

Kontrollskrivning 4 till Diskret Matematik SF1610, för CINTe1, TCOMK, vt 2021

Datum: 12 maj 2021

Lärare: Angélica Torres, amt@kth.se ; Armin Halilovic armin@kth.se

Examinator: Armin Halilovic,

Skrivtid: 10:15 -11:15 (+15 min för uppladdning. Uppladdningsmappen öppnas 10:45 och stängs 11:30)

Extra skrivtid (funka): 10:15 -11:45 (+15 min för uppladdning: Uppladdningsmappen (Extra tid) öppnas 10:45 och stängs 12:00)

Du använder papper och penna för att lösa nedanstående uppgifter. Du skannar eller tar bilder av dina lösningar. Dina lösningar (gärna PDF), **separat fil för varje uppgift**, laddar du upp på Canvas/uppgifter/KS4. (Komprimera INTE filer.)

För godkänt krävs 5 poäng av 9 möjliga poäng.

Till samtliga uppgifter krävs fullständiga lösningar. (Endast svar utan tillhörande lösning ger 0 poäng.)

Skriv namn och personnummer **på varje blad**.

Deklarera att du själv har gjort KS: Skriv på första inlämnade blad ” *Jag själv har gjort denna KS*” och signera.

Parametrarna p och q i nedanstående uppgifter är de sista två siffrorna i ditt personnummer. (T ex: Om ditt personnummer är 751332 2248 så är $p=4$ och $q=8$.)

Börja med att byta ut p och q med siffror från ditt personnummer och lös sedan uppgifterna.

1. (3p)

Låt $A = (p \bmod 2)$

a) Bestäm alla kodord som definieras av checkmatrisen

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

b) Bestäm minimala distansen mellan två kodord i ovanstående koden.

2. (3p)

Vi konstruerar en RSA krypteringssystem med hjälp av primtalen 5 och 11. Vi har $n = 5 \cdot 11 = 55$ och $m = (5-1) \cdot (11-1) = 40$.

Du ska välja en lämplig krypteringsnyckel e i intervallet $10 < e < 18$ och för detta e bestämma dekrypteringsnyckeln d .

3) (3p)

Låt $A = (p \bmod 2)$ och $B = (q \bmod 2)$.

En Boolesk funktion $f(x,y,z)$ definieras med hjälp av följande tabell:

x	y	z	$f(x,y,z)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	A
1	1	1	B

a) Skriv funktionen på disjunktiv normalform.

b) Skriv funktionen på konjunktiv normalform.

Lycka till.