Matematiska Institutionen
KTH

Lösningar resp svar till några övningar på felkorrigerande koder, RSA-kryptering och Boolesk algebra inför Ks4 för media vt07.

1. Betrakat ett RSA-krypto med $n = 51$ och $e = 5$. Kryptera meddelandet 3 och dekryptera meddelandet 5.

   Lösn. Allmänt gäller att det krypterade meddelandet blir $E(a) = a^e \pmod{n}$. Vi får alltså

   $$E(3) \equiv_{51} 3^5 \equiv_{51} 3^4 \cdot 3 \equiv_{51} 30 \cdot 3 \equiv_{51} 90 \equiv_{51} 29.$$

   Dekrypteringsnyckeln är $D(b) = b^d \pmod{n}$ där, om $n = pq$ så $m = (p-1)(q-1)$ och $e \cdot d \equiv 1 \pmod{m}$. Vi får $p = 3$ och $q = 17$ så $m = 2 \cdot 16 = 32$. För att finna d använder vi nu Euklides algoritm i sökandet efter $sgd(5, 32)$:

   $$\begin{array}{l} 32 = 6 \cdot 5 + 2 \\ 5 = 2 \cdot 2 + 1 \end{array} \quad \text{varur} \quad \left[\begin{array}{l} 1 = 5 - 2 \cdot 2 = 5 - 2(32 - 6 \cdot 5) = \\ 13 \cdot 5 - 2 \cdot 32. \end{array} \right] \quad \text{dvs} \quad 1 \equiv_{32} 13 \cdot 5.$$

   Sålunda $d = 13$ och $D(5) = 5^13 \equiv_{51} 5^8 \cdot 5^4 \cdot 5$. Vi finner att

   $$5^4 \equiv_{51} 5^2 \cdot 5^2 \equiv_{51} 625 \equiv_{51} 12 \cdot 51 + 13 \equiv_{51} 13$$

   och

   $$5^8 \equiv_{51} 5^4 \cdot 5^4 \equiv_{51} 13 \cdot 13 \equiv_{51} 169 \equiv_{51} 16.$$

   Alltså

   $$D(5) \equiv_{51} 16 \cdot 13 \cdot 5 \equiv_{51} 16 \cdot 65 \equiv_{51} 16 \cdot 14 \equiv_{51} 20.$$

2. Betrakta ett RSA-krypto med $n = 57$. Du får välja parametern e själv. Skriv upp de möjliga val av parametern e du har.

   Lösn. Precis de tal e sådana att $sgd(e, m) = 1$, där $n = pq$ och $m = (p-1)(q-1)$ duger. Vi har $p = 3$ och $q = 19$ så $m = 36$. Alla tal e mellan 1 och 35 sådana att inget av talen 2 eller 3 delar e duger. Detta ger vårt svar.

3. Visa med hjälp av ett lämpligt Fermattest att talet 18 inte är ett primtal.

   Lösn. Om $b^{p-1} \not\equiv 1 \pmod{p}$ för något tal b så är p inte ett primtal, för som man säger, talet p klarade inte i så fall Fermattestet med bas b.

   Vi kollar med $b = 2$. Då $2^4 \equiv_{18} (-2)$ så

   $$2^{16} \equiv_{18} (2^4)^4 \equiv_{18} (-2)^4 \equiv_{18} 2^4 \equiv_{18} -2,$$

   så får vi

   $$2^17 \equiv_{18} 2^{16} \cdot 2 \equiv_{18} -2 \cdot 2 \equiv_{18} -4 \not\equiv_{18} 1.$$

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.

Lösn. Kolonnerna 1, 2, 5, 6 och 7 är linjärt beroende så matrisens rang blir 5. Då totala antalet kolonner är 8 blir antalet ord $2^{8-5} = 8$.

b) Bestäm minst två olika ord i C.

Lösn. Ordet $\bar{x} = (x_1, x_2, \ldots, x_8)$ tillhör koden precis då

$$H\bar{x}^T = \bar{0}.$$

Genom lite trial and error får vi orden 00000000 och 10111111.

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

Lösn. $H(1,1,1,1,1,1,1,1)^T = (0,1,0,1,1)^T$ vilket är den andra kolonnen i matrisn H. Alltså var felet i poistion 2 och det sökta ordet var 10111111.

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

Lösn. Vi chansar och tar ett ord på måfå 11100000. Vi finner att

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

vilket ju inte ár någon av H:s kolonner. Alltså ligger ordet på ett avstånd större än ett från alla kodord.

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

Lösn. Varje sfär med radien 1 runt något kodord innehåller $1 + 8$ stycken ord. Då koden är 1-felsrättande så är sfärerna med radien ett runt kodorden disjunkta. Totalt finns 8 kodord så antalet ord på avstånd ett från något kodord blir då $8 \cdot (1 + 8)$ Totalt finns 2^8 stycken ord. De ord som inte ligger i någon 1-sfár går inte att rätta.

5. Bestäm en minimal disjunktiv form för uttrycket

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

Svar: $xz + \bar{z}\bar{y} + yz\bar{w}$

6. Bestäm en minimal disjunktiv form för uttrycket

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

Svar: $\bar{x}\bar{y}z + z\bar{w}x + x\bar{y}\bar{z} + \bar{z}\bar{w}\bar{x}$

7. Bestäm en minimal disjunktiv form för uttrycket

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

Svar: $z\bar{w} + x\bar{y}\bar{w} + \bar{x}yw$

8. Bestäm en minimal disjunktiv form för uttrycket

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

Svar: $\bar{x}y + yw + x\bar{y}\bar{w} + \bar{z}\bar{w}\bar{y}$

9. Bestäm en minimal disjunktiva form för nedanstående uttryck.

   (a) $xz + x\bar{z} + \bar{x}\bar{z}$.
   Svar: $z + x$

   (b) $\bar{x}y + \bar{x}\bar{y}\bar{w} + \bar{y}w$.
   Svar: $\bar{x} + \bar{y}w$

   (c) $z + x\bar{y}z + \bar{x}yz + \bar{x}\bar{y}z$.
   Svar: z

   (d) $\bar{x}yw + yz\bar{w} + \bar{x}\bar{y}z$.
   Svar: $z\bar{x} + zwy + \bar{x}yw$