

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

**Lösning till kontrollskrivning 4B, 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 .	x	
b) I ett RSA-krypto med parametrarna n , e , m och d kan n vara mindre än m .		x
c) För en 5-felrättande kod gäller att minsta avstånd mellan kodorden är lika med 11.	x	
d) I ett RSA-krypto med parametrarna n , e , m och d kan n vara lika med 99.		x
e) Om för elementen x och y i en Boolesk algebra gäller att $x + \bar{x}y = 1$ så måste $x = y$.		x
f) Antalet ord i en linjär 1-felrättande kod är alltid lika med 2^n för något heltal n .	x	

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 0111110 tillhör inte koden. Rätta ordet, dvs ange ett ord i koden C som har avståndet 1 till ordet 0111110.

SVAR: 0111010

b) (1p) Ett RSA-krypto har den offentliga nyckeln $n = 35$. Vilka av talen i mängden $\{6, 9, 11\}$ kan användas till den krypterande nyckeln e .

SVAR: 11

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

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

SVAR: $x\bar{y}\bar{z}w + xy\bar{z}w + xyz\bar{w} + xy\bar{z}\bar{w}$.

Namn	poäng uppg.3

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

Lösning: Då $n = 3 \cdot 23$ får vi att $m = 2 \cdot 22 = 44$. Med $e = 5$ blir $d = 9$ eftersom $5 \cdot 9 \equiv 1 \pmod{44}$. Vi dekrypterar nu meddelandet 2:

$$D(2) = 2^9 \pmod{69} = 512 \pmod{69} = 7 \cdot 69 + 29 \pmod{69} = 29.$$

SVAR: $D(2) = 29$.

Namn	poäng uppg.4

4) (3p) Betrakta den Booleska funktionen

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

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.)

$$x\bar{y}\bar{z}w + xy\bar{z}w + xyz\bar{w} + xy\bar{z}\bar{w}.$$

Lösning Vi skriver först f på en disjunktiv normalform

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

För varje Boolesk funktion g med en disjunktiv normalform

$$g(x, y, z) = \delta_1 xyz + \delta_2 \bar{x}yz + \delta_3 xy\bar{z} + x\bar{y}z + \bar{x}\bar{y}z + x\bar{y}\bar{z} + \bar{x}\bar{y}\bar{z} + \bar{x}y\bar{z}$$

gäller att $f(x, y, z) + g(x, y, z) = 1$, varvid vi kan välja δ_i , för $i = 1, 2$ och 3 , till ett eller noll valfritt, eftersom det då gäller att

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

SVAR: Till exempel

$$g_1(x, y, z) = x\bar{y}z + \bar{x}\bar{y}z + x\bar{y}\bar{z} + \bar{x}\bar{y}\bar{z} + \bar{x}y\bar{z},$$

$$g_2(x, y, z) = xyz + x\bar{y}z + \bar{x}\bar{y}z + x\bar{y}\bar{z} + \bar{x}\bar{y}\bar{z} + \bar{x}y\bar{z},$$

eller

$$g_3(x, y, z) = \bar{x}yz + x\bar{y}z + \bar{x}\bar{y}z + x\bar{y}\bar{z} + \bar{x}\bar{y}\bar{z} + \bar{x}y\bar{z}.$$

Namn	poäng uppg.5

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

$$\{1111111111, 0000111111, 0111000000\} \subseteq C$$

Förklara varför!

Lösning: En kod C är linjär om

$$\bar{c}, \bar{c}' \in C \quad \implies \quad \bar{c} - \bar{c}' \in C.$$

Den givna koden C innehåller då orden (OBS subtraktion är addition i ringen Z_2)

$$1111111111 + 1111111111 = 0000000000,$$

och

$$(1111111111 + 0000111111) + 01110000000000 = 100000000000.$$

Avståndet mellan orden 0000000000 och 10000000000 är 1, så kodens minavstånd är inte tre utan ett.

En kod C är e -felsrättande om kodens minavstånd är $2e + 1$.