KTH Matematik
B.Ek

Σ p	G/U	bonus

Efternamn	förnamn	pnr	program

Kontrollskrivning 4, må 3 maj 2010, 9.00–10.00,
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), $n = 1, \ldots, 5$.
13–15 poäng ger ett ytterligare bonuspoäng vid samma tentor.
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)	Om alla kodord utom $00\ldots0$ i en binär, linjär kod innehåller minst tre 1:or, rättar koden minst ett fel.		
b)	Om kontrollmatrisen H för en binär, linjär kod är av typ 3×8, finns minst ett fel som koden inte kan rätta.		
c)	$35^{2010} \equiv 3 \pmod{11}$.		
d)	Om p och q är olika primtal, $n = p \cdot q$, $m = (p-1)(q-1)$ och $s \equiv 1 \pmod{n}$ så är säkert $x^s \equiv x \pmod{m}$.		
e)	Den booleska funktionen $f(x, y, z) = x\bar{y} + y\bar{z}$ är given på disjunktiv normalform.		
f)	$(q \to p) \wedge (p \to \neg\, q) \equiv p$ gäller för alla satslogiska sentenser p och q. ('$\equiv$' betecknar logisk ekvivalens).		

Namn	poäng uppg.2

2a) (1p) Man vill skapa en binär kod av längd 13 som rättar två fel. Ge en (ganska bra) övre gräns för antalet ord i koden.
Koden förutsätts inte vara linjär.
Svaret får innehålla heltal, de fyra vanliga räknesätten och potenser.

b) (1p) A och B har varsitt krypteringssystem med offentliga krypteringsfunktioner E_A och E_B och hemliga avkrypteringsfunktioner D_A och D_B. B vill kryptera och skicka meddelandet $\boldsymbol{x}$ till A, så att ingen obehörig kan läsa det och A kan vara säker på att det kommer från B. Hur kan han göra?

c) (1p) Uttryck

"Om det regnar eller det är natt (eller båda), så är det inte en juninatt"

som en satslogisk sentens.

Använd beteckningarna A: "det regnar", B: "det är natt", C: "det är juni".

Namn	poäng uppg.3

3) En binär, linjär kod $\mathcal{C}$ av längd $n = 5$ skall definieras av kontrollmatrisen (i boken: checkmatrisen) H med 3 rader.

a) (2p) Ange en möjlig matris H om $\mathcal{C}$ skall rätta ett fel och orden 11010 och 01101 båda skall vara kodord i $\mathcal{C}$.

b) (1p) Om man med H från a) tar emot ordet **10101** och högst ett fel har uppstått, vilket var det sända kodordet?

Namn	poäng uppg.4

4) (3p) För ett (litet) RSA-system har man valt den offentliga parametern $n = 221 (= 13 \cdot 17)$.

a) (1p) Man tar den offentliga krypteringsexponenten e till det minsta möjliga värde som är ≥ 20. Vad blir e?

b) (2p) Vad blir motsvarande hemliga avkrypteringsexponent d?

Namn	poäng uppg.5

5) (3p) Uttryck den booleska funktionen $f(x, y, z, w) =$

$xyzw + \bar{x}yz\bar{w} + \bar{x}\bar{y}\bar{z}w + x\bar{y}\bar{z}w + \bar{x}y\bar{z}\bar{w} + xyz\bar{w} + \bar{x}\bar{y}zw + xy\bar{z}\bar{w} + x\bar{y}zw + xy\bar{z}w$

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.