

KTH Matematik
Olof Heden

| | | |
|------------|-----|-------|
| Σ p | G/U | bonus |
| | | |

| | | | |
|-----------|---------|-----|---------|
| Efternamn | förnamn | pnr | årskurs |
| | | | |

**Lösning till kontrollskrivning 4B, 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 . | | x |
| b) I ett RSA-krypto med parametrarna n, e, m och d kan m vara lika med 28. | x | |
| c) I varje Boolesk algebra gäller att $(x + xy) + \bar{x} = 1$. | x | |
| d) Orden 11110101 och 00110101 kan båda tillhöra samma 1-felsrättand kod. | | x |
| e) Ett RSA-krypto med $n = 123$ kan ha den dekrypterande nyckeln $d = 39$. | x | |
| f) Det finns 1-felsrättande koder C bestående av 16 ord, samtliga av längd 15. | x | |

| |
|-----------------|
| 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.)

SVAR: $n \in \{33, 34\}$

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

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

på disjunktiv normalform.

(Svara bara.)

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

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

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

SVAR: Två av matrisens kolonner är lika.

| | |
|------|-----------------|
| Namn | poäng uppg.3 |
| | |

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

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

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.

Lösning. Antal ord är $2^{\text{antal kolonner} - \text{antal rader}} = 2^{9-4} = 32$. För att rätta det givna ordet multiplicerar vi ordet med matrisen \mathbf{H} . Vi får

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

vilket är kolonn nummer fem. Vi rättar ordet i den positionen till ordet 110110000. Om vi multiplicerar matrisen \mathbf{H} med ordet 111000000 får vi

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

en kolonn som inte finns i matrisen \mathbf{H} . Därför kan ordet 111000000 inte rättas.

| 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.

Lösning. Då $n = 3 \cdot 11$ så $m = 2 \cdot 10 = 20$. Söker d med egenskapen $e \cdot d \equiv 1 \pmod{m}$, vilket ger $d = 7$ eftersom $3 \cdot 7 = 21$. Vi dekrypterar nu meddelandet 2 till $D(2) = 2^7 \pmod{33}$. Då

$$2^7 \equiv_{33} 128 \equiv_{33} 29,$$

så

SVAR: 29.

| | |
|------|-----------------|
| 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

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

OBS. Lösningen skall motiveras.

Lösning. Funktionen g måste ha värdet 0 i de punkter där $(xw + y)\bar{z} = 1$, i övriga punkter kan g tilldelas ett godtyckligt värde. Vi finner att

$$\begin{aligned} (xw + y)\bar{z} &= x(y + \bar{y})\bar{z}w + (x + \bar{x})y\bar{z}(w + \bar{w}) \\ &= xy\bar{z}w + x\bar{y}\bar{z}w + \bar{x}y\bar{z}w + xy\bar{z}\bar{w} + \bar{x}y\bar{z}\bar{w} \end{aligned}$$

Eftersom den disjunktiva normalformen av $(xw + y)\bar{z}$, vilket är "koefficienten" framför g , består av 5 fundamentala konjunktioner, så är detta uttryck 1 i precis 5 punkter. I resterande 11 punkter i g 's definitionsmängd kan alltså g 's funktionsvärde väljas godtyckligt, antagligen 0 eller 1. Vi får

SVAR: $2^{11} = 2048$.