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

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.

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

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

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

Namn	poäng uppg.3

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

Namn	poäng uppg.4

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

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

Namn	poäng uppg.5

5) (3p) Bestäm kontrollmatrisen till en 1-felsrättande kod som innehåller bland annat orden 11100000 och 1001110 och som totalt består av 16 olika ord.