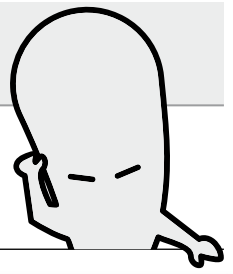
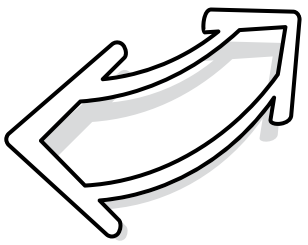
[Contratapa]



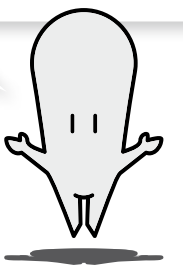
DESAFÍOS MATEMÁTICOS

Si y sólo si

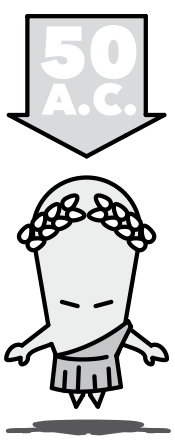


Si y sólo si es un conectivo utilizado para relacionar dos enunciados matemáticos, estableciendo que la validez de cualquiera de ellos depende de la validez del otro. En lenguaje matemático se usa el símbolo ⟺ para representar esta relación.

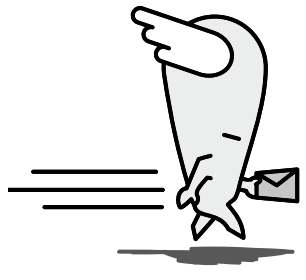
Las transformaciones criptográficas pueden describirse mediante una fórmula matemática, lo que permite automatizar fácilmente las operaciones de cifrado y descifrado mediante la programación de algoritmos ejecutables por una computadora.
En la actualidad, este sistema no se utiliza dado que es extremadamente inseguro. Las computadoras de hoy pueden descifrar mensajes como estos prácticamente al instante. El uso de la matemática, sin embargo, ha conseguido métodos de cifrado que ninguna computadora podría descifrar, aún si trabajara en ello durante siglos. La matemática aporta a la confidencialidad de las comunicaciones mediante métodos que forman parte de lo que se conoce como criptografía. Esta técnica experimentó cambios profundos en los últimos tiempos por el uso masivo de las comunicaciones por medios electrónicos para realizar diversas operaciones de la vida cotidiana, como transacciones bancarias y compras en Internet mediante tarjeta de crédito.



›Julio César conquistó buena parte de Europa para el Imperio Romano alrededor del año 50 antes de Cristo, planeando, coordinando y ejecutando la logística de un movimiento masivo de tropas. En ese entonces, necesitaba avisar a Roma dónde había estado y qué había conquistado. Además, tenía que comunicarse con tropas repartidas en un área geográfica muy extensa, solicitar suministros y nuevas tropas.



Por aquellos tiempos, se usaba un mensajero para comunicarse a través de esas largas distancias. Sin embargo, éste podía ser fácilmente interceptado, y si sus enemigos descubrían cuál iba a ser su próximo movimiento, tal vez podrían derrotarlo.
Para resolver este problema, Julio César ideó varias técnicas para ayudar a mantener sus mensajes indescifrables, excepto para sus aliados de confianza. Una de estas técnicas consistía en sustituir cada letra del alfabeto por la letra que se encuentra tres lugares más a la derecha en el abecedario (volviendo a empezar desde la primera letra después de la última). Por ejemplo, utilizando esta transformación la palabra ENIGMA se transforma en la palabra HPLJOD. Esta técnica dio origen a lo que hoy se llama cifrado del César o transformaciones del César, y se dice que la palabra ENIGMA ha sido encriptada como HPLJOD. Es claro que se puede utilizar un desplazamiento de cualquier cantidad fija de lugares hacia la derecha o izquierda.



Para descifrar o "desencriptar" el mensaje, se debe aplicar la regla "inversa" a la usada en la encriptación, es decir, trasladarse cinco lugares a la izquierda. Usando los 27 símbolos del alfabeto castellano junto a 23 símbolos adicionales que representan el espacio en blanco, los números del 0 al 9, las vocales acentuadas y algunos signos de puntuación, sólo tenemos 49 transformaciones distintas. Por lo tanto, no es difícil descifrar un mensaje interceptado sabiendo que éste se encriptó usando el cifrado de César, aún sin saber cuántos lugares a la derecha o izquierda se realizó el corrimiento. Para hacer esto, se puede simplemente probar con las 49 diferentes transformaciones, o utilizar algunos "trucos" para tratar de encontrar cuántos lugares de corrimiento hubo. Por ejemplo, se podría intentar identificar cuál es el símbolo que representa el espacio en blanco, considerando la longitud posible de las palabras y uno de los símbolos del mensaje cifrado que más se repita. También se podría intentar identificar alguna de las vocales, o las consonantes que puedan repetirse como la "ll" y la "rr".

Por ejemplo, si se utiliza la siguiente tabla como alfabeto para aplicar el cifrado del César:

A B C D E F G H I J K L M N Ñ O P Q R S T U V W X Y Z
Á É Í Ó Ú 0 1 2 3 4 5 6 7 8 9 . , : ¿ ? ¡ !

y se realiza un corrimiento de cinco lugares a la derecha, se obtiene la siguiente correspondencia de letras:

A B C D E F G H I J K L M	N Ñ O P Q R S T U V W X		
F G H I J K L M N Ñ O P Q	R S T U V W X Y Z Á É Í		
Y Z Á É Í Ó Ú 0 1 2 3 4 5	6 7 8 9	. , : ¿ ? ¡ !	
Ó Ú 0 1 2 3 4 5 6 7 8 9	. , : ¿ ? ¡ ! A B C D E		

Así, el mensaje

ATACAREMOS EN 10 DÍAS, REUNIR TROPAS.

se transforma en

FYFHFWJQTX?JR?65?I2FX!?WJZRNW?YWTUFX¡

¿Te animás a descubrir qué dice el siguiente mensaje encriptado?

H V X B Í N B Y Q N Á M J
É B T J É B Y Á X 1 Q U J
É B N M Q L Q X V N É B
M N T B É Q B 2 B É 7 T X
B É Q I

(Solución en página 2)

[+] info

www.fiq.unl.edu.ar/animate
www.facebook.com/culturacientifica

DRA. MARÍA CHARA
› *Docente-investigadora, Departamento de Matemática FIQ-UNL. Becaria Posdoctoral, IMAL-UNL-CONICET.*

LIC. CAROLINA REVUELTA
› *Directora de Cultura Científica FIQ*

GUILLERMO VALAROLO
› *Imagen Cultura Científica FIQ*