Codificació de la informació

Maria Bras-Amorós

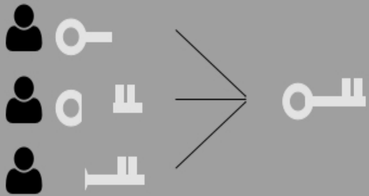
UNIVERSITAT ROVIRA i VIRGILI

13 de març del 2021

Teoria de codis

Esteganografia

Compartició de secrets



Emmagatzematge distribuït

Suposem que en una comunicació amb molt de soroll s'ha de comunicar una de les paraules

CERT o **FALS**.

Si el receptor rep la paraula

CART

quina paraula deduiríeu que s'ha enviat?

Suposem que en una comunicació amb molt de soroll s'ha de comunicar una de les paraules

CERT o **FALS**.

Si el receptor rep la paraula

CART

quina paraula deduiríeu que s'ha enviat?

CERT $\rightarrow$**CART**

En aquest cas podem dir que s'ha produït **un error**.

Suposem que s'han esborrat algunes lletres i hem rebut

??LS.

Què es deu haver enviat?

Suposem que s'han esborrat algunes lletres i hem rebut

??LS.

Què es deu haver enviat?

FALS $\rightarrow$**??LS**

En aquest cas podem dir que s'han produït **dos esborralls**.

Suposem que s'han esborrat algunes lletres i hem rebut

??LS.

Què es deu haver enviat?

FALS $\rightarrow$ **??LS**

En aquest cas podem dir que s'han produït **dos esborralls**.

I si rebem

CALT

Podem deduir què s'ha enviat?

$\{CERT, FALS\}$ és un ***codi*** amb

- 2 paraules, de 4 lletres cada una
- capacitat de corregir 1 error
- capacitat de corregir 3 esborralls

La Teoria de Codis estudia exemples més grans, emfatitzant en

Estructures de primer nivell:

Cossos finits

E. Galois

La Teoria de Codis estudia exemples més grans, emfatitzant en

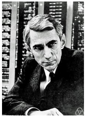
Estructures de primer nivell:

Cossos finits

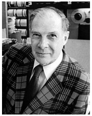
E. Galois

Estructures de segon nivell:

Codis correctors d'errors



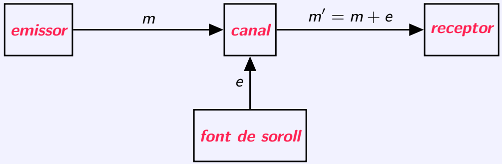
C. Shannon



R. Hamming

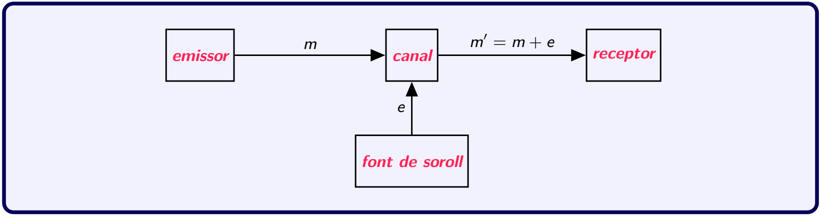
J. MacWilliams

Model sense codificació

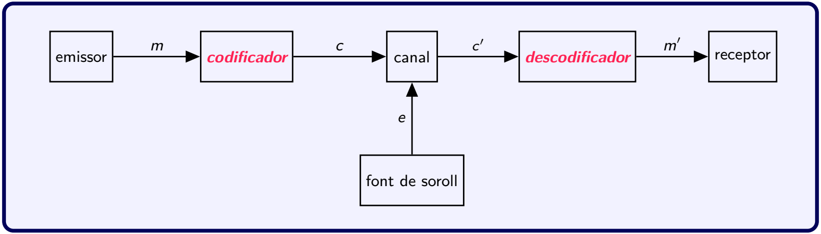


Teoria de codis

Model sense codificació



Model amb codificació



Separem tots els enters en 7 colors diferents

...	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	...

Un conjunt finit amb una operativa

Separem tots els enters en 7 colors diferents

$\cdots$ -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 $\cdots$

Un conjunt finit:

$$\mathbb{Z}_7 = \{ \boxed{0}, \boxed{1}, \boxed{2}, \boxed{3}, \boxed{4}, \boxed{5}, \boxed{6} \}$$

Amb una operativa: Operem de la forma habitual a $\mathbb{Z}$ i el resultat a $\mathbb{Z}_7$ vindrà donat pel color del resultat a $\mathbb{Z}$.

Un conjunt finit amb una operativa

Separem tots els enters en 7 colors diferents

$\cdots$ -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8 9 10 11 12 13 $\cdots$

Un conjunt finit:

$$\mathbb{Z}_7 = \{\, 0, 1, 2, 3, 4, 5, 6 \,\}$$

Amb una operativa: Operem de la forma habitual a $\mathbb{Z}$ i el resultat a $\mathbb{Z}_7$ vindrà donat pel color del resultat a $\mathbb{Z}$.

Així podem escriure, per exemple,

$$6 + 2 = 1$$

$$3 \times 4 = 5$$

$$5^2 = 4$$

Un codi Reed-Solomon

Considerem les primeres potències dels elements no nuls de $\mathbb{Z}_7$

$1^0 = 1$	$1^1 = 1$	$1^2 = 1$	$1^3 = 1$
$2^0 = 1$	$2^1 = 2$	$2^2 = 4$	$2^3 = 1$
$3^0 = 1$	$3^1 = 3$	$3^2 = 2$	$3^3 = 6$
$4^0 = 1$	$4^1 = 4$	$4^2 = 2$	$4^3 = 1$
$5^0 = 1$	$5^1 = 5$	$5^2 = 4$	$5^3 = 6$
$6^0 = 1$	$6^1 = 6$	$6^2 = 1$	$6^3 = 6$

Un codi Reed-Solomon

Considerem les primeres potències dels elements no nuls de $\mathbb{Z}_7$

$$\begin{array}{l} 1^0 = 1 \\ 2^0 = 1 \\ 3^0 = 1 \\ 4^0 = 1 \\ 5^0 = 1 \\ 6^0 = 1 \end{array} \qquad \begin{array}{l} 1^1 = 1 \\ 2^1 = 2 \\ 3^1 = 3 \\ 4^1 = 4 \\ 5^1 = 5 \\ 6^1 = 6 \end{array} \qquad \begin{array}{l} 1^2 = 1 \\ 2^2 = 4 \\ 3^2 = 2 \\ 4^2 = 2 \\ 5^2 = 4 \\ 6^2 = 1 \end{array} \qquad \begin{array}{l} 1^3 = 1 \\ 2^3 = 1 \\ 3^3 = 6 \\ 4^3 = 1 \\ 5^3 = 6 \\ 6^3 = 6 \end{array}$$

I així construïm la matriu

$$G = \begin{array}{cccccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 \end{array}$$

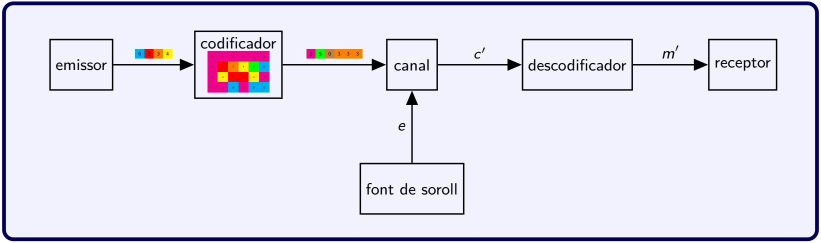
Per codificar una paraula com $\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix}$ amb la matriu G, la multipliquem per G.

$$\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 0 & 3 & 3 & 3 \end{pmatrix}$$

Un codi Reed-Solomon

Per codificar una paraula com $\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix}$ amb la matriu G, la multipliquem per G.

$$\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 0 & 3 & 3 & 3 \end{pmatrix}$$



Un codi Reed-Solomon

Suposem que ara volem codificar la imatge

6	6	6	6
6	6	6	2
6	6	2	3
6	2	3	4
2	3	4	4
3	4	4	4
6	4	4	1
6	4	4	1
6	4	4	1
6	4	4	4
6	4	5	4
6	5	5	4
5	5	5	5
5	5	5	5
6	5	5	5
6	5	5	5
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4

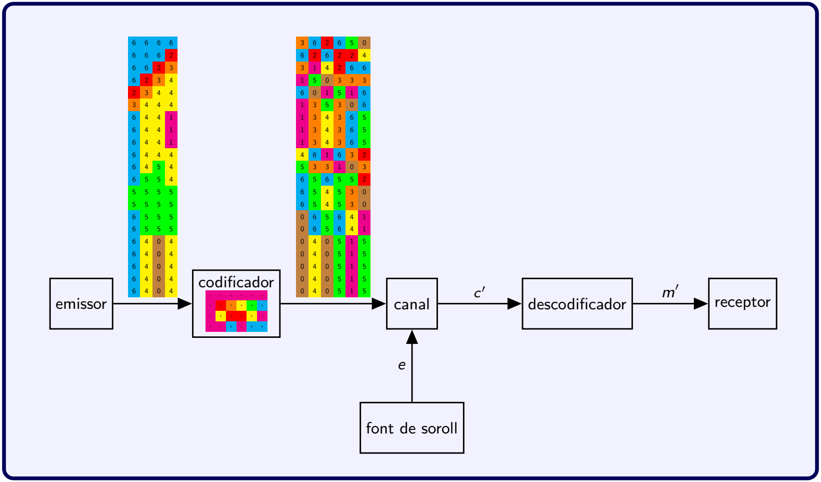
Un codi Reed-Solomon

Codificarem cadascuna de les seves files

6	6	6	6
6	6	6	2
6	6	2	3
6	2	3	4
2	3	4	4
3	4	4	4
6	4	4	1
6	4	4	1
6	4	4	1
6	4	4	4
6	4	5	4
6	5	5	4
5	5	5	5
5	5	5	5
6	5	5	5
6	5	5	5
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4

3	6	2	6	5	0
6	2	6	2	2	4
3	1	4	2	6	6
1	5	0	3	3	3
6	0	1	5	1	6
1	3	5	3	0	6
1	3	4	3	6	5
1	3	4	3	6	5
1	3	4	3	6	5
4	6	1	6	3	2
5	3	3	1	0	3
6	5	6	5	5	2
6	5	4	5	3	0
6	5	4	5	3	0
0	6	5	6	4	1
0	6	5	6	4	1
0	4	0	5	1	5
0	4	0	5	1	5
0	4	0	5	1	5
0	4	0	5	1	5
0	4	0	5	1	5

Un codi Reed-Solomon



Una alternativa: **matriu sistemàtica** equivalent a G:

$$G_s = \begin{array}{cccccc} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{array}$$

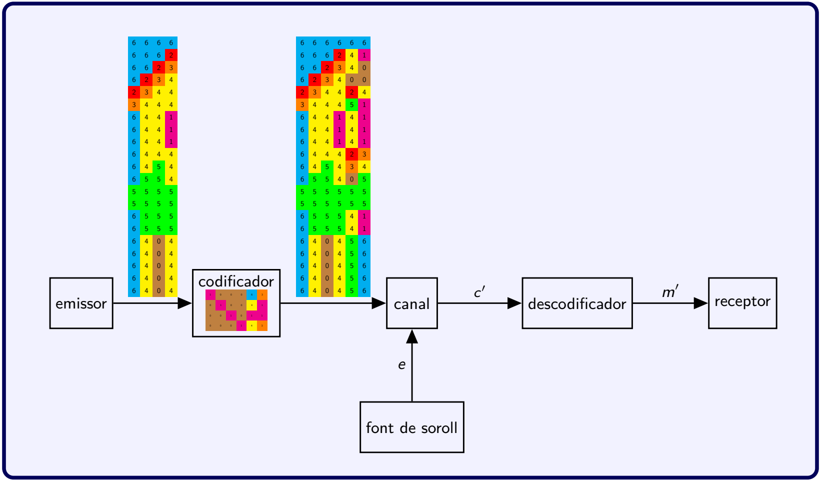
Una alternativa: **matriu sistemàtica** equivalent a G:

$$G_s = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix}$$

Així, codificar una paraula com $\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix}$ serà

$$\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 2 & 3 & 4 & 0 & 0 \end{pmatrix}$$

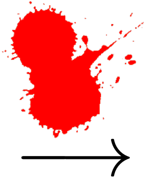
Ara, en codificar la imatge, què observem?



Un codi Reed-Solomon

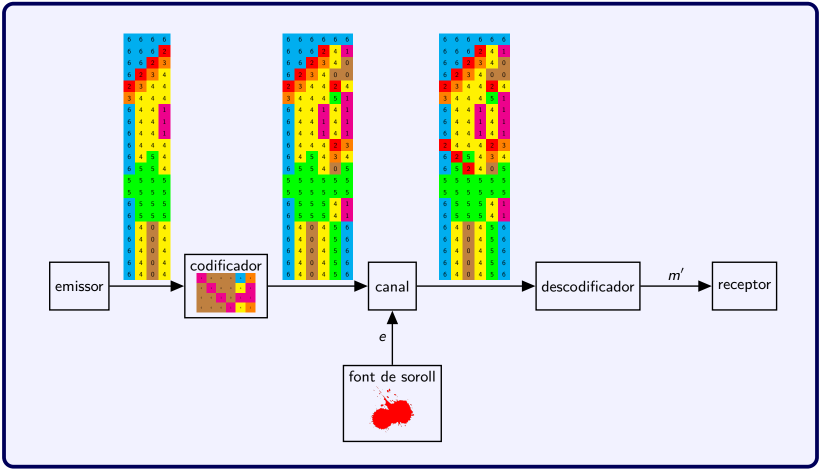
Suposem que se'ns embruta la imatge codificada:

6	6	6	6	6	6
6	6	6	2	4	1
6	6	2	3	4	0
6	2	3	4	0	0
2	3	4	4	2	4
3	4	4	4	5	1
6	4	4	1	4	1
6	4	4	1	4	1
6	4	4	1	4	1
6	4	4	4	2	3
6	4	5	4	3	4
6	5	5	4	0	5
5	5	5	5	5	5
5	5	5	5	5	5
6	5	5	5	4	1
6	5	5	5	4	1
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6



6	6	6	6	6	6
6	6	6	2	4	1
6	6	2	3	4	0
6	2	3	4	0	0
2	3	4	4	2	4
3	4	4	4	5	1
6	4	4	1	4	1
6	4	4	1	4	1
6	4	4	1	4	1
2	4	4	4	2	3
6	2	5	4	3	4
6	5	2	4	0	5
5	5	5	5	5	5
5	5	5	5	5	5
6	5	5	5	4	1
6	5	5	5	4	1
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6

Un codi Reed-Solomon



Un codi Reed-Solomon

Recordem:

$1^1 = 1$	$1^2 = 1$
$2^1 = 2$	$2^2 = 4$
$3^1 = 3$	$3^2 = 2$
$4^1 = 4$	$4^2 = 2$
$5^1 = 5$	$5^2 = 4$
$6^1 = 6$	$6^2 = 1$

Considerem ara

$$H = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 4 & 2 & 2 & 4 & 1 \\ \hline \end{array}$$

Recordem:

$1^1 = 1$	$1^2 = 1$
$2^1 = 2$	$2^2 = 4$
$3^1 = 3$	$3^2 = 2$
$4^1 = 4$	$4^2 = 2$
$5^1 = 5$	$5^2 = 4$
$6^1 = 6$	$6^2 = 1$

Considerem ara

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \end{pmatrix}$$

Les paraules codificades per G (i per G_s) són exactament el nucli d'H.

Donada una paraula qualsevol u, la seva ***síndrome*** és $s = uH^T$. Les paraules del codi seran les que tenen síndrome 0.

Per identificar on s'han produït els errors, multiplicarem cada fila per H^T.

$$
\begin{array}{cccccc}
6 & 6 & 6 & 6 & 6 & 6 \\
6 & 6 & 6 & 2 & 4 & 1 \\
6 & 6 & 2 & 3 & 4 & 0 \\
6 & 2 & 3 & 4 & 0 & 0 \\
2 & 3 & 4 & 4 & 2 & 4 \\
3 & 4 & 4 & 4 & 5 & 1 \\
6 & 4 & 4 & 1 & 4 & 1 \\
6 & 4 & 4 & 1 & 4 & 1 \\
6 & 4 & 4 & 1 & 4 & 1 \\
2 & 4 & 4 & 4 & 2 & 3 \\
6 & 2 & 5 & 4 & 3 & 4 \\
6 & 5 & 2 & 4 & 0 & 5 \\
5 & 5 & 5 & 5 & 5 & 5 \\
5 & 5 & 5 & 5 & 5 & 5 \\
6 & 5 & 5 & 5 & 4 & 1 \\
6 & 5 & 5 & 5 & 4 & 1 \\
6 & 4 & 0 & 4 & 5 & 6 \\
6 & 4 & 0 & 4 & 5 & 6 \\
6 & 4 & 0 & 4 & 5 & 6 \\
6 & 4 & 0 & 4 & 5 & 6 \\
6 & 4 & 0 & 4 & 5 & 6
\end{array}
\qquad
\begin{array}{cc}
1 & 1 \\
2 & 4 \\
3 & 2 \\
4 & 2 \\
5 & 4 \\
6 & 1
\end{array}
\longrightarrow
\qquad
\begin{array}{cc}
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
3 & 3 \\
3 & 6 \\
5 & 1 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0 \\
0 & 0
\end{array}
$$

Allà on el resultat és diferent de zero és on hi ha errors.

Un codi Reed-Solomon

Per trobar el valor dels errors, vegem que les síndromes són múltiples de columnes d'H

$$
\begin{array}{cc}
0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\
3 & 3\\ 3 & 6\\ 5 & 1\\
0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0
\end{array}
\quad \rightarrow \quad
\begin{array}{l}
\begin{pmatrix} 3 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1\\ 2 & 4\\ 3 & 2\\ 4 & 2\\ 5 & 4\\ 6 & 1 \end{pmatrix}\\[2ex]
\begin{pmatrix} 3 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 5 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1\\ 2 & 4\\ 3 & 2\\ 4 & 2\\ 5 & 4\\ 6 & 1 \end{pmatrix}\\[2ex]
\begin{pmatrix} 5 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 4 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1\\ 2 & 4\\ 3 & 2\\ 4 & 2\\ 5 & 4\\ 6 & 1 \end{pmatrix}
\end{array}
$$

Un codi Reed-Solomon

Per trobar el valor dels errors, vegem que les síndromes són múltiples de columnes d'H

$$
\begin{pmatrix}
0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\
3 & 3\\ 3 & 6\\ 5 & 1\\
0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0\\ 0 & 0
\end{pmatrix}
\rightarrow
\begin{array}{l}
\begin{pmatrix} 3 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1\\ 2 & 4\\ 3 & 2\\ 4 & 2\\ 5 & 4\\ 6 & 1 \end{pmatrix}\\[1em]
\begin{pmatrix} 3 & 6 \end{pmatrix} = \begin{pmatrix} 0 & 5 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1\\ 2 & 4\\ 3 & 2\\ 4 & 2\\ 5 & 4\\ 6 & 1 \end{pmatrix}\\[1em]
\begin{pmatrix} 5 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 4 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1\\ 2 & 4\\ 3 & 2\\ 4 & 2\\ 5 & 4\\ 6 & 1 \end{pmatrix}
\end{array}
$$

Deduïm que les paraules d'error són

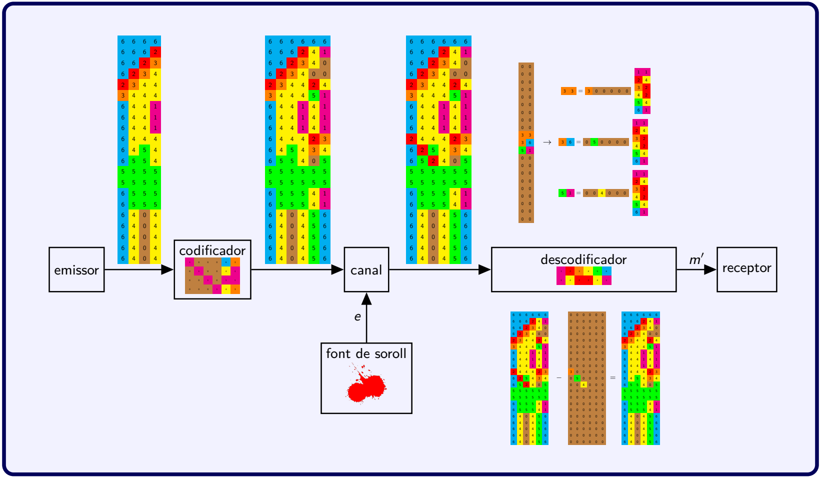
$$
\begin{pmatrix} 3 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 5 & 0 & 0 & 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 4 & 0 & 0 & 0 \end{pmatrix}
$$

Un codi Reed-Solomon

Restem les paraules d'error de les paraules rebudes

$$
\begin{array}{cccccc}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
2&4&4&4&2&3\\
6&2&5&4&3&4\\
6&5&2&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{array}
\quad - \quad
\begin{array}{cccccc}
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
3&0&0&0&0&0\\
0&5&0&0&0&0\\
0&0&4&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0
\end{array}
\quad = \quad
\begin{array}{cccccc}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&4&2&3\\
6&4&5&4&3&4\\
6&5&5&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{array}
$$

Un codi Reed-Solomon



Un codi Reed-Solomon

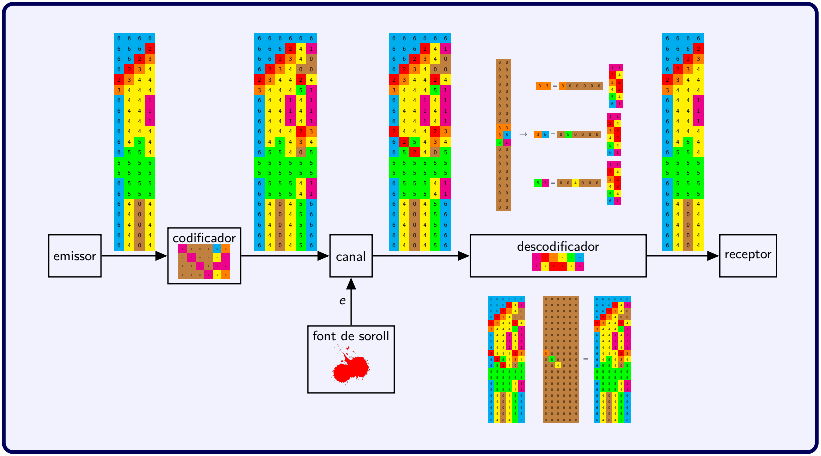
I descodifiquem per la part sistemàtica.

6	6	6	6	6	6
6	6	6	2	4	1
6	6	2	3	4	0
6	2	3	4	0	0
2	3	4	4	2	4
3	4	4	4	5	1
6	4	4	1	4	1
6	4	4	1	4	1
6	4	4	1	4	1
6	4	4	4	2	3
6	4	5	4	3	4
6	5	5	4	0	5
5	5	5	5	5	5
5	5	5	5	5	5
6	5	5	5	4	1
6	5	5	5	4	1
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6

$\rightarrow$

6	6	6	6
6	6	6	2
6	6	2	3
6	2	3	4
2	3	4	4
3	4	4	4
6	4	4	1
6	4	4	1
6	4	4	1
6	4	4	4
6	4	5	4
6	5	5	4
5	5	5	5
5	5	5	5
6	5	5	5
6	5	5	5
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4

Un codi Reed-Solomon



	Codis de Reed-Solomon	***Codis algebraico-geomètrics*** (de Goppa)
$\mathbb{Z}_p$	$\mathbb{F}_{q^d} = \mathbb{Z}_q[x]/m(x)$	$\mathcal{X}(\mathbb{F}_{q^d})$
$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 2 & \dots & (q-1) \\ 1^2 & 2^2 & \dots & (q-1)^2 \\ \vdots & \vdots & \vdots & \vdots \\ 1^r & 2^r & \dots & (q-1)^r \end{pmatrix}$	$\begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^0 & \alpha^1 & \dots & \alpha^\ell \\ (\alpha^0)^2 & (\alpha^1)^2 & \dots & (\alpha^\ell)^2 \\ \vdots & \vdots & \vdots & \vdots \\ (\alpha^0)^r & (\alpha^1)^r & \dots & (\alpha^\ell)^r \end{pmatrix}$	$\begin{pmatrix} f_0(P_1) & f_0(P_2) & \dots & f_0(P_n) \\ f_1(P_1) & f_1(P_2) & \dots & f_1(P_n) \\ f_2(P_1) & f_2(P_2) & \dots & f_2(P_n) \\ \vdots & \vdots & \vdots & \vdots \\ f_r(P_!) & f_r(P_2) & \dots & f_r(P_n) \end{pmatrix}$

Codis Reed-Solomon

Els codis Reed-Solomon han estat els més utilitzats històricament i en l'actualitat:

- Emmagatzematge (CD, DVD, etc.)
- Transmissions espacials
- Transmissions mòbils
- Codis QR

Les files d'una matriu de rang màxim G generen un ***codi lineal***.
Diem que G n'és la ***matriu generadora***. Si G és $k \times n$, aleshores n és la ***longitud*** del codi i k és la ***dimensió***.

En l'exemple, $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 \end{pmatrix}$, $n = 6$, $k = 4$.

Una matriu H tal que $G \cdot H^T = 0$, de rang màxim, de $n - k$ files i n columnes s'anomena una ***matriu de control***.

En l'exemple, $H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \end{pmatrix}$

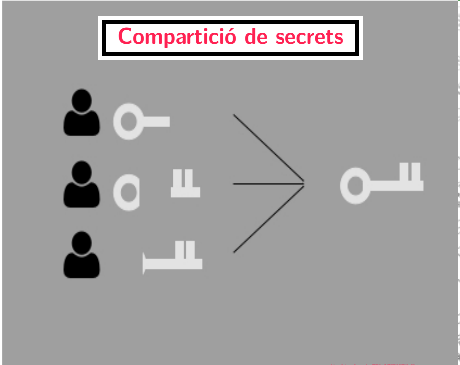
El codi generat per H és el ***codi dual***.

El ***pes*** d'una paraula és el nombre de posicions no nul·les de la paraula.

Teoria de codis

Esteganografia

Compartició de secrets



Emmagatzematge distribuït

Esteganografia

Suposem que volem incrustar el missatge

3	1	4	1	5	6	2	6	5	3	5	6	6	6	6	3	2	3	6	4	6
0	0	0	0	0	3	0	0	0	0	0	2	3	1	3	0	0	0	2	0	0

dins la imatge

6	6	6	6	6	6
6	6	6	2	2	6
6	6	2	3	3	2
6	2	3	4	4	3
2	3	4	4	4	4
3	4	4	4	4	4
6	4	4	1	1	4
6	4	4	1	1	4
6	4	4	1	1	4
6	4	4	4	4	4
6	4	5	4	4	4
6	5	5	4	4	4
5	5	5	5	4	4
5	5	5	5	4	4
6	5	5	5	4	4
6	5	5	5	4	4
6	4	0	4	4	2
6	4	0	4	4	5
6	4	0	4	4	2
6	4	0	4	4	5
6	4	0	4	4	3

Esteganografia

Calculem les síndromes

$$
\begin{pmatrix}
6 & 6 & 6 & 6 & 6 & 6 \\
6 & 6 & 6 & 2 & 2 & 6 \\
6 & 6 & 2 & 3 & 3 & 2 \\
6 & 2 & 3 & 4 & 4 & 3 \\
2 & 3 & 4 & 4 & 4 & 4 \\
3 & 4 & 4 & 4 & 4 & 4 \\
6 & 4 & 4 & 1 & 1 & 4 \\
6 & 4 & 4 & 1 & 1 & 4 \\
6 & 4 & 4 & 1 & 1 & 4 \\
6 & 4 & 4 & 4 & 4 & 4 \\
6 & 4 & 5 & 4 & 4 & 4 \\
6 & 5 & 5 & 4 & 4 & 4 \\
5 & 5 & 5 & 5 & 4 & 4 \\
5 & 5 & 5 & 5 & 4 & 4 \\
6 & 5 & 5 & 5 & 4 & 4 \\
6 & 5 & 5 & 5 & 4 & 4 \\
6 & 4 & 0 & 4 & 4 & 2 \\
6 & 4 & 0 & 4 & 4 & 5 \\
6 & 4 & 0 & 4 & 4 & 2 \\
6 & 4 & 0 & 4 & 4 & 5 \\
6 & 4 & 0 & 4 & 4 & 3
\end{pmatrix}
\cdot
\begin{pmatrix}
1 & 1 \\
2 & 4 \\
3 & 2 \\
4 & 2 \\
5 & 4 \\
6 & 1
\end{pmatrix}
\longrightarrow
\begin{pmatrix}
0 & 0 \\
6 & 4 \\
0 & 5 \\
3 & 5 \\
3 & 1 \\
6 & 6 \\
3 & 5 \\
3 & 5 \\
3 & 5 \\
2 & 2 \\
5 & 4 \\
0 & 1 \\
3 & 2 \\
3 & 2 \\
4 & 3 \\
4 & 3 \\
6 & 6 \\
3 & 2 \\
6 & 6 \\
3 & 2 \\
5 & 0
\end{pmatrix}
$$

Esteganografia

Les restem del missatge a incrustar

$$\begin{pmatrix} 6&6&6&6&6&6\\ 6&6&6&2&2&6\\ 6&6&2&3&3&2\\ 6&2&3&4&4&3\\ 2&3&4&4&4&4\\ 3&4&4&4&4&4\\ 6&4&4&1&1&4\\ 6&4&4&1&1&4\\ 6&4&4&1&1&4\\ 6&4&4&4&4&4\\ 6&4&5&4&4&4\\ 6&5&5&4&4&4\\ 5&5&5&5&4&4\\ 5&5&5&5&4&4\\ 6&5&5&5&4&4\\ 6&5&5&5&4&4\\ 6&4&0&4&4&2\\ 6&4&0&4&4&5\\ 6&4&0&4&4&2\\ 6&4&0&4&4&5\\ 6&4&0&4&4&3 \end{pmatrix} \cdot \begin{pmatrix} 1&1\\ 2&4\\ 3&2\\ 4&2\\ 5&4\\ 6&1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0&0\\ 6&4\\ 0&5\\ 3&5\\ 3&1\\ 6&6\\ 3&5\\ 3&5\\ 3&5\\ 2&2\\ 5&4\\ 0&1\\ 3&2\\ 3&2\\ 4&3\\ 4&3\\ 6&6\\ 3&2\\ 6&6\\ 3&2\\ 5&0 \end{pmatrix}$$

$$\begin{pmatrix} 3&0\\ 1&0\\ 4&0\\ 1&0\\ 5&0\\ 6&3\\ 2&0\\ 6&0\\ 5&0\\ 3&0\\ 5&0\\ 6&2\\ 6&3\\ 6&1\\ 6&3\\ 3&0\\ 2&0\\ 3&0\\ 6&2\\ 4&0\\ 6&0 \end{pmatrix} - \begin{pmatrix} 0&0\\ 6&4\\ 0&5\\ 3&5\\ 3&1\\ 6&6\\ 3&5\\ 3&5\\ 3&5\\ 2&2\\ 5&4\\ 0&1\\ 3&2\\ 3&2\\ 4&3\\ 4&3\\ 6&6\\ 3&2\\ 6&6\\ 3&2\\ 5&0 \end{pmatrix} = \begin{pmatrix} 3&0\\ 2&3\\ 4&2\\ 5&2\\ 2&6\\ 0&4\\ 6&2\\ 3&2\\ 2&2\\ 1&5\\ 0&3\\ 6&1\\ 3&1\\ 3&6\\ 2&0\\ 6&4\\ 3&1\\ 0&5\\ 0&3\\ 1&5\\ 1&0 \end{pmatrix}$$

Els seus *coset leaders* (vectors de mínim pes amb la mateixa síndrome):

3	0
2	3
4	2
5	2
2	6
0	4
6	2
3	2
2	2
1	5
0	3
6	1
3	1
3	6
2	0
6	4
3	1
0	5
0	3
1	5
1	0

$\xrightarrow{\textit{coset leaders}}$

1	0	3	0	0	0
0	0	0	0	6	0
0	0	0	1	0	0
0	0	0	0	0	2
0	0	3	0	0	0
1	0	0	5	0	0
0	0	0	0	4	0
0	0	1	0	0	0
2	0	0	0	0	0
0	0	0	0	3	0
1	0	0	0	4	0
0	0	0	0	0	1
0	0	0	0	2	0
0	5	0	0	0	0
1	0	0	0	0	6
0	0	2	0	0	0
0	0	0	0	2	0
1	0	2	0	0	0
1	0	0	0	4	0
0	0	0	0	3	0
2	3	0	0	0	0

L'*estegoimatge* serà

$$
\begin{pmatrix}
6&6&6&6&6&6\\
6&6&6&2&2&6\\
6&6&2&3&3&2\\
6&2&3&4&4&3\\
2&3&4&4&4&4\\
3&4&4&4&4&4\\
6&4&4&1&1&4\\
6&4&4&1&1&4\\
6&4&4&1&1&4\\
6&4&4&4&4&4\\
6&4&5&4&4&4\\
6&5&5&4&4&4\\
5&5&5&5&4&4\\
5&5&5&5&4&4\\
6&5&5&5&4&4\\
6&5&5&5&4&4\\
6&4&0&4&4&2\\
6&4&0&4&4&5\\
6&4&0&4&4&2\\
6&4&0&4&4&5\\
6&4&0&4&4&3
\end{pmatrix}
+
\begin{pmatrix}
1&0&3&0&0&0\\
0&0&0&0&6&0\\
0&0&0&1&0&0\\
0&0&0&0&0&2\\
0&0&3&0&0&0\\
1&0&0&5&0&0\\
0&0&0&0&4&0\\
0&0&1&0&0&0\\
2&0&0&0&0&0\\
0&0&0&0&3&0\\
1&0&0&0&4&0\\
0&0&0&0&0&1\\
0&0&0&0&2&0\\
0&5&0&0&0&0\\
1&0&0&0&0&6\\
0&0&2&0&0&0\\
0&0&0&0&2&0\\
1&0&2&0&0&0\\
1&0&0&0&4&0\\
0&0&0&0&3&0\\
2&3&0&0&0&0
\end{pmatrix}
=
\begin{pmatrix}
0&6&2&6&6&6\\
6&6&6&2&1&6\\
6&6&2&4&3&2\\
6&2&3&4&4&5\\
2&3&0&4&4&4\\
4&4&4&2&4&4\\
6&4&4&1&5&4\\
6&4&5&1&1&4\\
1&4&4&1&1&4\\
6&4&4&4&0&4\\
0&4&5&4&1&4\\
6&5&5&4&4&5\\
5&5&5&5&6&4\\
5&3&5&5&4&4\\
0&5&5&5&4&3\\
6&5&0&5&4&4\\
6&4&0&4&6&2\\
0&4&2&4&4&5\\
0&4&0&4&1&2\\
6&4&0&4&0&5\\
1&0&0&4&4&3
\end{pmatrix}
$$

Esteganografia

Observem que si ara multipliquem l'*estegoimatge* per H obtenim:

$$
\begin{pmatrix}
0 & 6 & 2 & 6 & 6 & 6 \\
6 & 6 & 6 & 2 & 1 & 6 \\
6 & 6 & 2 & 4 & 3 & 2 \\
6 & 2 & 3 & 4 & 4 & 5 \\
2 & 3 & 0 & 4 & 4 & 4 \\
4 & 4 & 4 & 2 & 4 & 4 \\
6 & 4 & 4 & 1 & 5 & 4 \\
6 & 4 & 5 & 1 & 1 & 4 \\
1 & 4 & 4 & 1 & 1 & 4 \\
6 & 4 & 4 & 4 & 0 & 4 \\
0 & 4 & 5 & 4 & 1 & 4 \\
6 & 5 & 5 & 4 & 4 & 5 \\
5 & 5 & 5 & 5 & 6 & 4 \\
5 & 3 & 5 & 5 & 4 & 4 \\
0 & 5 & 5 & 5 & 4 & 3 \\
6 & 5 & 0 & 5 & 4 & 4 \\
6 & 4 & 0 & 4 & 6 & 2 \\
0 & 4 & 2 & 4 & 4 & 5 \\
0 & 4 & 0 & 4 & 1 & 2 \\
6 & 4 & 0 & 4 & 0 & 5 \\
1 & 0 & 0 & 4 & 4 & 3
\end{pmatrix}
\cdot
\begin{pmatrix}
1 & 1 \\
2 & 4 \\
3 & 2 \\
4 & 2 \\
5 & 4 \\
6 & 1
\end{pmatrix}
\longrightarrow
\begin{pmatrix}
3 & 0 \\
1 & 0 \\
4 & 0 \\
1 & 0 \\
5 & 0 \\
6 & 3 \\
2 & 0 \\
6 & 0 \\
5 & 0 \\
3 & 0 \\
5 & 0 \\
6 & 2 \\
6 & 3 \\
6 & 1 \\
6 & 3 \\
3 & 0 \\
2 & 0 \\
3 & 0 \\
6 & 2 \\
4 & 0 \\
6 & 0
\end{pmatrix}
$$

Esteganografia

Volem incrustar un missatge m de r símbols en una coberta c de n símbols.

Utilitzem un codi de longitud n i dimensió $k = n - r$.

L'emissor crea una paraula que tingui com a síndrome el missatge m.

El receptor obté m multiplicant el missatge rebut per H.

Volem incrustar un missatge m de r símbols en una coberta c de n símbols.

Utilitzem un codi de longitud n i dimensió $k = n - r$.

L'emissor crea una paraula que tingui com a síndrome el missatge m.

El receptor obté m multiplicant el missatge rebut per H.

Per incrustar el missatge m de longitud r de manera imperceptible, transformem c en

$$c' = c + CosetLeader(m - H \cdot c).$$

Volem incrustar un missatge m de r símbols en una coberta c de n símbols.

Utilitzem un codi de longitud n i dimensió $k = n - r$.

L'emissor crea una paraula que tingui com a síndrome el missatge m.

El receptor obté m multiplicant el missatge rebut per H.

Per incrustar el missatge m de longitud r de manera imperceptible, transformem c en

$$c' = c + CosetLeader(m - H \cdot c).$$

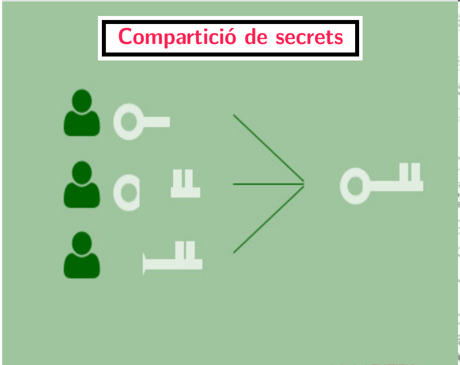
Observem que

- La síndrome de c' és m,
- c i c' són molt semblants
  (c' és el vector més semblant a c d'entre els que tenen síndrome m).

Teoria de codis

Esteganografia

Compartició de secrets



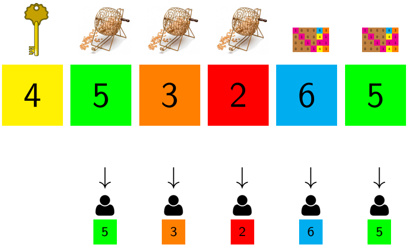
Emmagatzematge distribuït

4

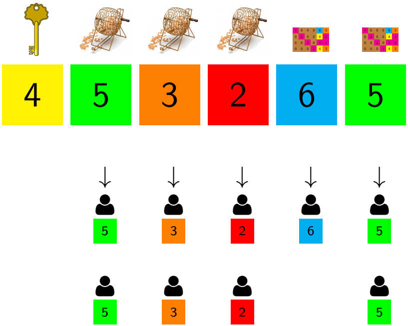
4	5	3	2

Compartició de secrets

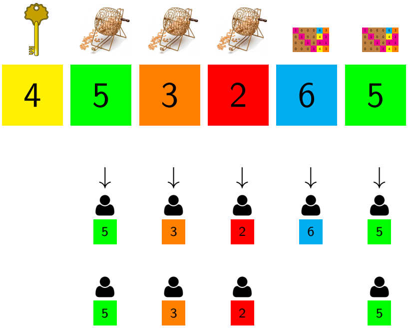
4	5	3	2	6	5


4
5
3
2
6
5
5
3
2
6
5

Compartició de secrets

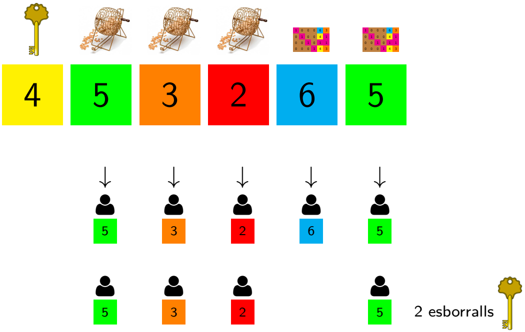


Compartició de secrets

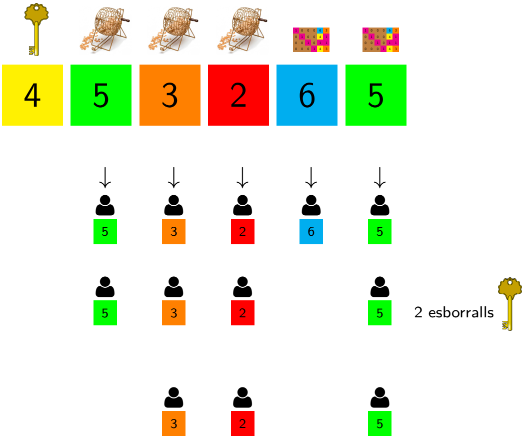


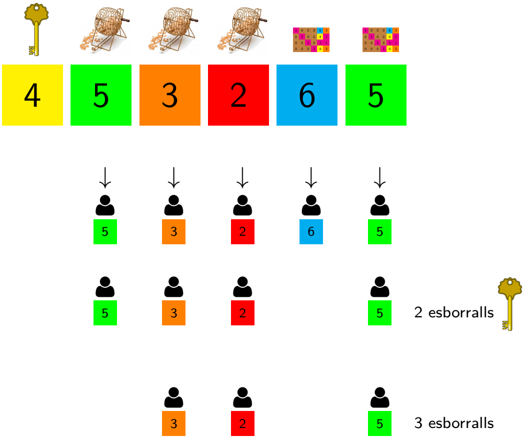
2 esborralls

Compartició de secrets

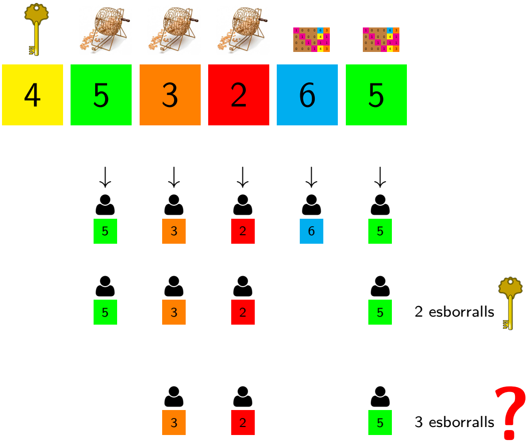


Compartició de secrets




4
5
3
2
6
5
5
3
2
6
5
5
3
2
5
2 esborralls
3
2
5
3 esborralls

Compartició de secrets



Esquema de Massey:

Considerem un codi lineal C de longitud n i dimensió k.

La seva matriu generadora tindrà una submatriu $k \times k$ formada per columnes linealment independents. Suposem que aquesta submatriu es troba en les posicions $i_0, \dots, i_{k-1}$.

Definim una paraula c del codi de la manera següent:

- c_{i_0} = secret
- c_{i_1} = valor aleatori, $\dots$ $c_{i_{k-1}}$ = valor aleatori,
- c_j amb $j \neq i_0, \dots, i_{k-1}$ els únics valors possibles donats per les condicions prèvies juntament amb $c \in C$.

Distribuïm $c_{i_1}, \dots, c_{i_{n-1}}$ entre els/les participants, assignant una component a cadascun/a d'ells/elles.

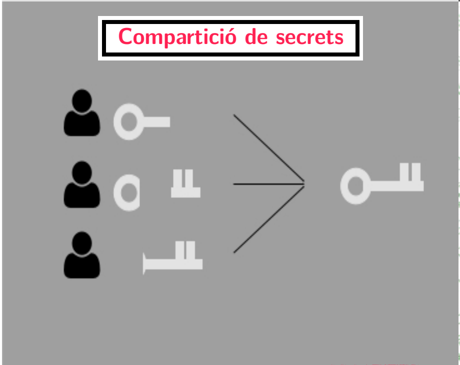
Suposem que existeix una paraula h del codi dual tal que $h_{i_0} = 1$. Sabem que $c \cdot h = 0$. D'aquí deduïm el secret c_{i_0} si obtenim tots els valors c_j tals que $h_j \neq 0$. En efecte,

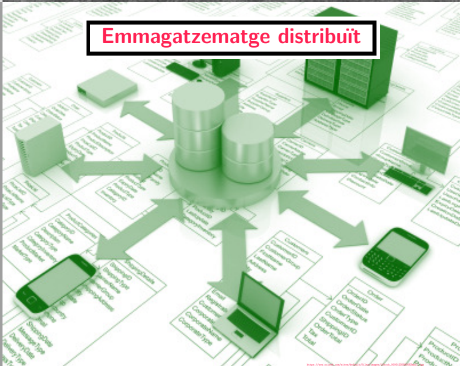
$$c_{i_0} = \sum_{j \neq i_0} h_j c_j = \sum_{j \neq i_0, h_j \neq 0} h_j c_j.$$

Els conjunts minimals de participants que poden obtenir el secret (*estructura d'accés*) corresponen a les paraules del codi dual de pes mínim d'entre les que tenen $h_{i_0} = 1$.

Els codis pels que qualsevol conjunt de k posicions pertany a l'estructura d'accés s'anomenen codis MDS (*maximum distance separable*).

Teoria de codis





Emmagatzematge distribuït

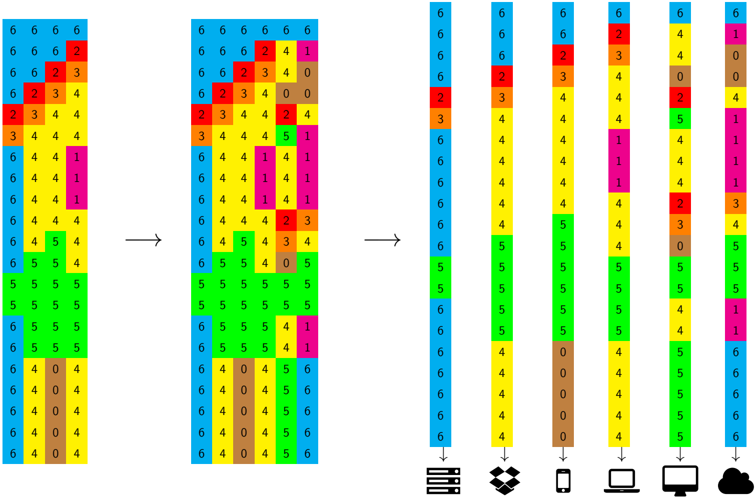
6	6	6	6
6	6	6	2
6	6	2	3
6	2	3	4
2	3	4	4
3	4	4	4
6	4	4	1
6	4	4	1
6	4	4	1
6	4	4	4
6	4	5	4
6	5	5	4
5	5	5	5
5	5	5	5
6	5	5	5
6	5	5	5
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4

6	6	6	6
6	6	6	2
6	6	2	3
6	2	3	4
2	3	4	4
3	4	4	4
6	4	4	1
6	4	4	1
6	4	4	1
6	4	4	4
6	4	5	4
6	5	5	4
5	5	5	5
5	5	5	5
6	5	5	5
6	5	5	5
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4
6	4	0	4

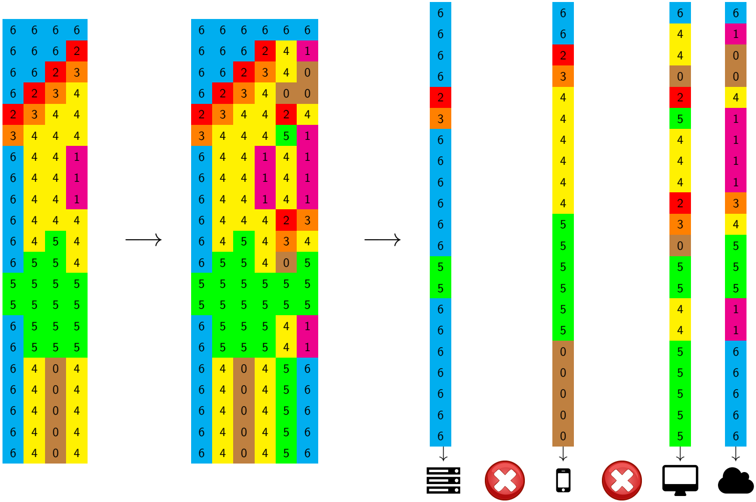
$\longrightarrow$

6	6	6	6	6	6
6	6	6	2	4	1
6	6	2	3	4	0
6	2	3	4	0	0
2	3	4	4	2	4
3	4	4	4	5	1
6	4	4	1	4	1
6	4	4	1	4	1
6	4	4	1	4	1
6	4	4	4	2	3
6	4	5	4	3	4
6	5	5	4	0	5
5	5	5	5	5	5
5	5	5	5	5	5
6	5	5	5	4	1
6	5	5	5	4	1
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6
6	4	0	4	5	6

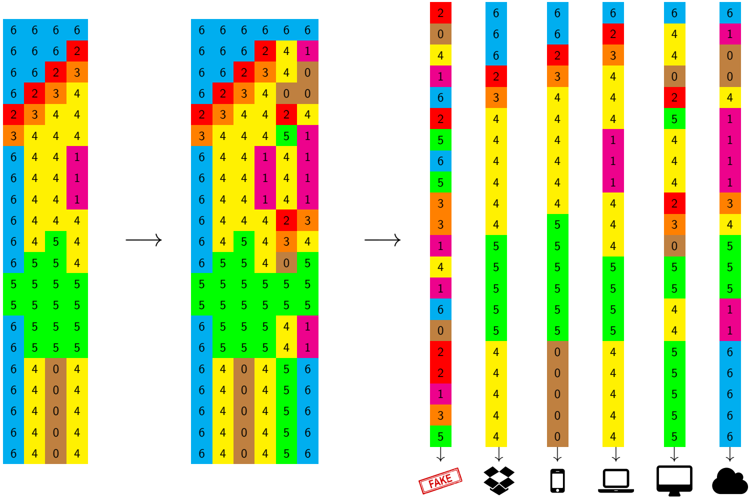
Emmagatzematge distribuït



Emmagatzematge distribuït



Emmagatzematge distribuït



Podem codificar la informació que volem emmagatzemar en paraules d'un codi de longitud igual al nombre de dispositius.

Emmagatzemem en cada dispositiu tots els símbols corresponents a una mateixa posició de les paraules.

Si un dispositiu (o un nombre petit de dispositius) deixa de respondre, encara podem **recuperar la informació perduda** utilitzant la informació emmagatzemada en els altres dispositius (correcció d'**esborralls**).

Si un dispositiu (o un nombre petit de dispositius) dona una informació equivocada, encara podem **corregir la informació modificada** utilitzant la informació emmagatzemada en els altres dispositius (correcció d'**errors**).

La quantitat d'informació emmagatzemada augmenta respecte la informació original en una proporció de $\frac{n-k}{n}$.

Codificació de la informació

Maria Bras-Amorós

UNIVERSITAT ROVIRA i VIRGILI

13 de març del 2021