2011-(04)apr-07: dag 21

3) Kodens längd n

Sfärpackningssatsen

$$4\underbrace{\left(\binom{n}{0} + \binom{n}{1} + \binom{n}{2}\right)}_{\frac{1}{2}(n^2 + n + 2)} \leq 2^n$$

Det vill säga

n:	$n^2 + n + 2$	$\leq$	2^{n-1}
1	4		1
2	8		2
3	14		4
4	22		8
5	32		16
6	44		32
7	58		64

Så sfärpackningssatsen ger $n \geq 7$.

Men om c_1, c_2 av längd 7 har avstånd minst 5 (för två felrättningar) till c_3 kan avståndet mellan c_1 och c_2 inte vara > 4:

Låt $A = \{\text{Positioner där } c_1 \text{ och } c_3 \text{ skiljer sig}\}$
$B = \{\text{Positioner där } c_2 \text{ och } c_3 \text{ skiljer sig}\}$

$$\partial(c_1, c_2) = |(A \cup B) \setminus (A \cap B)| = |A \cup B| - |A \cap B| \leq 4$$

$$\text{men } = \underbrace{|A \cup B|}_{\leq 7} - |A \cap B| = \underbrace{|A|}_{\geq 5} + \underbrace{|B|}_{\geq 5}$$

$\uparrow$
så ≥ 3

7 räcker inte, men med $n = 8$

C= {00000000, 11111000, 00011111, 11100111}

4)

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \underset{\substack{r3 + r1 \\ r4 + r2}}{\sim} \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix} \underset{r1 + r4}{\sim}$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \underset{\substack{r1 + r3 \\ r3 + r4}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} = H_1$$

H och H_1 definierar sama linjär kod C.
Linjärt oberoende rader så rang H = 4.

a) Antalet ord i C, $|C| = 2^k = 2^{n - \text{rank } H} = 2^{8-4} = 16$

c) Antalet ord inte i C:

$$2^8 - |C| = 256 - 16 = 240$$

d) Ett sådant ord: 00100111

e) Felaktiga ord med ett fel:

$$16 \cdot 8 = 128 \text{ stycken}$$

f) Rätta ordet 01111000

$$Hz = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \text{H:s 5:e kolonn}$$

Så det rättade ordet (ett fel): 01110000

5) Om H har en m linjört oberoende rader skall n = 7 + m ty dimensionen k = n − rank H = 7 − m.

1-felrättande om all kolonner olika $\neq \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ $\qquad 128 = 2^7$

Så $7 + m \leq 2^m - 1$

m	8 + m	≤	2^m		
1	9		2	X	
2	10		4	X	
3	11		8	X	
4	12		16	0	OK

Så minimala antalet rader i H = 4.
Kolonner: 11

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

8) RSA med $n = 77 = \overset{p}{7} \cdot \overset{q}{11}$

$m = (p - 1)(q - q) = 6 \cdot 10 = 60$

a) Parametern e = 45 går ej ty sgd(45, 6) = 13 ≠ 1

b) e = 13 går bra sgd(13, 60) = 1

Vad blir d? ($ed \equiv 1 \pmod{m}$)

Euklides' algoritm:

$60 = 4 \cdot 13 + 8$
$13 = 1 \cdot 8 + 5$
$8 = 1 \cdot 5 + 3$
$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$

$1 = 3 - 2 =$
$= 3 - (5 - 3) =$
$= 2{\cdot}3 - 5 =$
$= 2(8 - 5) - 5=$
$= 2{\cdot}8 - 3{\cdot}5 =$
$= 2{\cdot}8 - 3(13 - 8) =$
$= -3 \cdot 13 + 5{\cdot}8 =$
$= -3{\cdot}13 + 5(60 - 4{\cdot}13) =$
$= 5{\cdot}60 - 23{\cdot}13 =$
$= (5 - 13){\cdot}60 + (60 - 23){\cdot}13 =$
$= 37{\cdot}13 - 8{\cdot}60$

Så $37{\cdot}13 \equiv 1 \pmod{60}$ vi har d = 37

c) $E(3) = 3^{13} = 3^8 \cdot 3^4 \cdot 3^1$

$3^2 \equiv 9,\ 3^4 = 9^2 \equiv 4,\ 3^8 = 4^2 \equiv 16 \pmod{77}$

$E(3) \equiv 6 \cdot 4 \cdot 3 = 192 \equiv 36 \pmod{77}$

Så E(3) = 38

d) $D(2) \equiv 2^{37} \equiv 2^{32} \cdot 2^4 \cdot 2 \equiv 4 \cdot 16 \cdot 2 = 128 \equiv 51 \pmod{77}$

1	2	4	8	16	32
2	4	16	25	9	4

11) Är 63 ett primtal?

Fermattest med bas 2

$2^{62} \equiv ? \pmod{63}$

$2^{62} = 2^{32} \cdot 2^{16} \cdot 2^{8} \cdot 2^{4} \cdot 2^{2}$

mod 63:

$$
\begin{aligned}
2^2 &= 4 \\
2^4 &= 4^2 = 16 \\
2^8 &= 16^2 = 256 \equiv 4 \\
2^{16} &= 4^2 = 16 \\
2^{32} &= 16^2 \equiv 4
\end{aligned}
$$

$$2^{64} \equiv 4 \cdot \underbrace{16 \cdot 4}_{1} \cdot \underbrace{16 \cdot 4}_{1} = 4 \pmod{63}$$

Ej primtal.

12) Vad är $43^{139702} \pmod{101}$?

101 är ett primtal och $101 \nmid 43$ så

$43^{100} \equiv 1 \pmod{101}$ {Fermats lilla sats}

Så:

$$43^{139702} = 43^{1307} \cdot 43^{2} = 43^{2} = 1849$$

$$18 \cdot 101 + 31 = 31$$