

KTH Matematik
Olof Heden

Σ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

**Lösning till 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 $n > m$.	x	
b) I varje Boolesk algebra gäller att $(x + xy)(\bar{x} + \bar{xy}) = 0$.		x
c) Det finns total 16 olika Booleska funktioner i de fyra variablerna x, y, z och w .		x
d) Ett RSA-krypto kan ha de offentliga nycklarna $n = 99$ och $e = 31$.		x
e) En kod är e -felsrättande om minsta avståndet mellan ord i koden är $2e - 1$.		x
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 .	x	

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.)

SVAR: $e \in \{13, 15, 17\}$

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.)

SVAR: 1

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

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

SVAR:

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

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.

Lösning: Då $n = 3 \cdot 11$ så $m = (3 - 1)(11 - 1) = 20$. Den dekrypterande nyckeln d fås ur villkoret $de \equiv 1 \pmod{m}$. Eftersom vi vet att $9 \cdot 9 = 81$ finner vi att $d = 9$. Vi dekrypterar nu

$$2^d = 2^9 \equiv_{33} 2^5 2^4 \equiv_{33} (-1)2^4 \equiv_{33} -16 \equiv_{33} 17$$

SVAR: 17.

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.

Lösning: Då

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

vilket är den fjärde kolonnen i matrisen \mathbf{H} så uppstod ett fel i position fyra i ordet. Det givna ordet rättas då till ordet 11101111.

Antalet ord i koden ges av uttrycket 2^{n-r} där n är antalet kolonner och r är antalet rader. Således, antalet ord i koden är $2^{8-4} = 16$.

Nollordet 00000000 är ett ord i koden, eftersom \mathbf{H} multiplicerar detta ord till nollkolonnen. Ett annat har vi redan, nämligen kodordet 11101111 som vi fann tidigare.

Namn	poäng uppg.5

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

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

för alla värden på x, y och z .

OBS. Lösningen skall motiveras.

Lösning: Vi förenklar först det Booleska uttrycket ovan:

$$\begin{aligned} 0 &= (x + \bar{y}\bar{z})xyg(x, y, z) = (x + \bar{y} + \bar{z})xyg(x, y, z) = \\ &= (xy + xy\bar{z})g(x, y, z) = xyg(x, y, z). \end{aligned}$$

I de punkter där $xy = 1$ måste $g(x, y, z)$ vara lika med noll, i övriga punkter kan funktionsvärdet $g(x, y, z)$ väljas godtyckligt. Men $xy = 1$ uppfylls endast av två punkter:

$$(x, y, z) \in Z = \{(1, 1, 0), (1, 1, 1)\}.$$

Alltså, då det finns totalt 8 olika punkter (x, y, z)

SVAR: $2^{8-|Z|} = 64$.