Matematiska Institutionen
KTH

Några övningar på felkorrigerande koder, RSA-kryptering och Boolesk algebra inför Ks4 i Diskret Matematik Mediavt07.

1. Betrakat ett RSA-krypto med $n = 51$ och $e = 5$. Kryptera meddelandet 3 och dekryptera meddelandet 5.
2. Betrakta ett RSA-krypto med $n = 57$. Du får välja parametern e själv. Skriv upp de möjliga val av parametern e du har.
3. Visa med hjälp av ett lämpligt Fermattest att talet 18 inte är ett primtal.
4. Låt C vara en 1-felsrättande kod med kontrollmatrisen

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

   a) Bestäm antalet ord i koden C.

   b) Bestäm minst två olika ord i C.

   c) Ordet 11111111 ligger på avståndet ett från precis ett ord i C. Vilket.

   d) Bestäm minst ett ord av längd åtta som inte tillhör C och som inte ligger på avståndet ett från något kodord

   e) Bestäm antalet binära ord av längd åtta som varken tillhör C eller ligger på avståndet ett från något ord i C.

5. Bestäm en minimal disjunktiv form för uttrycket

$$x\bar{y} + xyz + \bar{x}\bar{y}\bar{z} + \bar{x}yz\bar{w}.$$

6. Bestäm en minimal disjunktiv form för uttrycket

$$xyz\bar{w} + x\bar{y}z\bar{w} + x\bar{y}\bar{z}\bar{w} + x\bar{y}\bar{z}w + \bar{x}\bar{y}zw + \bar{x}\bar{y}z\bar{w} + \bar{x}\bar{y}\bar{z}\bar{w} + \bar{x}y\bar{z}\bar{w}.$$

7. Bestäm en minimal disjunktiv form för uttrycket

$$xyz\bar{w} + x\bar{y}z\bar{w} + \bar{x}\bar{y}z\bar{w} + \bar{x}yz\bar{w} + x\bar{y}\bar{z}\bar{w} + \bar{x}yzw + \bar{x}y\bar{z}w.$$

8. Bestäm en minimal disjunktiv form för uttrycket

$$xyzw + xy\bar{z}w + x\bar{y}z\bar{w} + x\bar{y}\bar{z}\bar{w} + \bar{x}\bar{y}\bar{z}\bar{w} + \bar{x}yzw + \bar{x}y\bar{z}w + \bar{x}y\bar{z}\bar{w} + \bar{x}yz\bar{w}.$$

9. Bestäm en minimal disjunktiva form för nedanstående uttryck.
   (a) $xz + x\bar{z} + \bar{x}\bar{z}$.
   (b) $\bar{x}y + \bar{x}\bar{y}\bar{w} + \bar{y}w$.
   (c) $z + x\bar{y}z + \bar{x}yz + \bar{x}\bar{y}z$.
   (d) $\bar{x}yw + yz\bar{w} + \bar{x}\bar{y}z$.