KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	kodnr

Kontrollskrivning 4A, 13 maj 2015, 10.15–11.15,
i SF1610 Diskret matematik för CINTE, CMETE mfl.

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)	Koden $C = \{0000000, 1111111\}$ är 3-felsrättande.		
b)	Ett RSA-krypto kan ha de publika nycklarna $n = 143$ och $e = 64$.		
c)	I ett RSA-krypto med nycklarna n, e, m och d kan $e = d$.		
d)	Det finns precis 32 stycken Booleska funktioner i de fem variablerna x, y, z, w och u.		
e)	Till varje element $x \neq 0$ i en Boolesk algebra $\mathcal{B}$, sådan att $\lvert\mathcal{B}\rvert \geq 4$, finns minst två olika element y sådana att $x + y = 1$.		
f)	Till varje positivt heltal n finns minst en 1-felsrättande kod med precis n stycken ord.		

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Ett RSA krypto har $n = 119$. Vilka av heltalen i mängden $\{76, 77, 78, 79, 80\}$ kan väljas till parametern e.

b) (1p) Den 1-felsrättande koden C har kontrollmatrisen

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

Du tar emot ordet 0001100. Rätta ordet.

c) (1p) Ge den disjunktiva normalformen (d.n.f.) för den Booleska funktionen $f(x, y, z) = x\bar{y} + \bar{y}z$.

Namn	poäng uppg.3

3) (3p) Ett RSA-krypto har de publika parametrarna $n = 77$ och $e = 43$. Dekryptera meddelandet 2, dvs, bestäm $D(2)$.
OBS. En komplett lösning med fullständiga motiveringar skall ges.

Namn	poäng uppg.4

4) (3p) Bestäm kontrollmatrisen till en 1-felsrättande linjär kod C av längd 12 med 256 ord och som är sådan att ordet 111100000000 ligger på avstånd minst 2 från varje ord i koden C. (**Obs** delpoäng ges för svar som inte uppfyller alla av specifikationerna ovan.)

OBS. En komplett lösning med fullständiga motiveringar skall ges.

Namn	poäng uppg.5

5) (3p) Låt f vara den Booleska funktionen $f(x,y,z) = x\bar{y} + \bar{x}\bar{y}z$. Bestäm alla Boolesk funktioner g i de tre Booleska variablerna x, y och z sådana att

$$fg = 0 \qquad \text{och} \qquad f + g = 1.$$

OBS. En komplett lösning med fullständiga motiveringar skall ges.