2011-(04)apr-06: dag 20

Enkelt sätt att hitta fel i en kod:
paritetskontrollbit (jämför med sista siffran i personnummer).

$$\begin{array}{l}
670723\text{-}146 \\
\quad\downarrow \\
12, 7, 0, 7, 4, 3, 2, 4, 12 \\
\quad\downarrow \\
1, 2, 7, 0, 7, 4, 3, 2, 4, 1, 2
\end{array}
\qquad
\begin{array}{l}
\text{Summa: } 33 \\
\\
33 + \underline{7} = 40 \equiv 0 \pmod{10} \\
\quad\downarrow \\
670723\text{-}146\underline{7}
\end{array}$$

Lite allmännare:

(paritets)kontrollmatris

$$H = \underbrace{\begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & & & & & & & \end{pmatrix}}_{n} \left.\vphantom{\begin{pmatrix} 0 \\ 0 \end{pmatrix}}\right\} m \qquad m \times n \text{ 0/1-matris}$$

Till H hör en linjär kod

$$C = \{x \in \mathbb{Z}_2^n : \underset{(m\times n)x}{Hx} \underset{=}{=} \underset{n\times 1}{0}\} \qquad \text{med dimension } n - \text{rank } H$$

antalet linjärt oberoende rader i H.

Enkelt fall:

$$H = \begin{pmatrix} \underset{m\times m}{I} & \underset{m\times(n-m)}{B} \end{pmatrix}$$

Sista $(n - m)$ positionen kan väljas fritt.

Vad är C om $H = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$?

x_2 och x_4 kan vara godtyckliga,

då bestäms x_1, x_3: $x_1 + x_2 + x_4 = 0 \Rightarrow x_1 = x_2 + x_4$

$x_2 + x_3 = 0 \Rightarrow x_3 = x_2$ (i $\mathbb{Z}_2$)

C = {0000, 1001, 1110, 0111}

x_2:	x_4:
0	0
0	1
1	0
1	1

Sats: Om H inte har någon kolonn = 0 samt att alla kolonner är unika, så rättar C ett fel.

Koden som ges av H.

Ty: Vi skall se att $\omega_{min} \geq 3$

Hc = 0 och $\omega(c) = 1$ skulle ge nollkolonn i H.

Hc = 0 och $\omega(c) = 2$ ger två lika kolonner.

Med sådana H är det lätt att rätta ett fel (på position i)

Om vi tar emot $z_{n \times 1} = c + e = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$ rad i

kodord i koden

Så Hz = Hc + He = H:s i:te kolonn.

= 0 eftersom c är ett kodord

Exempel:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix} \qquad \text{rättar enlig stsen minst ett fel.}$$

Vi tar emot $z = 11011$, vad sändes?
(Förutsätt att bara ett fel uppstod.)

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

Så första biten (siffran) är fel. $\Rightarrow$ $c = 01011$

Hammingkod: $\overbrace{H}^{r \times \underbrace{(2^r - 1)}_{\text{Maximal bredd}}}$ med alla kolonner unika och inte 0.

Exempel:

$r = 2$

$2^r - 1 = 3$

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

r stycken ger $x_1, x_2, \ldots, x_r$ uttryckta i resten.

Dimension: $k = 2^r - r - 1$
Minsta avstånd: $\delta = 3$
Längd: $n = 2^r - 1$

$$|C| = 2^k = 2^{2^r - r - 1}$$

Sfärpackningssatsen med e = 1:

$$|C|\left(1 + \binom{n}{1}\right) \leq 2^n$$

$$\Downarrow$$

$$2^{2^r - r - 1} \cdot \underbrace{(1 + n)}_{2^r} \leq 2^n$$

$$\Downarrow$$

$$\underbrace{2^{2^r - 1}}_{2^n} \leq 2^n$$

$$\Downarrow$$

$2^n \leq 2^n$ Likhet!
Perfekta koder.

Exempelet:

$$H = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \qquad \overset{Hx = 0}{\text{ger:}} \quad C = \{000, 111\}$$

$$\overset{Hx = 0}{\left(\begin{array}{ccc|c} 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right)} \Leftrightarrow \left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right)$$

H ger: $x_2 + x_3 = 0$ (rad 1)
$x_1 + x_3 = 0$ (rad 2)

Alltså: Antingen $x_2 = 1 \Rightarrow x_3 = 1 \;\&\; x_1 = 1$
eller $x_2 = 0 \Rightarrow x_3 = 1 \;\&\; x_1 = 1$

Kryptering (mest RSA)

Koder för att skydda information från obehöriga

Allmänt:

$$\mathcal{M} \underset{D}{\overset{E}{\rightleftarrows}} \mathcal{C}$$

$\mathcal{M}$ — Meddelandet i klartext
$\mathcal{C}$ — Chiffer, krypterad text

E — Kryptering
D — Dekrypering (avkryptering)

$D = E^{-1}$

Klassiskt chiffer: byta bokstäver,
vanligtvis måste då E och D vara hemliga.

Ny idé: (Diffle, Hellman, 1976)

Offentlig nyckel E: allmänt känd, men så pass komplicerad att det är svårt(!) att bestämma inversen, D.

Kallas envägsfunktion.

Exempel på sådant system:

RSA (Rivest, Shamir Adleman) Simon Singh: Kodboken (☺)

Fermats lilla sats är grunden till RSA.

Fermats lilla sats

Om p är ett primtal och $a \in \mathbb{Z}_p \setminus \{0\}$:

$a^{p-1} = 1 \quad$ i $\mathbb{Z}_p \qquad (a^{p-1} \equiv 1 \pmod{p})$

$p \nmid a \;\Rightarrow\; p \mid a^{p-1} - 1 \quad$ i $\mathbb{Z}$
$p \mid a^p - a \quad$ alla a

Exempel:

$$5^6 = \{5^6 = 5^{7-1}\} = 15625 = 2232 \cdot 7 + 1$$

Ty: $\quad a \in \mathbb{Z}_p \setminus \{0\}$

En grupp med multiplikation, med $p - 1$ stycken element.
Så $a^{p-1} = 1$ i $\mathbb{Z}_p$.

Följdsats:

Låt p, q vara olika primtal

$n = pq,\ m = (p-1)(q-1)$

$s \equiv 1 \pmod{m} \;\Rightarrow\; x^s \equiv x \pmod{n} \quad$ för alla $x \in \mathbb{Z}$

Ty:
$s = 1 + k(p-1)(q-1)$, något heltal k

$x^s - x = x(x^{k(p-1)(q-1)} - 1) = x((x^{(p-1)})^{(q-1)k} - 1) \equiv$
$\equiv x(1^k - 1) = x(1-1) = x \cdot 0 = 0 \qquad \pmod{p, q}$

$p, q \setminus x^5 - x \qquad$ så $\qquad n = pq \setminus x^5 - x$

dualprimtal

RSA-systemet på på satsen:

Tag två olika stora(!) primtal, p, q. ($\sim 10^{150}$)
Beräkna $n = pq$, $m = (p - 1)(q - 1)$
Välj e med $sgd(e, m) = 1$ och
finn d med $ed \equiv 1 \pmod{m}$ (Euklides' algoritm)

Offentliggör n och e, men hemlighåll d (kasta m).

$E(x) \equiv x^e \pmod{n}$ $\quad E : \mathbb{Z}_n \to \mathbb{Z}_n$
$D(x) \equiv x^d \pmod{n}$ $\quad D : \mathbb{Z}_n \to \mathbb{Z}_n$

Gäller enär $D(E(x)) \equiv (E(x))^d \equiv (x^e)^d = x^{ed} \equiv x \pmod{n}$

$\therefore \quad D(E(x)) = E(D(x))$

E är en envägsfunktion (gör det klurigt) ty det är (troligen) svårt att primtalsfaktorisera stora tal.

Elektronisk signatur

B skickar till A:

$E_A(D_B(x))$ eller $D_B(E_A(x))$

För att läsa det gör A:

$D_A(E_A(D_B(x))) = D_B(x)$ och så:

$E_B(D_B(x)) = x$ $\quad$ (E_B är offentlig)

Kan läsas bara av den som har tillgång till D_A (alltså A) och bara skrivits av den med D_B (alltså B).

Alternativt:

Offentliggör D(x), alla kan läsa med E,
men bara den som hade D kunde ha skrivit det.

Hur får man tag i stora primtal, p, q?

Det finns ganska gott om primtal.
Sannolikheten för att ett tal ska ara primtal:

$$\text{täthet} \sim \frac{1}{\ln n}, \quad n = \text{längden av talet}$$

det svåra är dock att känna igenom dem, hur gör vi?

Primtalitetstest

Pröva faktorer $(\sqrt{n} \approx 10^{75})$

Fermats lilla sats!

Fermattestet:

(Med bas b) för primtalitet hos N

Är $b^{N-1} \equiv 1 \pmod{N}$?

Nej: N sammansatt, ej primtal.

Ja: Vi vet inte säkert.

Pseudoprimtal (bas b)

Sammansatta tal som klarar testet

Till exempel för bas 2:

$341 = 11 \cdot 31$