(F26, to 27 feb)

C är en **linjär kod** om

$$a, b \in C \Rightarrow a + b \in C$$

dvs C är ett **delrum** till vektorrummet V^n

$|C| = 2^k$, där k kallas (och är) C:s **dimension**

För en linjär kod är minimala avståndet = **minimala** (nollskilda) **vikten**, dvs

$$\delta = w_{\min} = \min\{w(c) \mid c \in C,\ c \neq 0\}$$

där vikten för c, $w(c)$, är antalet 1:or i c.

Om H är en $m \times n$-matris är $C = \{x \in V^n \mid Hx = 0\}$ en linjär kod av dimension $n - rankH$. H kallas kodens (paritets)**kontrollmatris**.

Sats: Om H:s alla kolonner är olika och $\neq \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$, så rättar C (minst) ett fel.

För att rätta fel :

z ett kodord med fel i position $i \ \Rightarrow \ Hz = H$:s i:e kolonn.

Hammingkod ges av en kontrollmatris H med r rader och $2^r - 1$ kolonner, alla olika och $\neq 0$

längd	$n = 2^r - 1$
minimiavstånd	$\delta = 3$
dimension	$k = 2^r - r - 1$

Hammingkoder ger likhet i sfärpackningssatsen, de är **perfekta koder**.

Om **kryptering**

$\mathcal{M}$ och $\mathcal{C}$: Meddelanden (klartext) och chiffer (krypterad text),
E och D : Kryptering och dekryptering,

$$\mathcal{M} \underset{D}{\overset{E}{\rightleftarrows}} \mathcal{C} \ , \qquad D = E^{-1}$$

Traditionellt : E och D är bara kända av behöriga.

Nytt (1976) : **Offentlig nyckel**, E en **envägsfunktion**, känd av "alla". Svårt att bestämma E^{-1} ur E.

Sats: Låt p, q vara olika primtal, $n = pq$, $m = (p-1)(q-1)$ $(= \phi(n))$.
Då gäller $s \equiv_m 1 \ \Rightarrow \ x^s \equiv_n x$, alla $x \in \mathbb{Z}$

Så **RSA-algoritmen** :

Tag p, q stora, olika, primtal ($\approx 10^{100}$), **beräkna** $n = pq$, $m = (p-1)(q-1)$
Välj e med $\text{sgd}(e, m) = 1$ och **finn** d med $ed \equiv_m 1$ (Euklides)
Offentliggör n, e och **hemlighåll** d.

$E : \mathbb{N}_n \to \mathbb{N}_n$, $E(x) \equiv_n x^e$ och $D : \mathbb{N}_n \to \mathbb{N}_n$, $D(x) \equiv_n x^d$
ger då $D = E^{-1}$.

$E(x)$ **beräknas** med $f_0, f_1 : \mathbb{N}_n \to \mathbb{N}_n$, givna av $f_0(t) \equiv_n t^2$, $f_1(t) \equiv_n t^2 \cdot x$:
Om e är $(e_k e_{k-1} \dots e_1 e_0)_2$ binärt är

$$E(x) = f_{e_0}(f_{e_1}(\dots(f_{e_{k-1}}(f_{e_k}(1)))\dots)).$$

Elektronisk signatur :

1. Sänd $D(x)$. Alla kan läsa (med E), ingen utan D kunde ha skrivit.
2. B sänder $E_A(D_B(x))$ (eller $D_B(E_A(x))$) till A. Bara någon med D_A kan läsa, bara någon med D_B kunde ha skrivit.