Matematiska Institutionen
KTH

Läxtal till den 30 september 2009 till kursen Diskret Matematik SF1610 för CINTE.

OBS Läxtalen är frivilliga och om du vill kan du lämna in dina lösningar och få dem rättade.

1. Betrakta ett RSA-krypto med $n = 77$ och $e = 7$, kryptera meddelandet 2 och dekryptera meddelandet 2.

2. Bestäm samtliga RSA-krypton som har $e = 7$ och ett n som tillhör intervallet $1 \leq n \leq 75$.

3. Visa med hjälp av ett Fermattest (Om vi ej hann gå igenom det på tisdagslektionen gås det igenom på onsdagen) att 4 inte är ett primtal.