KTH Matematik
Examinator: Maurice Duits
Kursansvarig: Olof Sisask

Σ p	G/U	bonus

Efternamn	förnamn	pnr	programkod

Kontrollskrivning 4A till Diskret Matematik SF1610, för CINTE, vt2017

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)	I Boolesk algebra gäller det att $p \cdot (\bar{p} + \bar{p} \cdot (p+1)) = 0$.	X	
b)	Det finns en linjär kod C av längd 7, med 8 kodord, som har en kontrollmatris med 3 rader.		X
c)	Ett RSA-krypto kan ha offentlig modulo $n = 77$ och offentlig krypteringsnyckel $e = 9$.		X
d)	Om C är en linjär kod och x, y är kodord i C, då är $x - y$ också ett kodord i C.	X	
e)	Det finns 2^n olika Booleska funktioner i n variabler.		X
f)	Ett RSA-krypto med offentlig modulo $n = 65$ kan ha krypteringsnyckel $e = 5$ och avkrypteringsnyckel $d = 29$.	X	

poäng uppg.1

	poäng
Namn	uppg.2

2a) (1p) Låt den Booleska funktionen $f(x, y, z)$ i tre variabler x, y och z definieras genom

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

Bestäm $f(0, 1, 1)$.
(Det räcker att ange rätt svar.)

Svar: 1.

b) (1p) En kod C är 1-felsrättande med kontrollmatrisen

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

Rätta ordet `0110010`.
(Det räcker att ange rätt svar.)

Svar: `0110011`.

c) (1p) Ett RSA-krypto har $n = 33$. Ange samtliga möjliga värden på den offentliga krypteringsnyckeln e som vi kan välja i intervallet $1 < e < 12$.
(Det räcker att ange rätt svar.)

Svar: 3, 7, 9, 11.

Namn	poäng uppg.3

3) (3p) Låt $B = \{0, 1\}$ vara en Boolesk algebra och låt $g : B^3 \to B$ vara den Booleska funktionen given av formeln

$$g(x, y, z) = \overline{y} + y \cdot z.$$

a) Bestäm hur många olika Booleska funktioner $f : B^3 \to B$ det finns sådana att

$$f(x, y, z) \cdot g(x, y, z) = (x + \overline{x}) \cdot \overline{y} \cdot z.$$

b) Skriv ned en möjlig sådan funktion f antingen i disjunktiv normalform eller konjunktiv normalform (ditt val).

OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: Eftersom $x + \overline{x} = 1$ har vi att högerledet kan förenklas:

$$(x + \overline{x}) \cdot \overline{y} \cdot z = \overline{y} \cdot z.$$

Nu använder vi oss av en sanningstabell för g och $\overline{y} \cdot z$ för att härleda de möjliga värdena på f:

x	y	z	$g(x, y, z)$	$\overline{y} \cdot z$	möjliga värden för $f(x, y, z)$
0	0	0	1	0	0
0	0	1	1	1	1
0	1	0	0	0	$0, 1$
0	1	1	1	0	0
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	0	0	$0, 1$
1	1	1	1	0	0

Enligt multiplikationsprincipen finns det $2 \cdot 2 = 4$ val för f: funktionsvärdet är bestämt för alla inputs (x, y, z) förutom $(0, 1, 0)$ och $(1, 1, 0)$, och för varje av dessa inputs har vi två möjligheter.

En möjlig sådan f är där vi väljer 0 för båda dessa inputs. Då är $f(x, y, z) = 1$ omm $(x, y, z) = (0, 1, 0)$ eller $(1, 1, 0)$. Dessa inputs kan selekteras i disjunktiv normalform på ett enkelt sätt:

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

Svar: 4 funktioner, varav en är $\overline{x}y\overline{z} + xy\overline{z}$.

Namn	poäng uppg.4

4) (3p)

a) För vilka värden på parametrarna x, $y \in \{0, 1\}$ blir matrisen $\mathbf{H}$ nedan en binär kontrollmatris till en linjär 1-felsrättande kod C?

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

b) För samtliga värden på parametrarna x, y som uppfyller ovan krav, bestäm hur många kodord det finns i koden.

c) En mottagare tar emot orden `101111` och `101100`. Rätta dessa ord till kodord i C enligt närmaste-granne-principen, för samtliga värden på parametrarna x, y som uppfyller kravet i (a).

OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning:

a) För att koden ska bli 1-felsrättande så får den inte innehålla någon kolonn med enbart `0`:or, eller några två kolonner som är lika. Därför måste vi ha

$$x = 1 \quad \text{och} \quad y = 1.$$

b) 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, t.ex., är linjärt oberoende); alltså har koden $2^3 = 8$ kodord.

c)

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

vilket är 1:a kolonnen i $\mathbf{H}$. Alltså ändrar vi på 1:a biten i meddelandet; enligt känd sats rättar detta ordet till det närmast-liggande kodordet, som blir `001111`.

För det andra ordet har vi

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

Alltså ligger ordet redan i koden.

Svar: `001111` resp. `101100`.

Namn	poäng uppg.5

5) (3p) Ett RSA-krypto har den offentliga modulon $n = 85$ och krypteringsnyckel $e = 13$. Finn avkrypteringsnyckeln d och använd denna för att avkryptera meddelandet $b = 3$.
OBS. En komplett lösning med fullständiga motiveringar skall ges.

Lösning: Vi kan skriva $n = 85$ som produkten $85 = 5 \cdot 17$ av primtalen $p = 5$ och $q = 17$. Därför är vår privata modulo $m = (p-1)(q-1) = 64$.

Eftersom
$$e \cdot 5 = 13 \cdot 5 = 65 \equiv 1 \pmod{m}$$
så ser vi att vår privata avkrypteringsnyckel är $d = 5$. Enligt beräkningen med Fermats lilla sats++ vet vi då att vi kan avkryptera meddelandet $b = 3$ genom att beräkna
$$3^5 = 9 \cdot 9 \cdot 3 = 81 \cdot 3 = 243 \equiv 73 \mod n,$$
eftersom $n = 85$. Alltså avkrypteras meddelandet $b = 3$ till meddelandet 73.

Svar: 73.