

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

**Kontrollskrivning 4A, 2 oktober 2012, 08.45–09.45,
i SF1610 Diskret matematik för CINTE och CMETE.**

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), $n = 1, \dots, 5$.

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) Det finns totalt 256 Booleska funktioner i de tre variablerna x , y och z .		
b) I ett RSA-krypto med parametrarna n , e , m och d kan n vara lika med 99.		
c) I ett RSA-krypto med parametrarna n , e , m och d kan n vara mindre än m .		
d) För en 5-felrättande kod gäller att minsta avstånd mellan kodorden är lika med 11.		
e) Antalet ord i en linjär 1-felrättande kod är alltid lika med 2^n för något heltal n .		
f) Om för elementen x och y i en Boolesk algebra gäller att $x + \bar{x}y = 1$ så måste $x = y$.		

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Den 1-felsrättande koden C defineras av kontrollmatrisen

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

Ordet 0011111 tillhör inte koden. Rätta ordet, dvs ange ett ord i koden C som har avståndet 1 till ordet 0011111.

b) (1p) Ett RSA-krypto har den offentliga nyckeln $n = 35$. Vilka av talen i mängden $\{5, 7, 9\}$ kan användas till den krypterande nyckeln e .

c) (1p) Ange en disjunktiv normalform för den Booleska funktionen

$$f(x, y, z, w) = (xw + x\bar{y}\bar{z})z + xyw.$$

Namn	poäng uppg.3

3) (3p) Ett RSA-krypto har parametrarna $n = 69$ och $e = 5$. Dekryptera meddelandet $b = 2$, dvs bestäm $D(2)$.

Namn	poäng uppg.4

4) (3p) Betrakta den Booleska funktionen

$$f(x, y, z) = xy + xz$$

i de tre variablerna x , y och z . Bestäm tre olika Booleska funktioner $g_1(x, y, z)$, $g_2(x, y, z)$ och $g_3(x, y, z)$ sådana att både $f(x, y, z) + g_1(x, y, z)$, $f(x, y, z) + g_2(x, y, z)$ och $f(x, y, z) + g_3(x, y, z)$ antar värdet 1 för varje värde på variablerna x , y och z . (Du får beskriva de Booleska funktionerna du svarar med på valfritt sätt.)

Namn	poäng uppg.5

5) (3p) Det finns ingen linjär 1-fels-rättande kod C sådan att

$$\{1111111111, 1111000000, 00000111100\} \subseteq C$$

Förklara varför!