Matematiska Institutionen, KTH

Några grupptal till övning 10 den 1 december, Diskret matematik IT1, ht05.

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