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, onsdagen den 8 oktober 2008, 09.15–10.15, i SF1610 Diskret matematik för IT2.

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 ett RSA-krypto med $n = p \cdot q$ måste p och q vara olika primtal.		
b)	Koden $C = \{00000, 11111\}$ är 2-felsrättande.		
c)	I varje Boolesk algebra gäller det alltid att $ab + c = (a + c)(b + c)$		
d)	Det Booleska uttrycket $x + \bar{y}z$ i de tre variablerna x, y och z, är skrivet på minimal disjunktiv form.		
e)	I ett RSA-krypto med $n = p \cdot q$ kan e aldrig vara lika med $p - 1$.		
f)	Om en kontrollmatris H har 7 rader och 3 kolonner kan samtliga ord av längd 7 rättas.		

poäng uppg.1

Namn	poäng uppg.2

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

$$\begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Rätta ordet 111101.

b) (1p) Ett RSA-krypto har $n = 35$. Varför kan man inte ha nyckeln $e = 16$ i kryptot?

c) (1p) Förenkla uttrycket $x + xy$.

Namn	poäng uppg.3

3) (3p) I ett RSA-krypto är $n = 33$ och $e = 7$. Dekryptera meddelandet 2, dvs bestäm $D(2)$. (OBS värdet av $D(2)$ skall beräknas)

Namn	poäng uppg.4

4) (3p) (3p) Bestäm en kontrollmatris H till en 1-felsrättande kod C med ord av längd 10 och som är sådan att C har så många ord som möjligt.

Namn	poäng uppg.5

5) Skriv den Booleska funktionen $\overline{xyzw + \bar{x}y\bar{z}w}$ på en minimal disjunktiv form.