Matematiska Institutionen, KTH

Några övningar till den 30 november, Diskret matematik IT2, ht07.

1. Du skall tillverka ett RSA-krypto med parametern $n = 77$.
   (a) Förklara varför du inte kan använda parametern $e = 45$.
   (b) Du väljer $e = 13$. Bestäm d.
   (c) Kryptera meddelandet $a = 3$.
   (d) Dekryptera meddelandet $b = 2$.
2. Du betraktar ett RSA-krypto med $n = 265$ och $e = 37$. Försök dekryptera meddelandet $b = 2$.
3. Använd ett Fermattest för att visa att talet 63 inte är ett primtal.
4. Beräkna $43^{10000} \pmod{101}$.
5. Konstruera en 1-felsrättande linjär kod med 128 kodord och med en så liten längd som möjligt.
6. Vilka av följande koder är inte linjära:

$$C_1 = \{00000, 11111, 11100\}$$
$$C_2 = \{000000, 111111, 111000, 000111\}$$
$$C_3 = \{0000000, 1111111, 0001111, 1001111\}$$

7. Visa att det inte finns någon 2-felsrättande binär kod av längd 8 innehållande 7 kodord.
8. Betrakat en linjär kod C. Visa att orden av jämn vikt i C bildar en linjär kod E. Visa också att om det finns minst ett ord i C av udda vikt så är antalet ord av jämn vikt i C lika med antalet ord av udda vikt i C.
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) $\bar{x}yw + yz\bar{w} + \bar{x}\bar{y}z$.