

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

**Kontrollskrivning 4A, den 8 oktber 2013, kl 11.00-12.00
i SF1610 Diskret matematik för CİNTE 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) I ett RSA-krypto med parametrarna n , e , m och d är alltid $n > m$.		
b) I varje Boolesk algebra gäller att $(x + xy)(\bar{x} + \bar{xy}) = 0$.		
c) Det finns total 16 olika Booleska funktioner i de fyra variablerna x , y , z och w .		
d) Ett RSA-krypto kan ha de offentliga nycklarna $n = 99$ och $e = 31$.		
e) En kod är e -felsrättande om minsta avståndet mellan ord i koden är $2e - 1$.		
f) Om \bar{c} och \bar{d} är ord i en 1-felsrättande kod C definierad av en kontrollmatrix \mathbf{H} så är också $\bar{c} + \bar{d}$ ett ord i C .		

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Om ett RSA-krypto har den offentliga nyckeln $n = 51$ vilka möjligheter finns då för den krypterande nyckeln e om vi dessutom kräver att $12 < e < 18$.
(Svara bara.)

b) (1p) Betrakta den Booleska funktionen

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

Bestäm funktionens värde i punkten $(x, y, z, w) = (0, 0, 1, 1)$.
(Svara bara.)

c) (1p) Fyll i matrisen \mathbf{H} nedan så att \mathbf{H} blir kontrollmatrisen (parity-check matrix) till en 1-felsrättande kod.

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

Namn	poäng uppg.3

3) (3p) Ett RSA krypto har de offentliga nycklarna $n = 33$ och $e = 9$.
Dekryptera meddelandet 2.

OBS. Lösningen skall motiveras och kalkyler redovisas.

Namn	poäng uppg.4

4) (3p) Den 1-felsrättande koden C har kontrollmatrisen

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

a) Ordet 11111111 tillhör inte C men går att rätta till ett ord \bar{c} i C . Bestäm detta ord \bar{c} .

b) Bestäm antalet ord i C .

c) Bestäm minst två av orden i C .

OBS. Lösningen skall motiveras.

Namn	poäng uppg.5

5) (3p) Bestäm antalet Booleska funktioner $g(x, y, z)$ sådana att

$$(x + \overline{yz})xyg(x, y, z) = 0,$$

för alla värden på x, y och z .

OBS. Lösningen skall motiveras.