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 4A, torsdagen den 3 maj 2007, 10.15–11.15, i 5B1118 Diskret matematik för Media1

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 de offentliga nycklarna $n = 49$ och $e = 5$.		
b)	I ett RSA-krypto kan den hemliga parametern m var lika med 35.		
c)	000 och 111 bildar orden i en 1-felsrättande kod av längd 3.		
d)	En linjär binär kod innehåller alltid 2^n stycken ord för något heltal n.		
e)	Antalet olika Booleska funktioner i tre variabler x, y, z är 8.		
f)	Uttrycket $xyz + \bar{x}\bar{y}\bar{z} + yz$ är en disjunktiv normalform för någon Boolesk funktion i variablerna x, y, z.		

poäng uppg.1

Namn	poäng uppg.2

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

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

Du tar emot ordet 111000 som inte tillhör koden. Rätta detta ord till ett kodord på avstånd ett från detta ord.

b) (1p) Låt C vara som ovan. Ange tre olika kodord.

c) (1p) Ett RSA-krypto har de offentliga nycklarna $n = 21$ och $e = 7$. Ange d.

Namn	poäng uppg.3

3) (3p) Skriv det Booleska uttrycket $yu + y\bar{u}$ i de fyra variablerna x, y, z, u

a) på en disjunktiv normalform.

b) på en minimal disjunktiv form.

Namn	poäng uppg.4

4) (3p) Givet är ett RSA-krypto med de offentliga nycklarna $n = 33$ och $e = 3$. Dekryptera det krypterade meddelandet 2.

Namn	poäng uppg.5

5) (3p) Låt C bestå av de ord $c_1c_2c_3c_4c_5$ sådana att

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Bestäm antalet binära ord som ligger på avståndet ett från ord i koden.