KTH Matematik
Examinator: Maurice Duits

Σ p	G/U	bonus

Efternamn	förnamn	pnr	programkod

Kontrollskrivning 4A till Diskret Matematik SF1610, för CINTE, vt2016

Inga hjälpmedel tillåtna.
Minst 8 poäng ger godkänt.
Godkänd KS nr n medför godkänd uppgift n vid tentor till (men inte med) nästa ordinarie tenta (högst ett år), $n = 1, \ldots, 5$.
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 en linjär binär kod med 6 kodord.		X
b)	Ett RSA-krypto med offentlig parameter n och krypteringsnyckel e kan ha $n = 105$.		X
c)	I Boolesk algebra håller det alltid att $(x + y)\bar{x}\bar{y} = 0$.	X	
d)	Det finns ett RSA-krypto med krypteringsnyckel $e = 11$.	X	
e)	Orden `10101010` och `11111010` kan tillhöra samma 1-felsrättande kod.		X
f)	Det finns 16 olika Booleska funktioner i de fyra variablarna x, y, z, w.		X

poäng uppg.1

Namn	poäng uppg.2

2a) (1p) Ett RSA-krypto har krypteringsnyckel $e = 11$. Vilket/vilka av talen i mängden $\{64, 65, 66, 67, 68\}$ kan den offentliga parametern n vara?
(Det räcker att ange rätt svar.)

Svar: 65

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

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

(Det räcker att ange rätt svar.)

Svar:

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

c) (1p) Bestäm värdet på den Booleska funktionen

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

i punkten $(x, y, z, w) = (1, 0, 1, 0)$.
(Det räcker att ange rätt svar.)

Svar: 1

Namn	poäng uppg.3

3) (3p) Ett RSA-krypto har de offentliga parametrarna $n = 33$ och $e = 9$, där e är krypteringsnyckeln. Ett meddelande a krypterades till talet 2 enligt kryptot. Dekryptera meddelandet, d.v.s. bestäm a.
OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: Vi börjar med att primtalsfaktorisera n för att på fram primtalen p, q. Vi har $n = 3 \cdot 11$, så vi låter $p = 3$ och $q = 11$. Då får vi $m = (p-1)(q-1) = 20$. För att dekyptera ett medelande behöver vi hitta den multiplikativa inversen d till e i $\mathbb{Z}_m$, dvs ett tal d sådant att $9d \equiv 1 \pmod{20}$. Eftersom $9 \cdot 9 = 81 \equiv 1 \pmod{20}$ tar vi $d = 9$.

Det ursprungliga meddelandet a fås då från det krypterade meddelandet 2 via $a = 2^d \pmod{n}$, dvs

$$a = 2^9 \bmod 33 = 2^5 \cdot 2^4 \bmod 33 = 32 \cdot 16 \bmod 33 = -16 \bmod 33 = 17.$$

Svar: $a = 17$.

Namn	poäng uppg.4

4) (3p) Matrisen $\mathbf{H}$ nedan är kontrollmatrisen till en linjär 1-felsrättande kod C.

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

a) Hur många kodord finns det i koden?

b) En mottagare tar emot orden `011111` och `011100`. Rätta dessa ord till kodord i C enligt närmaste-granne-principen.

OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning:

a) Det finns 2^{n-r} kodord i en kod som ges av en kontrollmatris med n kolonner och rang r. Matrisen $\mathbf{H}$ har $n = 6$ och $r = 3$ (kolonner 1, 2 och 4 är uppenbarligen linjärt oberoende), alltså har koden $2^3 = 8$ kodord.

b)

$$\mathbf{H} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

vilket är 3:e kolonnen i $\mathbf{H}$. Alltså ändrar vi på 3:e biten i meddelandet; enligt känd sats rättar detta ordet till det närmast-liggande kodordet.

För det andra ordet har vi

$$\mathbf{H} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Alltså ligger ordet redan i koden.

Svar: `010111` och `011100`.

Namn	poäng uppg.5

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

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

för alla värden på x, y, z.

OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: Vi börjar med att förenkla: eftersom $(y + x\bar{z})yz = yz$ så vill vi hitta antelet f med

$$yzf(x, y, z) = 0.$$

Vänsterledet är automatisk noll om $y = 0$ eller $z = 0$, så då finns det inga krav på f. Men om $y = z = 1$ då måste $f(x, y, z) = 0$. Alltså är det ursprungliga kravet på f ekvivalent med $f(x, 1, 1) = 0$ för alla x, dvs att

$$f(0, 1, 1) = 0 = f(1, 1, 1).$$

För alla andra inputs, varav det finns $2^3 - 2 = 6$ stycken, kan f ta vilket som helst av 2 värden (antingen 0 eller 1). Därför finns det, enligt multiplikationsprincipen, 2^6 sådana funktioner.

Svar: Det finns 2^6 sådana funktioner f.