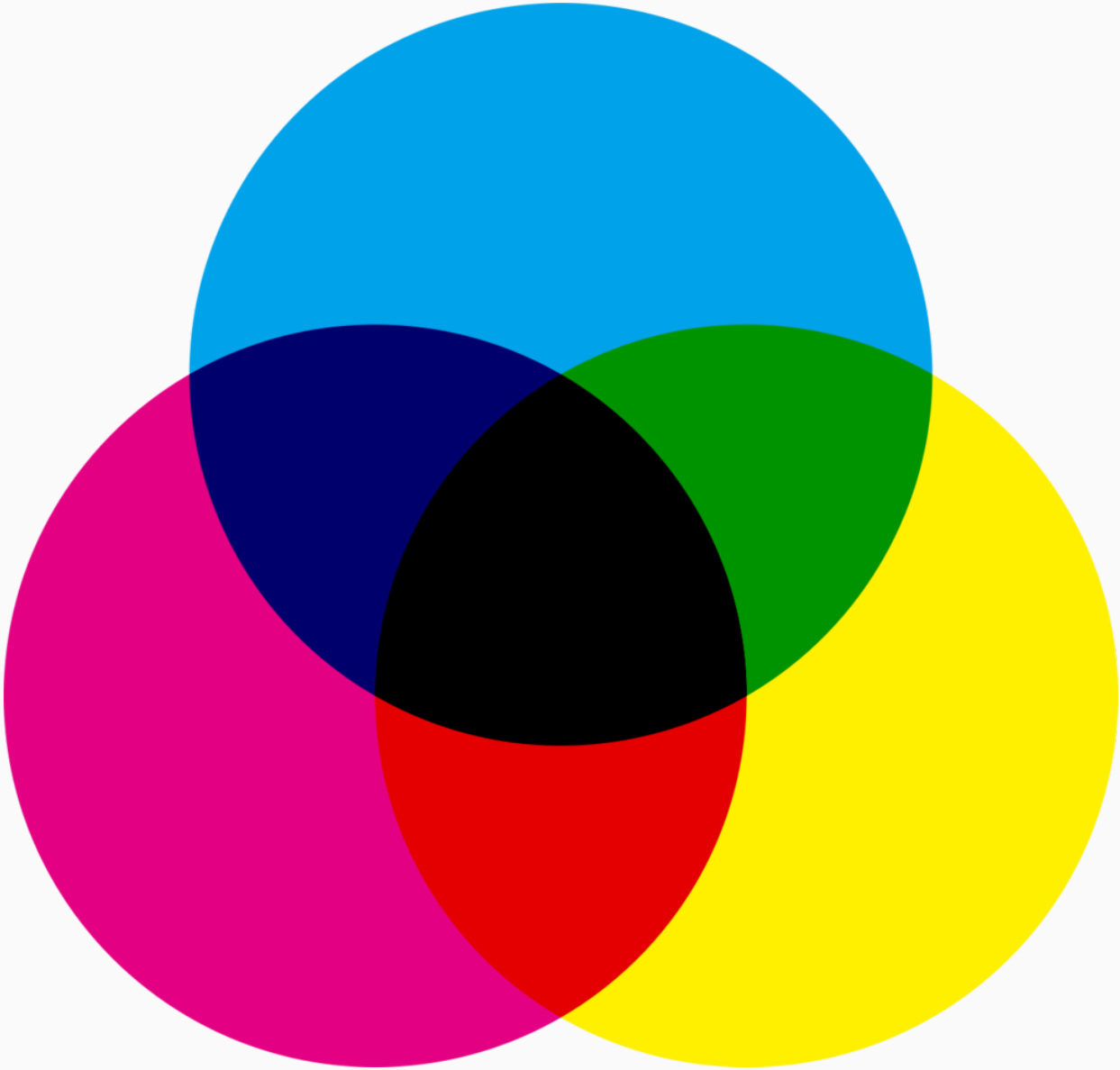
Trenzas y criptografía

Lucía Asencio

Table of contents

Grupos

¿Qué es un grupo?



¿Qué es un grupo?

Tendremos:

- Un conjunto de **elementos**,
- Una **operación**,
- Cada elemento tendrá su **inverso** respecto a la operación,
- Unos pocos **generadores** de todos los elementos

Ejemplos feítos

$(\mathbb{Z}, +)$

Elementos $-\infty \dots 0, 1, 2 \dots \infty$

Operación $n_1 + n_2$

Inversos $1 \to -1,$
$2 \to -2,$
$\vdots$
$n \to -n$

$GL_n(\mathbb{R})$

Elementos $\mathcal{M}$ matrices invertibles

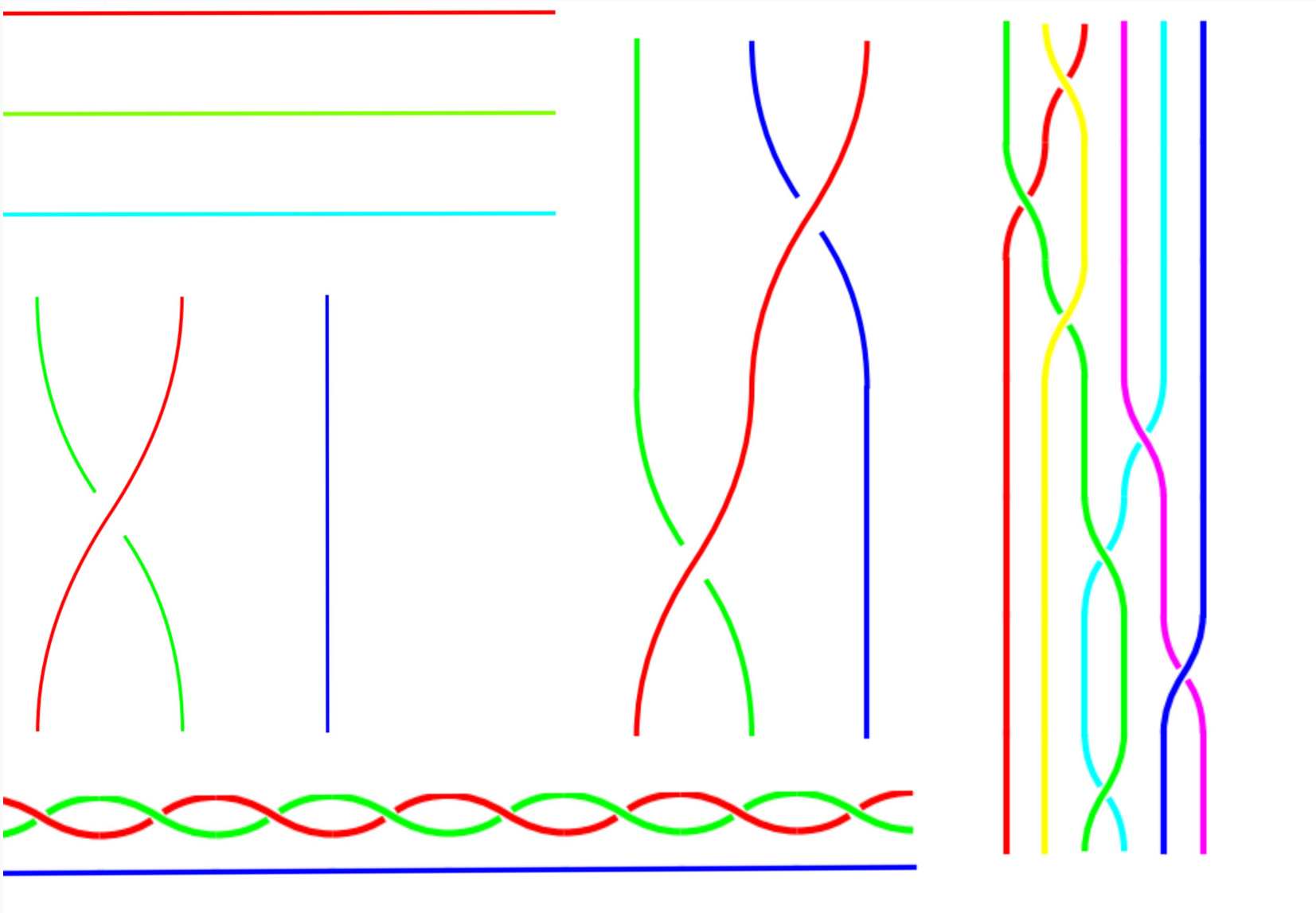
Operación $\mathcal{M}_1 \cdot \mathcal{M}_2$

Inversos $\mathcal{M} \to \mathcal{M}^{-1}$

Trenzas

¿Qué son?

Trenzas cortas, trenzas largas, sencillas, complejas...



Como grupo

Elementos Todas las trenzas del mundo mundial

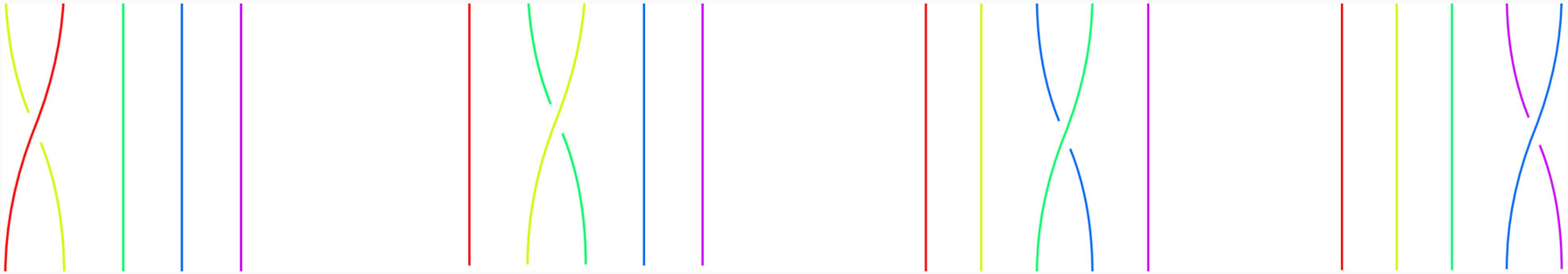
Operación ¡Concatenar!

$\sigma_1 \cdot \sigma_2 = \sigma_1\sigma_2$

$\sigma_1 \cdot \sigma_2 \cdot \sigma_1 = \sigma_1\sigma_2\sigma_1$

Inversos Espejo

Generadores Las mini-trenzas $\sigma_1, \sigma_2 \ldots \sigma_{n-1}$



σ_1 σ_2 σ_3 σ_4

Problemas

1. ¿Cuándo dos trenzas son iguales?
2. ¿Cuándo dos trenzas son conjugadas?

Conjugación

- 2 trenzas a, b
- Conjugar a por $b = \mathit{conjugar}(a, b) = b \cdot a \cdot b^{-1} = c$
- Decimos que a y c están conjugadas

Criptografía

Protocolo de intercambio de claves

Alice $\rightarrow$ clave privada a

$+$

Bob $\rightarrow$ clave privada b

$+$

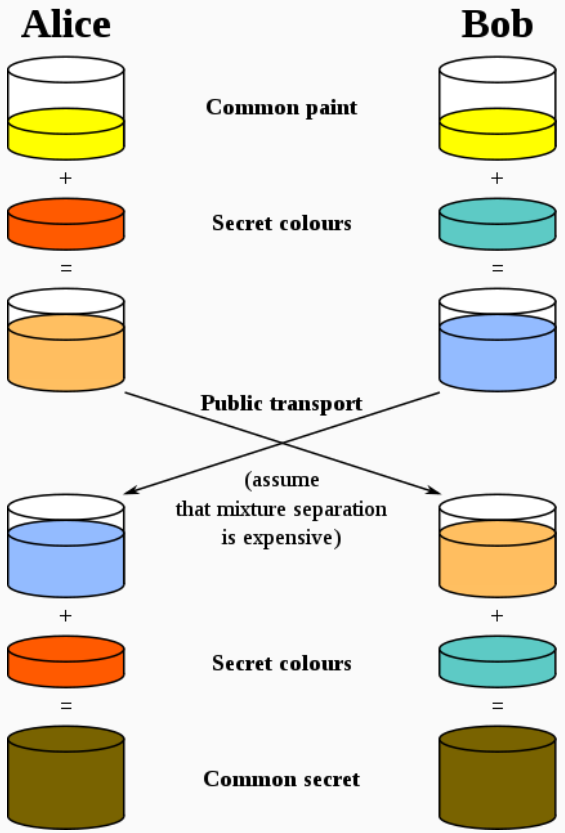
Alice y Bob comparten públicamente información p

$+$

Mensajes A $\leftrightarrow$ B en canal inseguro

$=$

Clave secreta compartida entre Alice y Bob



Protocolo de intercambio de claves... con trenzas

Trenzas de 7 cuerdas ($\equiv$ multiplicar $\sigma_1, \sigma_2, \sigma_3 \ldots \sigma_6$)

Comparten	$p = \{\sigma_1, \sigma_2, \sigma_3\}$
K$^-$ Alice	$a = \sigma_1\sigma_2\sigma_1^{-1}\sigma_3$
K$^-$ Bob	$b = \sigma_3\sigma_2\sigma_1^{-1}\sigma_2^{-1}$
Alice $\rightarrow$ Bob	$\{a\sigma_1 a^{-1}, a\sigma_2 a^{-1}, a\sigma_3 a^{-1}\}$
Bob $\rightarrow$ Alice	$\{b\sigma_1 b^{-1}, b\sigma_2 b^{-1}, b\sigma_3 b^{-1}\}$
Secreto	$aba^{-1}b^{-1}$

¿Y ahora?

The minimal braid problem?

The square-root problem?

E-multiplication?