

Matematiska Institutionen  
KTH

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

1. Ett RSA krypto har  $n = 33$  och  $e = 7$ , dvs i kryptot räknar man modulo 33 och krypterar meddelandet  $a$  till  $E(a) = a^e \pmod{33}$ . Du tar emot det krypterade meddelandet 3, dvs  $E(a) = 3$  för något tal  $a$ . Bestäm detta tal  $a$  genom att använda den dekrypteringsmetod som RSA föreskriver.

**Lösning:** Det gäller att  $a = D(3) = 3^d \pmod{33}$  där  $d$  satisfierar  $ed \equiv 1 \pmod{(p-1)(q-1)}$  för primtal  $p$  och  $q$  sådana att  $33 = pq$ . Vi söker  $d$ :  $33 = 3 \cdot 11$  och  $e = 7$  ger att  $7d \equiv 1 \pmod{20}$  som lätt ger  $d = 3$  eftersom  $7 \cdot 3 = 21 \equiv 1 \pmod{20}$ .

**SVAR:**  $3^3 = 27$ .

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

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

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

**Lösning:** Matrisen har sju kolonner och tre linjärt oberoende rader vilket ger att antalet ord är  $2^{7-3} = 16$ . Vi söker nu ord  $x = (x_1, \dots, x_7)$  sådana att  $Hx^T$ , (där  $T$  betyder transponering), blir lika med nollkolonnen när vi räknar modulo två. Orden  $(0, 0, \dots, 0)$  och  $(1, 1, 1, 0, 0, 0, 0)$ , som vi hittar genom prövning, uppfyller detta.

För att utföra den sökta felkorrigeringen låter vi nu  $x = (1, 0, 0, 0, 1, 0, 1)$  och får då att  $Hx^T$  blir lika med den andra kolonnen. Felet uppstod i position två och det korrigerade ordet är ordet 1100101.

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

**Lösning:**  $x = \varphi^{-1}\tau$ . Då  $\varphi^{-1} = (2 \ 3 \ 1)(5 \ 4)$  får vi

**SVAR:**  $(2 \ 3 \ 1)(5 \ 4)(1 \ 2 \ 3 \ 5 \ 4) = (1 \ 3 \ 4 \ 2)(5)$