto är $n = 33$ och $e = 7$. Dekryptera meddelandet 2, dvs bestäm $D(2)$. (OBS värdet av $D(2)$ skall beräknas)

LÖSNING: $n = 3 \cdot 11$ ger att $m = (3-1)(11-1) = 20$. För dekrypteringsnyckeln d skall gälla att $e \cdot d = 1$ i ringen Z_m. Vi gissar lätt att $d = 3$ ty $7 \cdot 3 \equiv 1 \pmod{20}$.

Formeln för dekryptering ger nu att

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

Namn	poäng uppg.4

4) (3p) (3p) Bestäm en kontrollmatris H till en 1-felsrättande kod C med ord av längd 10 och som är sådan att C har så många ord som möjligt.

LÖSNING: Kontrollmatrisen skall bestå av 10 distinkta kolonner, som ingen är nollkolonnen. Eftersom det bara finns sju olika sådana kolonner av höjd tre, så måste antalet rader i kontrollmatrisen vara minst fyra. Antalet ord i koden är 2^{10-n} där n är antalet rader, så antalet ord blir störst när n är som minst, i detta fall $n = 4$. Vi ger nu en sådan kontrollmatris H:

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

Namn	poäng uppg.5

5) Skriv den Booleska funktionen $\overline{xyzw + \bar{x}y\bar{z}w}$ på en minimal disjunktiv form.

LÖSNING: Vi ritar ett karnaughdiagram och markerar de rutor som utgör komplementet till rutorna $xyzw$ och $\bar{x}y\bar{z}w$:

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

Med Karnaughs metod för vi samman rutor till rektanglar som består av 1, 2, 4, eller 8 rutor, vilket ger det booleska uttrycket

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