

## Övningsks 4.

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) Ett RSA-krypto kan ha parametrarna $n = 46$ och $e = 2$ .                                                              |      |        |
| b) Ett RSA-krypto kan ha $d = 5$ och $e = 5$ .                                                                            |      |        |
| c) Om kolonnerna i matrisen $H$ , med 1:or och 0:or, alla är olika så är $H$ kontrollmatris för en 1-felsrättande kod.    |      |        |
| d) Om $\mathcal{C}$ är en 1-felsrättande kod av längd 7 med 8 ord så har $\mathcal{C}$ 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 $x, y \in B$ .                                        |      |        |

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

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

och tar emot meddelandet 111111. Om ordet går att rätta, skall du rätta det. Om det inte går att rätta, skall du svara att ordet inte går att rätta.

**b)** (1p) Ange en minimal disjunktiv form för nedanstående booleska funktion i de tre variablerna  $x, y$  och  $z$ :

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

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

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

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

**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.)

**5)** (3p) Bestäm en kontrollmatris till en 1-felsrättande kod  $\mathcal{C}$  av längd 7 och som innehåller 16 ord och som är sådan att ordet 1011000 tillhör koden  $\mathcal{C}$ .