KTH Matematik
B.Ek

Σ p	G/U

Efternamn	förnamn	pnr	årskurs

Kontrollskrivning 4, on 9 april 2008, 10.15–11.15,
i SF1610(/5B1118) Diskret matematik för CL

Inga hjälpmedel tillåtna.
Minst 8 poäng ger godkänt.
Godkänd ks n medför godkänd (3p) uppgift n vid tentor till (men inte med) nästa ordinarie tenta (högst ett år), $n = 1, \ldots, 5$.
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) (På **a)**–**f)** 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 är sanna eller falska (eller avstå)!

poäng uppg.1

		sant	**falskt**
a)	Koden $\mathcal{C} = \{1010, 1101, 0111\}$ är 1-felsrättande.		
b)	Koden $\mathcal{C} = \{00000, 11010, 10011, 01001\}$ är en **linjär kod**.		
c)	I ett krypteringssystem med **offentlig nyckel** bör man ha en krypteringsfunktion E som saknar invers.		
d)	Om ett tal N klarar fermattestet med bas ett primtal p, vet vi säkert att N är ett primtal.		
e)	Den satslogiska sentensen $\neg(A \vee B) \rightarrow (A \rightarrow B)$ är en **tautologi**, dvs den är sann i alla tolkningar.		
f)	Om $\mathcal{B}$ är en boolesk algebra och $p, q, r, s \in \mathcal{B}$ gäller $p \cdot q + r \cdot s = (p + r) \cdot (q + r) \cdot (p + s) \cdot (q + s)$.		
g)	Detta påstående är inte sant.		

Namn	poäng uppg.2

2a) (1p) Avgör om en linjär kod med kontrollmatrisen (checkmatrisen)

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

säkert kan rätta ett fel.
Om den kan det, rätta ordet 01111.
Om den inte kan det, ange ett ord med ett fel som inte kan rättas.

b) (1p) A vill sända ett krypterat meddelande till B, som skall vara säker på att A skrivit det.
Hur kan A göra om de använder RSA-kryptering där person i har dekrypteringsfunktionen D_i och (den offentliga) krypteringsfunktionen E_i (i =A,B)?

c) (1p) Låt $f(x, y, z)$ vara den booleska funktion som har $f(1, 1, 0) = f(1, 0, 1) = f(0, 0, 1) = 1$, alla övriga värden 0.
Uttryck $f(x, y, z)$ på **disjunktiv normalform**.

Namn	poäng uppg.3

3) (3p) Vilken är den minimala (ord)längden för en linjär, 1-felsrättande kod som innehåller 32 ord?
(Tips: Vad är sambandet mellan antalet (linjärt oberoende) rader i kontrollmatrisen och ordlängden?)

Namn	poäng uppg.4

4) (3p) I ett RSA-system för kryptering används parametern $e = 15$ i krypteringsfunktionen.
Visa att precis ett av värdena $75, 85, 95$ är möjligt för "det stora talet n" och ange det värdet.
Kan man för det n-värdet ta dekrypteringsparametern $d = 7$? Motivera.

Namn	poäng uppg.5

5) (3p) Uttryck den booleska funktionen

$$f(x, y, z, w) = xyzw + x\bar{z}\bar{w} + \bar{x}y\bar{w} + \bar{x}\bar{y}\bar{z}\bar{w} + yz\bar{w}$$

på **minimal disjunktiv form**, dvs disjunktiv form med så få '$\cdot$' och '+' som möjligt. ('$\cdot$' skall förstås räknas även när de underförstås.)

Lösningar kommer att läggas ut på kurssidan efter skrivningen.