

SECRETOS CUÁNTICOS CON CHOCOLATE, POR FAVOR...

Jennifer López Chacón^{1*}, Alfredo Raya Montaño²

¹Facultad de Biología Universidad Michoacana de San Nicolás de Hidalgo, Facultad de ²Ingeniería Eléctrica
Universidad Michoacana de San Nicolás de Hidalgo

*jennifer.lopez@umich.mx



La criptografía es una forma de enviar mensajes secretos para que solo las personas correctas puedan leerlos. En la criptografía clásica, esto se logra usando claves matemáticas, como si fueran candados y llaves. La criptografía cuántica es diferente, porque usa las reglas que rigen los objetos más pequeños del universo, las que hacen que la luz y la energía se comporten de forma especial. Estas reglas permiten que, si alguien trata de mirar un mensaje sin permiso, el mensaje cambia por sí solo y todos pueden saber que alguien quiso espiar.

¿Suena complicado? No te preocupes. Para entenderlo mejor, vamos a jugar.

Te mostraremos cómo funciona la criptografía cuántica usando chocolates y lentes de colores. En nuestro juego, los chocolates representan los mensajes secretos y los lentes de colores simbolizan las formas cuánticas de leerlos. Si alguien usa el lente equivocado o trata de mirar los dos números al mismo tiempo, el "mensaje" cambia y se nota de inmediato que alguien espió. Así, igual que en la criptografía cuántica real, el sistema avisa cuando alguien rompe las reglas, garantizando que el mensaje solo pueda ser entendido por quien tiene la clave correcta.

OBJETIVO DEL JUEGO

Construir un mensaje secreto entre dos jugadores usando chocolates y lentes de colores.

¿QUÉ NECESITAS PARA JUGAR?

El juego puede realizarse mínimo con 2 jugadores (quien envía el mensaje y quien lo recibe), pero también pueden participar más personas si quieren formar equipos. En ese caso, un grupo puede encargarse de enviar los mensajes secretos y el otro de recibirlos y descubrirlos.

AHORA PREGÚNTENSE: ¿POR QUÉ ES IMPORTANTE COOPERAR?

- Una caja o bote con muchos chocolates envueltos en papel oscuro.
 - Toma tus chocolates y escríbeles dos números pequeños, uno con tinta roja y otro con tinta verde.
 - Cada número puede ser 0 o 1, y pueden repetirse (por ejemplo, rojo 0 y verde 0, o rojo 1 y verde 0).
 - Los dos números deben ir en lados opuestos del chocolate, para que al verlo con los lentes especiales, con un color no se note el otro.
- Dos pares de lentes hechos con papel celofán: uno rojo y uno verde.
- Una moneda para cada jugador.
- Banderitas de papel (una roja y una verde por jugador).
- Un cuaderno para anotar los resultados.

¿CÓMO SE JUEGA?



Formen una pareja de juego: Jugador 1 y Jugador 2. El Jugador 1 será quien envíe el mensaje secreto, y Jugador 2 será quien lo reciba. Además, elijan a una tercera persona que será quien lleve el mensaje. La o el mensajero solo lleva el chocolate de un jugador al otro sin mirar los números. Su tarea es asegurarse de que el mensaje llegue intacto y sin ser espiado, igual que en la criptografía cuántica.



2

Jugador 1 lanza su moneda:

- Si sale cara, se pone los lentes verdes.
- Si sale cruz, se pone los lentes rojos.

4

La o el mensajero lleva ese mismo chocolate hasta el Jugador 2. La o el mensajero solo puede revisar que el envoltorio esté cerrado o sin daño, pero no puede mirar ninguno de los números, ni el que vio el Jugador 1 ni el otro color.

6

Jugador 2 observa el chocolate, anota el número y el color de sus lentes.

8

Jueguen varias rondas. Entre más coincidencias haya, más largo será el mensaje secreto.

3

Jugador 1 toma un chocolate y lo observa con sus lentes.

- Solo verá el número del color correspondiente a los lentes que lleva puestos.
- Anota el número y el color.
- Está prohibido mirar el otro número del chocolate. Si lo intenta, el mensajero se queda con ese chocolate (para simular que "alguien interceptó el mensaje").

5

Jugador 2 lanza su moneda y escoge lentes:

- Si sale cara, se pone los lentes verdes.
- Si sale cruz, se pone los lentes rojos.

7

Ahora, Jugador 1 y Jugador 2 levantan su banderita (verde o roja), según el color de los lentes que usaron para ver el chocolate.

- Si los colores coinciden, significa que ambos usaron el mismo tipo de lentes, así que el número se guarda como parte del mensaje secreto.
- Si los colores no coinciden, el número se descarta, porque no se puede usar para crear un mensaje confiable.

¿CUÁNDO SE COMEN LOS CHOCOLATES?

Los chocolates solo se pueden comer cuando el número se guarda en el mensaje secreto, es decir, cuando Jugador 1 y Jugador 2 usan el mismo color de lentes. En ese caso, ambos jugadores ganan juntos el chocolate, porque lograron comunicarse sin errores ni espías, igual que en la criptografía cuántica real. Si los colores no coinciden o alguien rompe las reglas, el chocolate se queda con el mensajero (como señal de que el mensaje fue interceptado).

Figura 1. Pasos del juego “¡Adivina el secreto y gana un chocolate!”. Lanza una moneda para elegir los lentes de color, observa un número escondido en un chocolate, entrégalo a tu compañero, anota el número, comparen los colores y, si coinciden, ¡pueden comer un chocolate!



¿QUÉ APRENDIMOS?

Aprendemos que la información puede viajar escondida y que solo se revela a quienes usan la “forma correcta de mirar”. En el mundo real, la criptografía cuántica funciona igual: solo las personas con la clave correcta pueden leer el mensaje. También descubrimos algo muy importante: Si alguien intenta espionar un mensaje cuántico, deja una huella que todos pueden notar, igual que cuando un jugador intenta ver el número equivocado del chocolate. La ciencia puede proteger secretos, cuidar la información en internet y evitar espías digitales. Y todo empieza entendiendo un número, un color y una buena forma de mirar.



Las computadoras cuánticas son un tipo nuevo de procesadores que funcionan con reglas diferentes a las que usan las computadoras normales. Mientras que una computadora común piensa usando bits (la unidad más pequeña de información) que pueden ser un 0 o un 1, las computadoras cuánticas usan qubits, que pueden ser 0, 1 o los dos a la vez ¡como si el número estuviera jugando a esconderse!

Esto las hace muy poderosas para resolver ciertos problemas muy difíciles, como buscar patrones, predecir el clima o proteger información, igual que en nuestro juego con chocolates. Aunque todavía se están desarrollando, los científicos creen que cuando estén listas, las computadoras cuánticas podrían ayudarnos mucho, por ejemplo, en la medicina, la ciencia y la seguridad de internet.

¡Y TODO EMPIEZA ENTENDIENDO CÓMO FUNCIONA UN SECRETO BIEN GUARDADO!

REFERENCIAS BIBLIOGRÁFICAS

1. Svozil, K. (2006). Puesta en escena de la criptografía cuántica con bolas de chocolate. *American Journal of Physics*, 74 (9), 800-803. <https://doi.org/10.1119/1.2205879>