La matematica di ogni giorno

Fernando Rodriguez Villegas

ICTP

Jan 2015

Messaggi

- Alice vuole mandare un messaggio a Bob

Messaggi

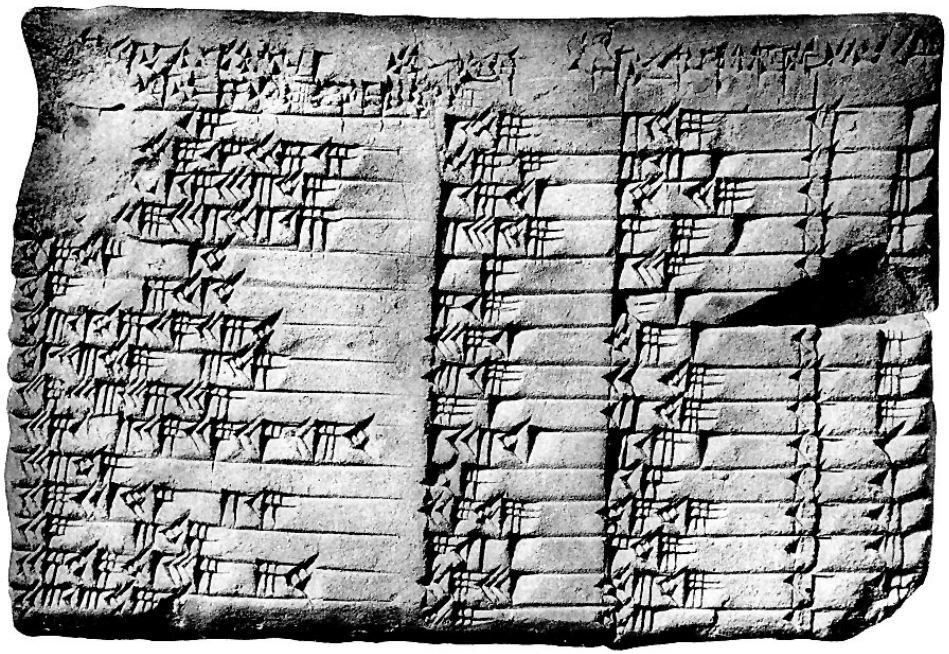
- Alice vuole mandare un messaggio a Bob
- *Tu mi devi* 35 *euro!*

Messaggi

- Alice vuole mandare un messaggio a Bob
- *Tu mi devi* 35 *euro!*
- Codificazione/Decodificazione

Messaggi

- Alice vuole mandare un messaggio a Bob
- *Tu mi devi* 35 *euro!*
- Codificazione/Decodificazione
- Babilonia $\sim$ 1800 BC



Messaggi

- Trasmissione:

$$A \mapsto B$$

Messaggi

- Trasmissione:

$$A \mapsto B$$

- 

Problema 1

- Errori nella trasmissione

Problema 1

- Errori nella trasmissione
- *Grazia, impossibile giustiziarlo!*

Problema 1

- Errori nella trasmissione
- *Grazia, impossibile giustiziarlo!*
- *Grazia impossibile, giustiziarlo!*

Problema 2

- Spie

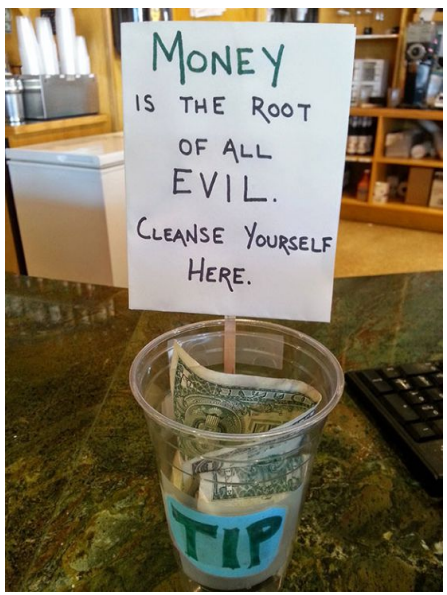
Problema 2

- Spie
- 

Ambiguità

-

Ambiguità

- 

Ambiguità

- *We like tipping customers*

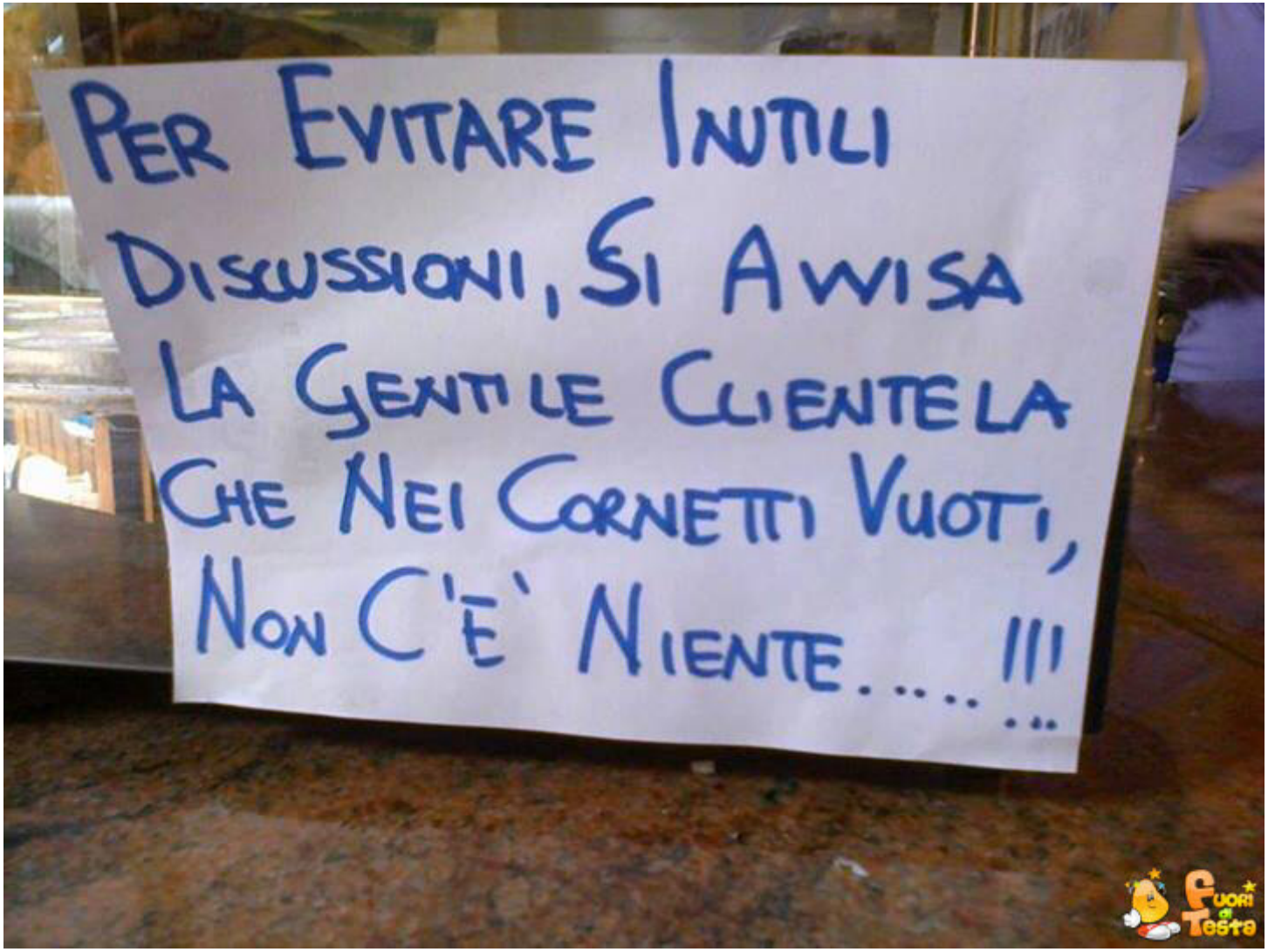
Ambiguità

- *We like tipping customers*
- `Google translate`

Ambiguità

- *We like tipping customers*
- `Google translate`
- *Ci piace ribaltamento clienti*

Contenuto


PER EVITARE INUTILI
DISCUSSIONI, SI AVVISA
LA GENTILE CLIENTELA
CHE NEI CORNETTI VUOTI,
NON C'È NIENTE.....!!!
Fuori di Testa

Numero binario

Decimale	*Binario*
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
...	...

TV circa 1950

$$\begin{array}{lll} \rightarrow & 0111 & \rightarrow 7 \\ \rightarrow & 1000 & \rightarrow 8 \end{array}$$

$$
\begin{array}{lll}
\rightarrow & 0111 & \rightarrow 7 \\
 & 011\underline{0} & \rightarrow 6 \\
\rightarrow & 1000 & \rightarrow 8
\end{array}
$$

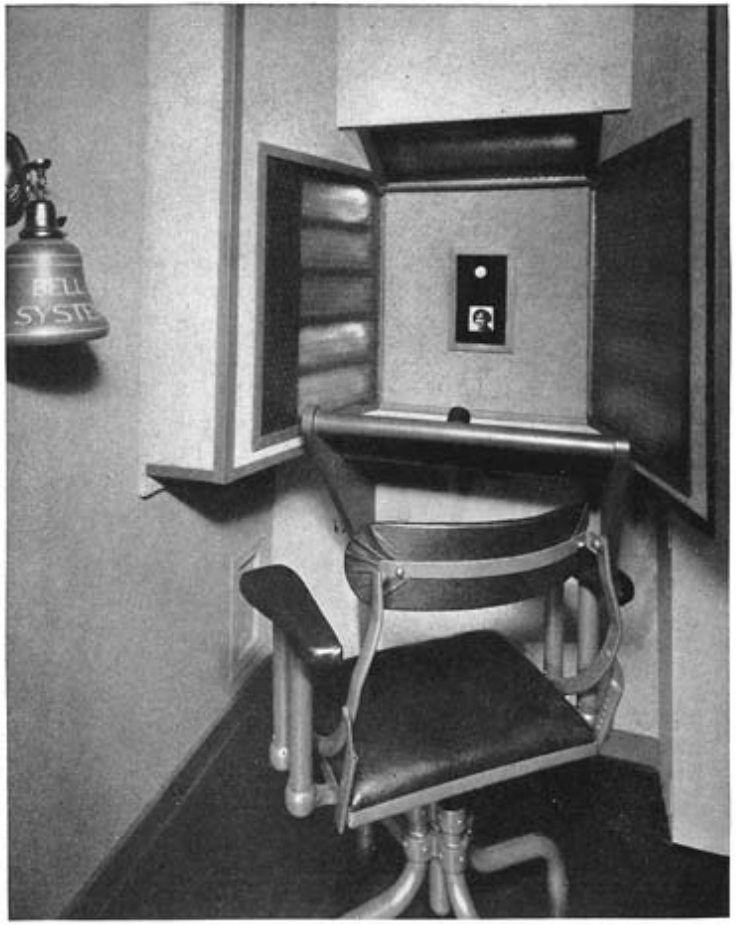
$$
\begin{array}{lll}
\rightarrow & 0111 & \rightarrow 7 \\
 & 0110 & \rightarrow 6 \\
 & 01\underline{0}0 & \rightarrow 4 \\
\rightarrow & 1000 & \rightarrow 8
\end{array}
$$

$$
\begin{array}{lll}
\rightarrow & 0111 & \rightarrow 7 \\
 & 0110 & \rightarrow 6 \\
 & 0100 & \rightarrow 4 \\
 & 0\underline{0}00 & \rightarrow 0 \\
\rightarrow & 1000 & \rightarrow 8
\end{array}
$$

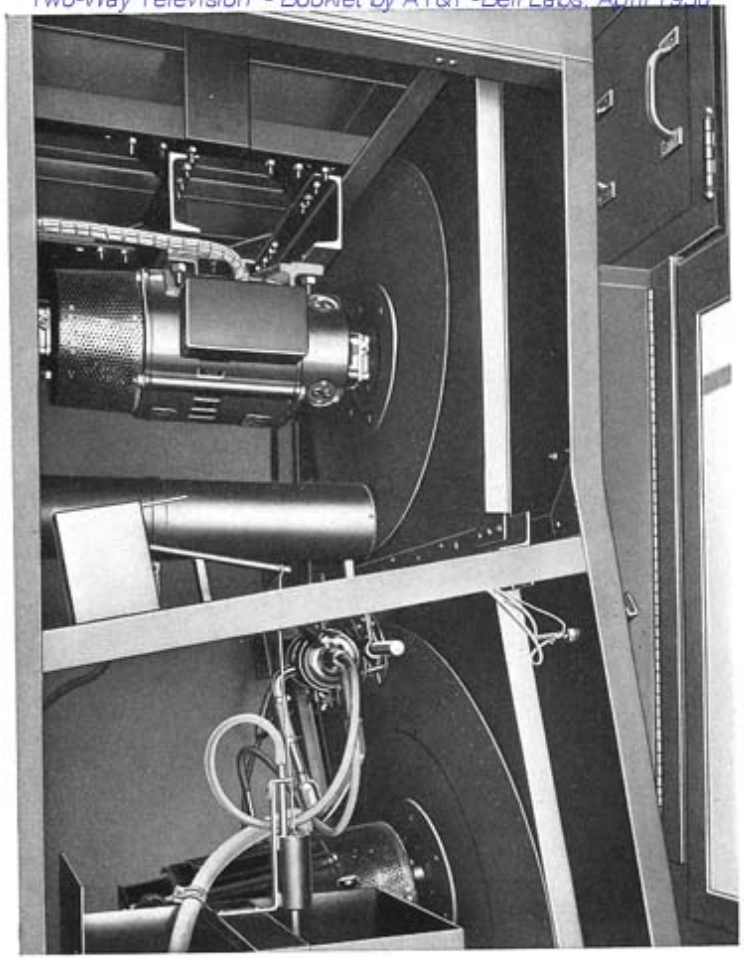
$$
\begin{array}{lll}
\rightarrow & 0111 & \rightarrow 7 \\
 & 0110 & \rightarrow 6 \\
 & 0100 & \rightarrow 4 \\
 & 0000 & \rightarrow 0 \\
\rightarrow & \underline{1}000 & \rightarrow 8
\end{array}
$$

FRANK GRAY and A. L. Johnsrud in television booth. Behind the glass panels at sides and top are the photo-electric cells.

D. G. BLATTNER and L. G. Bostwick inspecting microphone and loud speaker, which are ordinarily concealed.



INTERIOR of television booth showing position of incoming image and, just above it, the hole through which the scanning beam is projected.

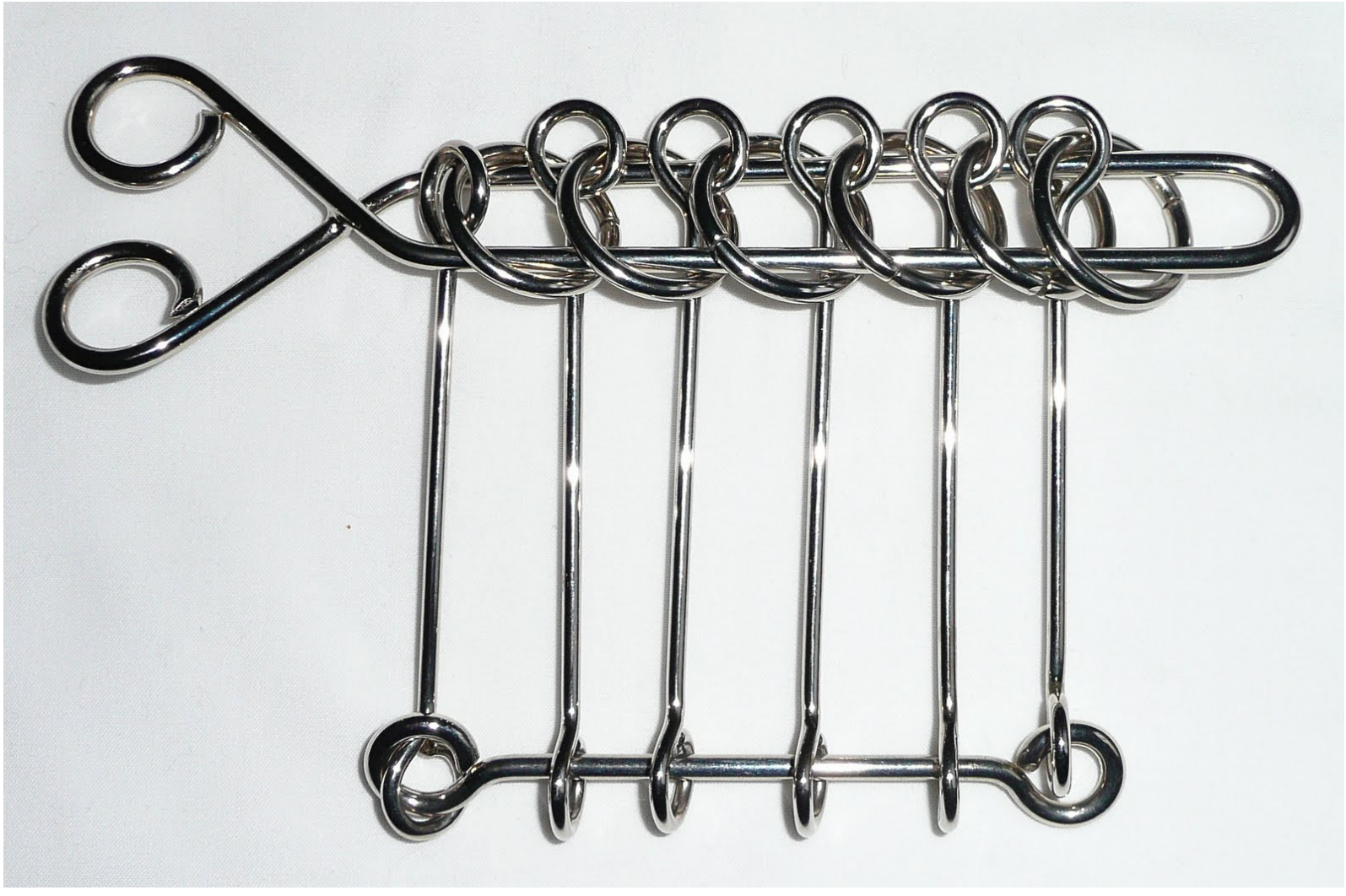


SIDE view of synchronous motors, scanning discs and water-cooled neon lamp.

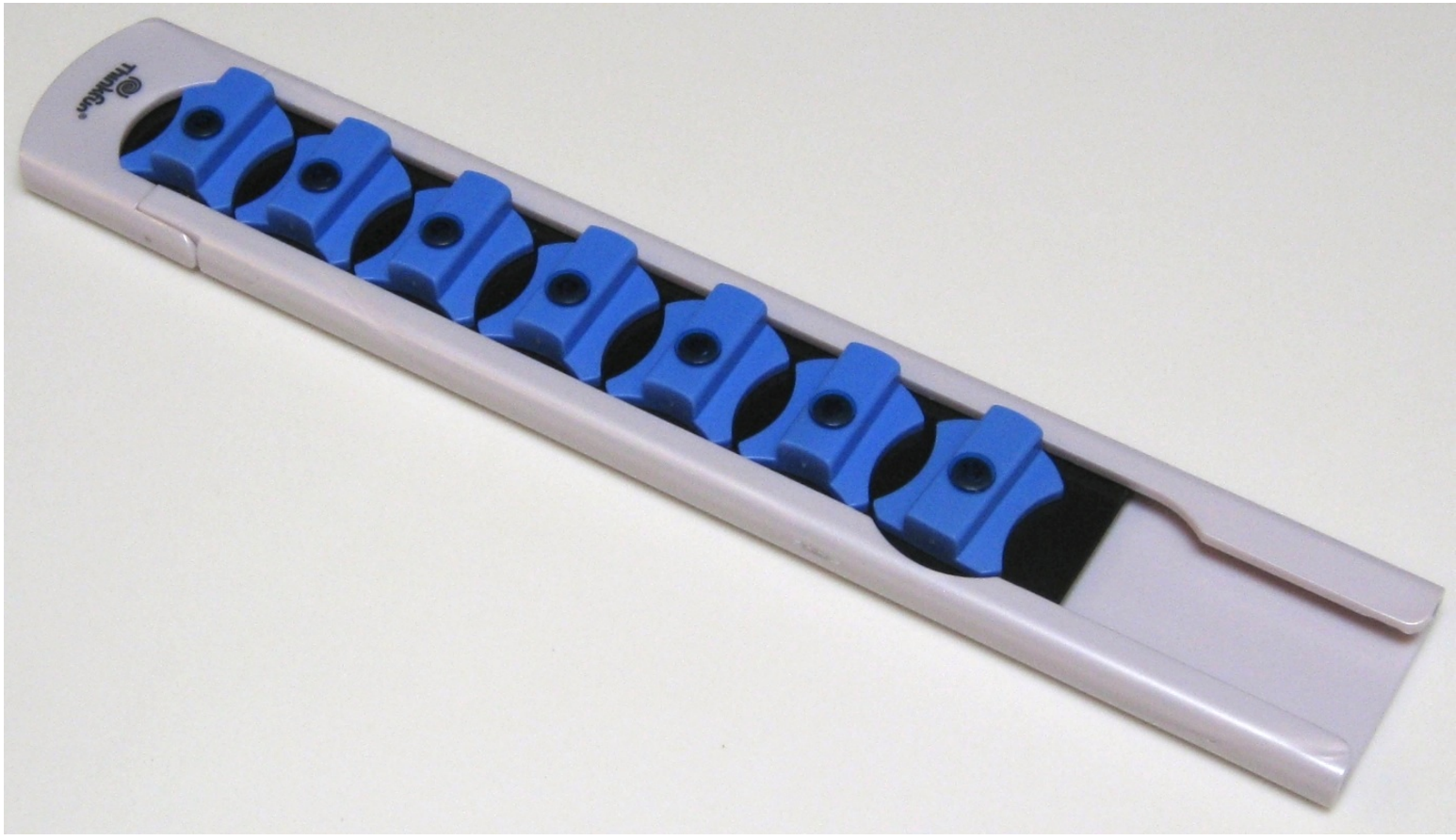
Codice Gray

Decimale	*Gray*
0	0000
1	0001
2	0011
3	0010
4	0110
5	0111
6	0101
7	0100
8	1100
9	1101
...	...

Rompicapo 1



Rompicapo 2



Condividere un segreto

- Alice e Bob vogliono condividere un segreto.

Condividere un segreto

- Alice e Bob vogliono condividere un segreto.
- Diffie-Hellman key-exchange (1975)

Condividere un segreto

- Alice e Bob vogliono condividere un segreto.
- Diffie-Hellman key-exchange (1975)
- Prendiamo g, generatore di un gruppo G.

Condividere un segreto

- Alice e Bob vogliono condividere un segreto.
- Diffie-Hellman key-exchange (1975)
- Prendiamo g, generatore di un gruppo G.
- 

Condividire un segreto

- Alice prende suo numero segreto a.

Condividire un segreto

- Alice prende suo numero segreto a.
- Bob prende suo numero segreto b.

Condividere un segreto

- Alice manda a Bob: $x := g^a$.

Condividere un segreto

- Alice manda a Bob: $x := g^a$.
- Bob manda ad Alice: $y := g^b$.

Condividere un segreto

- Alice manda a Bob: $x := g^a$.
- Bob manda ad Alice: $y := g^b$.
- Alice calcola: y^a.

Condividere un segreto

- Alice manda a Bob: $x := g^a$.
- Bob manda ad Alice: $y := g^b$.
- Alice calcola: y^a.
- Bob calcola: x^b.

Condividere un segreto

- Alice manda a Bob: $x := g^a$.
- Bob manda ad Alice: $y := g^b$.
- Alice calcola: y^a.
- Bob calcola: x^b.
- Segreto in comune

$$x^b = (g^a)^b$$

Condividere un segreto

- Alice manda a Bob: $x := g^a$.
- Bob manda ad Alice: $y := g^b$.
- Alice calcola: y^a.
- Bob calcola: x^b.
- Segreto in comune

$$x^b = (g^a)^b = g^{ab}$$

Condividere un segreto

- Alice manda a Bob: $x := g^a$.
- Bob manda ad Alice: $y := g^b$.
- Alice calcola: y^a.
- Bob calcola: x^b.
- Segreto in comune

$$x^b = (g^a)^b = g^{ab} = (g^b)^a$$

Condividere un segreto

- Alice manda a Bob: $x := g^a$.
- Bob manda ad Alice: $y := g^b$.
- Alice calcola: y^a.
- Bob calcola: x^b.
- Segreto in comune

$$x^b = (g^a)^b = g^{ab} = (g^b)^a = y^a$$