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.		
b)	Ett RSA-krypto med offentlig parameter n och krypteringsnyckel e kan ha $n = 105$.		
c)	I Boolesk algebra håller det alltid att $(x + y)\bar{x}\bar{y} = 0$.		
d)	Det finns ett RSA-krypto med krypteringsnyckel $e = 11$.		
e)	Orden `10101010` och `11111010` kan tillhöra samma 1-felsrättande kod.		
f)	Det finns 16 olika Booleska funktioner i de fyra variablarna x, y, z, w.		

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.)

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.)

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.)

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.

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.

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.