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, 5 oktober 2010, 15.45–16.45, 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)	I varje RSA-krypto med parametrarna n, e och d gäller det att $ed \equiv 1 \pmod{n-1}$.		
b)	I varje Boolesk algebra är $\overline{(x+y)} = xy$.		
c)	Minimiavståndet i en 1-felsrättande kod är 2.		
d)	Ett RSA-krypto kan ha $n = 60$.		
e)	En kontrollmatris till en 1-felsrättande kod kan ha 3 rader och 8 kolonner.		
f)	I varje Boolesk algebra gäller att om $a + b = 0$ så är $a = 0$ och $b = 0$.		

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Ett RSA-krypto har $n = 33$ och $e = 7$. Ange $D(2)$, dvs det tal man får när man dekrypterar talet 2.

b) (1p) Låt den Booleska funktionen $f(x, y, z)$ i de tre variablerna x, y och z definieras genom

$$f(x, y, z) = xy\bar{z} + \bar{x}(y + z) + \overline{(\bar{y} + z)} \, .$$

Bestäm $f(0, 1, 0)$.

c) (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 1101010.

Namn	poäng uppg.3

3) (3p) Bestäm en minimal disjunktiv form till den Booleska funktionen

$$f(x, y, z) = xyz + \bar{x}yz + \bar{x}y\bar{z} + \bar{x}\bar{y}\bar{z} + x\bar{y}\bar{z} \ .$$

Namn	poäng uppg.4

4) (3p) Bestäm ett RSA-krypto, dvs bestäm de tre parametrarna n, e och d, med kravet på parametrarna n och e att $45 < n < 55$ och $2 < e < 9$.

Namn	poäng uppg.5

5) (3p) Bestäm kontrollmatrisen till en 1-felsrättande kod C vars ord har längden 9 och antalet kodord är 64, dvs $|C| = 64$, och som rättar ordet 101111001 till ordet $101011001 \in C$.