Matematiska Institutionen
KTH

Lappskrivning nr 6, variant B, på kursen Diskret matematik, 5B1118, för IT1, tisdagen den 7 december 2004 kl 13.15-14.00.

Namn:

Resultat:

Vardera uppgift ger 3 poäng för korrekt lösning, för godkänt krävs 5 poäng (vilket ger att uppgift nummer 6 på tentamensskrivningen räknas som godkänd med tre poäng. Detta gäller ordinarie tentamenstillfället och de två följande omtentamina).

OBS Svaren skall motiveras och lösningarna skrivas på detta pappers fram- och baksida. Inga hjälpmedel är tillåtna.

1. Ett RSA krypto har $n = 21$ och $e = 5$, dvs i kryptot räknar man modulo 21 och krypterar meddelandet a till $E(a) = a^e \pmod{21}$. Du tar emot det krypterade meddelandet 2, dvs $E(a) = 2$ för något tal a. Bestäm detta tal a genom att använda den dekrypteringsmetod som RSA föreskriver.

2. En felkorrigerande kod C har checkmatrisen (eller kontrollmatrisen)

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

   Ange antal ord koden har samt minst två olika kodord $c_1, c_2 \in C$. Utför felkorrigering av ordet 1000101.

3. Bestäm en permutation x sådan att $\varphi \cdot x = \tau$ där $\varphi = (1\ \ 2\ \ 3)(4\ \ 5)$ och $\tau = (1\ \ 2\ \ 3\ \ 4\ \ 5)$.