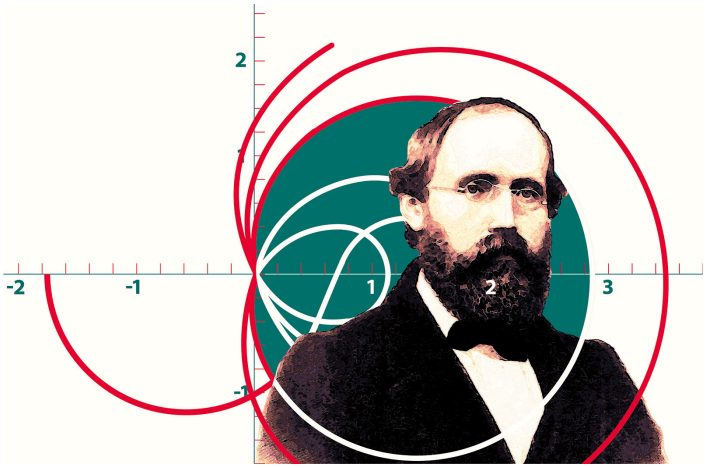
REVISTA
Avance y Perspectiva
Cinvestav




# COMUNICACIÓN INQUEBRANTABLE

*Posted on 5 marzo, 2018*

**Tag:** Volumen 3 - Número 3

Durante nuestra infancia, algunos inventamos un lenguaje secreto que sólo compartimos con los amigos para que los mensajes no fueran descubiertos, debido a que su información era de vital importancia, por ejemplo, el nombre de la chica que nos gustaba o algo embarazoso que no querríamos que nadie más supiera; de modo que aunque alguien interceptara el mensaje, ningún entrometido pudiera entenderlo.

Es decir, desde pequeños conocemos la importancia de mantener una comunicación segura de manera que nadie indeseado conozca nuestros valiosos secretos. Esto se lleva a nuestra vida cotidiana, ya que mandamos y recibimos nuestros datos importantes, como números de tarjetas bancarias, contraseñas de cuentas o datos personales.

Esta idea de privacidad ha sido tan importante que durante la Segunda Guerra Mundial, cualquier persona con una radio podía interceptar los mensajes de uno u otro bando, pero dicha señal era inútil si no sabían descifrarla. De hecho, ese cifrado fue gracias al desarrollo de las máquinas alemanas “Enigma”, las cuales se creían inescrutables, pero se enfrentaron a grandes mentes como Marian Rejewski, en Polonia, y Alan Turing, en Inglaterra, que al crear una máquina capaz de descifrar el código “Enigma”, cambió el rumbo de la guerra y del mundo entero.

Actualmente, la comunicación segura se ha vuelto tan compleja e importante que una de las razones por las que se desea implementar a toda costa el algoritmo de Shor, para factorizar grandes números en las emergentes computadoras cuánticas, es que daría la llave para descifrar grandes cantidades de información alrededor del mundo. Todo esto nos lleva a la pregunta, ¿existe alguna forma de inventar comunicaciones totalmente seguras? La respuesta es sí, a través del cifrado cuántico.

## Cifrado clásico

El cifrado clásico tiene muchas formas y colores, pero el más básico emplea el uso de una llave, que puede ser una palabra como contraseña o un patrón a seguir para la configuración específica de una máquina que tanto el emisor como el receptor poseen. Aunado a la “llave” necesitamos obviamente el “texto sin formato”, el cual es recibido (generalmente en forma de 0 y 1) a través del medio de comunicación que utilizamos para mandar la información por medio de señales eléctricas a lo largo de líneas de cables u ondas radio.

La función de la "llave" es que el "texto sin formato" que cualquier persona puede interceptar les resulte inútil si no saben cómo descifrar este mensaje, de manera similar a como nos es inútil una tarjeta bancaria de la que no recordamos el NIP, una cuenta de internet que no recordamos la contraseña o a los aliados en la Segunda Guerra Mundial que les eran inútiles los mensajes alemanes si no sabían la configuración específica de las máquinas Enigma alemanas.

Máquina Enigma en el Museo Nacional de la Ciencia y Tecnología "Leonardo Da Vinci" en Milán, para su uso, los alemanes cada día asignaban una configuración diferente entre las 10 millones de billones de posibilidades.

## Cifrado cuántico

En 1984, Charles Bennett y Gilles Brassard inventaron el protocolo BB84 para generar "llaves" de seguridad que se aprovecha de propiedades cuánticas. Para explicarlo, existe un ejemplo clásico de dos niños, en este caso Alicia y Beto, ambos muy inteligentes que se comunican entre ellos escribiéndose notitas usando sólo código binario (0 y 1). Cada uno compró un paquete especial de plumones mágicos, el cual contiene dos plumones con tinta invisible roja y verde; además de los plumones, el paquete contiene dos lámparas especiales, una con etiqueta que corresponde a cada uno de los colores de los marcadores.

Lo que hacen los plumones es lo siguiente: cuando escribes en una hoja con cualquiera de los plumones la tinta no se ve (porque son de tinta invisible), si escribes con el plumón verde un 0 o 1 e iluminas esa hoja con la lámpara de etiqueta verde, el número escrito será revelado y se borrará un instante después, pero si iluminas esta nota con la lámpara de etiqueta roja, el mensaje podrá aparecer un 0 o un 1 al azar, con 50 por ciento de posibilidades, y de igual manera se borrará un instante después; de manera similar ocurre con el plumón rojo.

Alicia quiere mandarle un mensaje en binario a Beto con los plumones mágicos que acaban de comprar, para hacerlo se les ocurrió una brillante idea que a continuación se describe:

Alicia escribe cada dígito del mensaje en una hoja separada con uno de los plumones mágicos (el rojo o el verde), sólo ella sabe el dígito y el color de plumón de cada nota. Le manda estas hojas a Beto, y su trabajo es iluminar cada nota con cualquiera de las lámparas al azar, registra el número que vio y la lámpara con la que iluminó la hojita, guardándose Beto esta información para sí mismo.

Al terminar de iluminar y registrar los dígitos, Beto le manda un mensaje a Alicia por Whatsapp (cualquier entrometido puede ver este mensaje) diciéndole cuál lámpara utilizó para iluminar cada nota (sólo le dice a Alicia con que lámpara iluminó, no el número que vio) y Alicia le responde diciéndole qué notas iluminó correctamente; es decir, ella le responde qué notas iluminó con la lámpara correcta, al leer la Beto descarta todos los dígitos que recopiló excepto los que Alicia le dijo que eran correctos y obtiene una tabla como la siguiente:

**TABLA 1**

| Resultados de un ejemplo hipotético de la analogía del protocolo BB84 | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Número de notita | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Plumón utilizado por Alicia | | | | | | | | |
| Número escrito por Alicia | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |
| Lámpara utilizada por Beto para leer | | | | | | | | |
| Número registrado por Beto | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| ¿Fue correcta la lámpara utilizada por Beto? | Sí | No | Sí | No | No | No | Sí | Sí |
| Número que Beto no descarta | 1 | | 1 | | | | 0 | 1 |

Tabla 1

Notemos que todos los dígitos registrados al final por Beto (los que Alicia corroboró que los iluminó con la lámpara correcta) son aquellos dígitos que Alicia escribió y en ninguno de estos debería de haber error. Por desgracia Alicia y Beto perdieron algunos dígitos en el proceso pero repiten este procedimiento con los faltantes hasta completar el mensaje.

Ahora imaginemos una entrometida Eva, quien también tiene un paquete de plumones mágicos e intercepta los mensajes antes de que lleguen a Beto para descifrarlo; notemos que en el momento en que los intercepta, Eva no sabe con qué plumón Alicia escribió cada nota y al iluminarla con cualquiera de las lámparas pierde el mensaje original de Alicia.

Si Eva intenta leer cualquier nota, se borrará y tendrá que falsificar el mensaje de Alicia, donde vemos que si Eva de pura casualidad iluminó la nota con la lámpara correcta, solo tiene que escribir el dígito que vio con el plumón del color de la lámpara para falsificarlo, pero si Eva se equivoca de lámpara (lo cual a priori no sabe), puede errar al enviar la falsificación, porque tiene 50 por ciento de oportunidad de que el dígito que Alicia envió fuera cambiado.

Cuando llegan las notas falsificadas a Beto y él hace su trabajo, los dígitos que no descartó Beto después de la comparación de lámparas con Alicia tendrán errores por ser falsificaciones de Eva (piense detenidamente por qué), a diferencia del caso en el cual nadie interceptó las notas, y vemos que lo único que tienen que hacer Beto y Alicia para ver si alguien interceptó su mensaje es compartir entre ellos por Whatsapp algunos de los dígitos del mensaje que no descarta Beto, compararlos con lo que escribió originalmente Alicia y si

alguno está mal saben con certeza que Eva trató de leer el mensaje. Uno podría argumentar, con justa razón, el caso en el cual Eva tiene una fotocopiadora la cual le permite copiar el mensaje de Alicia sin borrarlo y dejarse una copia para ella, y así enviar el mensaje de Alicia sin modificar y ella analizar la copia para extraer el mensaje, pero aquí es en donde en los sistemas reales cuánticos, como lo son fotones polarizados o espines, la teoría cuántica predice que no existe dicha maquina copiadora1.

Esta tecnología cuántica, aunque suene lejana, no es un sueño, ya que en septiembre de 2017 se realizó la primer videollamada intercontinental cifrada cuánticamente entre las ciudades de Viena y Pekín, convirtiéndola en la más segura del mundo y, así abriendo paso a una nueva forma de comunicarnos donde nuestros mensajes siempre estarán seguros.

**Referencias:**

1. Schumacher, B., Westmoreland M. (2010). Quantum Processes Systems, & Information. Cambridge University Press. Estados Unidos.