

Matematiska Institutionen  
KTH

**Några övningar på felkorrigerande koder, RSA-kryptering och permutationer inför lappskrivning 6 media.**

1. Betrakta ett RSA-krypto med  $n = 51$  och  $e = 5$ . Kryptera meddelandet 3 och dekryptera meddelandet 5.
2. Betrakta ett RSA-krypto med  $n = 57$ . Du får välja parametern  $e$  själv. Skriv upp de möjliga val av parametern  $e$  du har.
3. Visa med hjälp av ett lämpligt Fermattest att talet 18 inte är ett primtal.
4. Låt  $C$  vara en 1-felsrättande kod med kontrollmatrisen

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

- a) Bestäm antalet ord i koden  $C$ .
  - b) Bestäm minst fem olika ord i  $C$ .
  - c) Ordet 11111111 ligger på avståndet ett från precis ett ord i  $C$ . Vilket.
  - d) Bestäm minst ett ord av längd åtta som inte tillhör  $C$  och som inte ligger på avståndet ett från något kodord
  - e) Bestäm antalet binära ord av längd åtta som varken tillhör  $C$  eller ligger på avståndet ett från något ord i  $C$ .
5. Låt  $\varphi = (1\ 2\ 4\ 7)(3\ 5\ 6)$ ,  $\psi = (1\ 5\ 3)(4\ 2)(6\ 7)$  och  $\gamma = (1\ 2\ 3\ 4\ 5\ 6\ 7)$ .
    - a) Skriv permutationerna  $\varphi\psi\gamma$  och  $\psi\gamma\varphi$  som produkter av disjunkta cykler.
    - b) Bestäm  $\psi^{-1}\varphi^{-1}$ .
    - c) Beräkna  $\psi^{-1}\gamma\psi$ .
    - d) Bestäm ordningen hos permutationerna  $\psi^{-1}\varphi^{-1}$ ,  $\gamma$  och  $\psi^{-1}\gamma\psi$ .
    - e) Skriv permutationerna  $\varphi$ ,  $\psi$  och  $\gamma$  som produkter av transpositioner.
    - f) Vilka av permutationerna i uppgift d) är udda respektive jämna.

**Svar:**

1.  $E(3) = 39$ ,  $d = 13$  ger att  $D(5) = 20$ .
2. 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.
- 3.
4. a) 8, b) , c) 10111111, d) 11100000, e)  $2^8 - 8 \cdot (1 + 8)$ .
5. a)  $\varphi\psi\gamma = (1\ 7\ 6\ 3\ 4\ 5)(2)$  och  $\psi\gamma\varphi = (1)(2\ 3\ 7\ 4\ 5\ 6)$ .  
 b)  $(1\ 6)(2\ 3\ 7)(4)(5)$   
 c)  $(1\ 7\ 6\ 3\ 4\ 5\ 2)$   
 d) 6, 7 resp 7.  
 e)  $\varphi = (1\ 7)(1\ 4)(1\ 2)$ ,  $\psi = (1\ 3)(1\ 5)(4\ 2)(6\ 7)$ ,  $\gamma = (1\ 7)(1\ 6)(1\ 5)(1\ 4)(1\ 3)(1\ 2)$ .  
 f)  $\varphi$  är udda och de övriga är jämna.