

Skrivningskod:   
Glöm den inte!

Om du vill:   
Lägg till tre bokstäver.

**KTH Matematik**  
Olof Heden

$\Sigma$ p	G/U	bonus

Efternamn	förnamn	pnr	årskurs

### Övningskontrollskrivning 4 till kursen SF1610 Diskret matematik.

Inga hjälpmedel tillåtna.

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!)

	<b>sant</b>	<b>falskt</b>
a) Ett RSA-krypto kan ha parametrarna $n = 46$ och $e = 2$ .		
b) Ett RSA-krypto kan ha $d = 5$ och $e = 5$ .		
c) Om kolonner i matrisen $H$ , med ettor och nollor, är olika så är $H$ en kontrollmatris till en 1-felsrättande kod.		
d) Om $C$ är en 1-felsrättande kod av längd 7 med 8 ord så har $C$ en kontrollmatris $H$ med 3 rader.		
e) Det finns precis 8 booleska funktioner i de tre variablerna $x, y$ och $z$ .		
f) I en boolesk algebra $B$ gäller alltid att $x + xy = x$ för alla $x, y \in B$ .		

poäng uppg.1

Namn	poäng uppg.2

**2a)** (1p) Du använder en 1-felsrättande kod med kontrollmatrisen

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

Du tar emot meddelandet 111111. Om ordet går att rätta skall du rätta det. Om det inte går att rätta skall du skriva att ordet inte går att rätta.

**b)** (1p) Betrakta nedanstående booleska funktion i de tre variablerna  $x$ ,  $y$  och  $z$ :

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

Ange de värden på  $x$ ,  $y$  och  $z$  som är sådana att  $f(x, y, z) = 0$ .

**c)** (1p) Du vill ha ett RSA-krypto med parametern  $n = 65$ . Ange ett möjligt värde på parametern  $e$ .

Namn	poäng uppg.3

**3)** (3p) Skriv följande booleska funktion, i de tre variablerna  $x, y, z$  och  $w$ , på en disjunktiv normalform:

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

Namn	poäng uppg.4

4) (3p) Ett RSA-krypto har de offentliga nycklarna  $n = 39$  och  $e = 11$ . Bestäm parametern  $d$  och ange hur meddelande 2 kan dekrypteras, dvs ange hur  $D(2)$  beräknas.

(Du behöver alltså inte beräkna  $D(2)$  för att få full poäng på denna uppgift men du skall berätta hur man går till väga.)

Namn	poäng uppg.5

5) (3p) Bestäm en 1-felsrättande kod  $C$  av längd 7 och som innehåller 10 ord och som är sådan att ordet 1011000 tillhör koden  $C$ .