

**KTH Matematik**  
Olof Heden

$\Sigma$ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

**Kontrollskrivning 4A, den 7 maj 2014, kl 10.00-11.00  
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 total 32 stycken Booleska funktioner i de fem variablerna $x, y, z, w$ och $u$ .		
b) I varje Boolesk algebra gäller att $(x + xy) + \bar{x} = 1$ .		
c) I ett RSA-krypto med parametrarna $n, e, m$ och $d$ kan $m$ vara lika med 28.		
d) Ett RSA-krypto med $n = 123$ kan ha den dekrypterande nyckeln $d = 45$ .		
e) Orden 11110101 och 00110101 kan båda tillhöra samma 1-felsrättand kod.		
f) Det finns 1-felsrättande koder $C$ bestående av 16 ord, samtliga av längd 15.		

poäng uppg.1

Namn	poäng uppg.2

**2a)** (1p) Om ett RSA-krypto har den offentliga nyckeln  $e = 9$  vilka möjligheter finns då för parametern  $n$  om vi kräver att  $33 \leq n \leq 40$ .

(Svara bara.)

**b)** (1p) Skriv nedanstående Booleska funktion  $f(x, y, z)$

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

på disjunktiv normalform.

(Svara bara.)

**c)** (1p) Förklara varför matrisen  $\mathbf{H}$  nedan inte kan användas som kontrollmatris (parity-check matris) till en 1-felsrättande kod.

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

Namn	poäng uppg.3

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

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

a) Ordet 110100000 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 ett ord som koden inte klarar av att rätta.

**OBS. Lösningen skall motiveras.**

Namn	poäng uppg.4

4) (3p) Ett RSA krypto har de offentliga nycklarna  $n = 33$  och  $e = 3$ .  
Dekryptera meddelandet 2.

**OBS. Lösningen skall motiveras och kalkyler redovisas.**

Namn	poäng uppg.5

5) (3p) Bestäm antalet Booleska funktioner  $g$  i fyra variablerna  $x$ ,  $y$ ,  $z$  och  $w$ , dvs  $g = g(x, y, z, w)$ , som satisfierar ekvationssystemet

$$(x + yz)\bar{w}g(x, y, z, w) = 0.$$

**OBS. Lösningen skall motiveras.**