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

poäng uppg.1

Namn	poäng 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.)

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` till det närmaste kodordet i C.
(Det räcker att ange rätt svar.)

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.)

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.

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.

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.