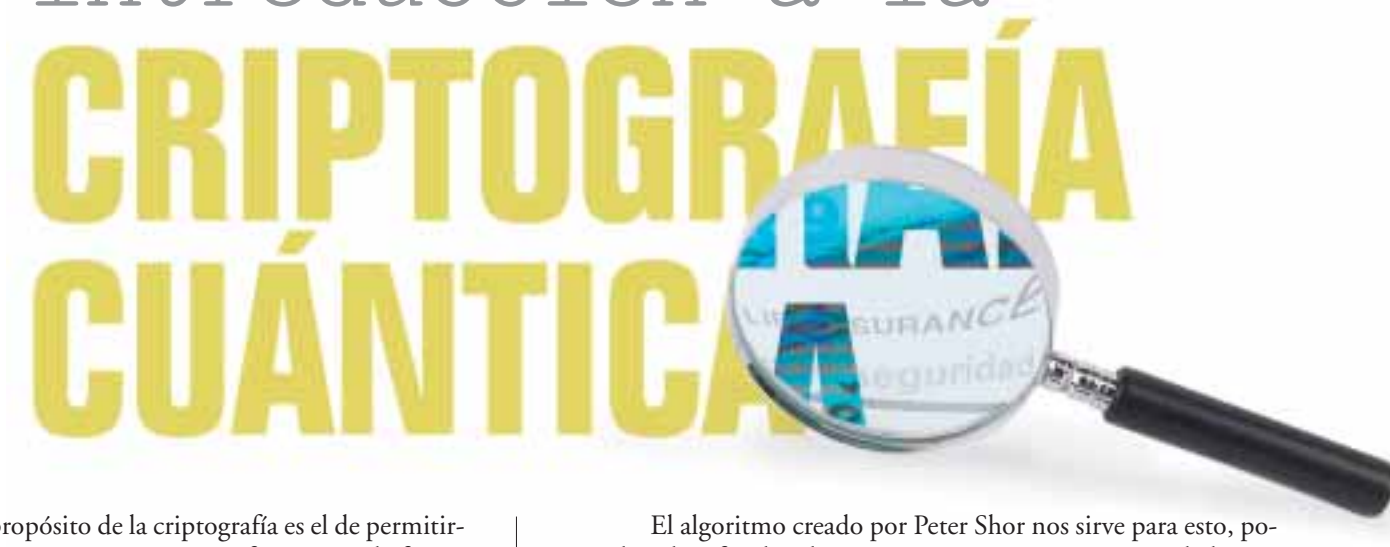
Introducción a la CRIPTOGRAFÍA CUÁNTICA



El propósito de la criptografía es el de permitirnos transmitir nuestra información de forma que aunque alguien la intercepte le sea imposible poder descifrarla. Los métodos criptológicos actuales no son capaces de cumplir al 100% esta tarea, aunque sí son capaces de dificultar bastante el descifrado de la información.

En los algoritmos criptográficos actuales se emplean dos claves, una pública y otra privada. Tal como lo dice su nombre, la clave pública puede ser vista por todos, mientras que la clave privada sólo puede verla su dueño. Estas claves son creadas con un principio matemático muy sencillo, se trata de la facilidad de realizar operaciones en un sentido y la alta dificultad de realizar operaciones en el sentido contrario. Veamos un ejemplo:

• Si quieres elevar al cuadrado el 6, con una operación simple como (6*6) ya tendrías el resultado, que es 36.
• Ahora hagamos lo contrario, trata de sacarle la raíz cuadrada a 6. Esto es más difícil, y requeriría hacer unas cuentas o en su defecto el uso de una calculadora, hacer la operación mentalmente sería algo complejo, sobre todo con números más grandes.

Ahora, si nos ponemos a pensar que en las claves RSA se usan números mucho más grandes, aun usando las computadoras más potentes tomaría miles de años tratar de factorizar una de estas claves.

La computación cuántica cambiará con todo esto, ya que uniendo su capacidad de procesamiento y algoritmos como los creados por Peter Shor y Lov Glover, estas super computadoras serán capaces de factorizar números enormes en fracciones de tiempo de lo que le tomaría a una computadora actual.

El algoritmo creado por Peter Shor nos sirve para esto, podría descifrar las claves RSA en muy poco tiempo. El algoritmo de Glover permite buscar alguna cadena en una lista a velocidades ahora imposibles, en cuestiones criptográficas podría descifrar rápidamente las claves secretas de algoritmos como DES o RC5.

Esto terminaría con la seguridad de nuestras operaciones, ya que cualquier individuo con una computadora cuántica usando estos algoritmos podría descifrar toda nuestra información, afortunadamente hay dos razones para mantener la calma:

1. Aún estamos a al menos 10 años antes de que la tecnología de la computación cuántica se desarrolle de forma adecuada.
2. Las computadoras cuánticas traerán también la existencia de la criptología cuántica, la cual reemplazará los métodos criptográficos actuales.

TEORÍAS DE LO CUÁNTICO

La criptología cuántica se basa en los principios cuánticos de la materia, como los dos estados del átomo o las dos polarizaciones de un fotón. Además de estos dos estados, que son representados por 1 y 0, el átomo se puede encontrar en ambos valores a la vez, aquí aparecen los "qubits". Los qubits son una unidad básica de información cuántica, que representa al 0 o 1 o a ambos valores a la vez.

La base de la criptografía cuántica radica en el principio de incertidumbre de Heisenberg, que nos dice que no es posible saber con exactitud dos variables complementarias, como la posición y la velocidad de una partícula.

El protocolo BB84, sugerido por C. H. Bennet y G. Brassard en 1984, es un ejemplo del uso de la criptografía cuántica. Este ejemplo implica a un emisor y un receptor, el emisor envía fotones en una de estas cuatro polarizaciones: horizontal, vertical, o inclinados, también se le conoce por sus grados, que serian 0, 90, 45 o 135 y representan a: — | / \

A continuación, un pequeño gráfico obtenido desde Google con estas representaciones y algunos valores de bits para facilitar su comprensión.

Secuencia de Alicia	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Secuencia de Bob	+	x	+	+	x	x	+	+	x	+	x	x	+	+
Secuencia de Alicia	1	0	0	1	0	0	1	1	0	0	0	1	0	0

Una vez mencionado esto, analicemos un caso de estudio, con un emisor y un receptor, que tradicionalmente se conocen como Alicia y Bob.

Alicia, con una de estas 4 polarizaciones, le envía a Bob una serie de fotones polarizados de forma aleatoria.

Bob tiene cuatro filtros, en forma de un (+) y un (x) Bob puede filtrar los fotones usando uno de estos dos filtros, pero no puede emplear ambos filtros a la vez. Cuando a Bob le llega esta serie de fotones, Bob elige de forma aleatoria el filtro que va a usar, ya sea (+) o (x), Bob guarda los resultados pero los mantiene ocultos, pero le informa al emisor acerca de los filtros que usó y el emisor le responde diciéndole cuáles filtros fueron correctos.

Después, Alicia compara los resultados con la lista que ella envió originalmente y le dice a Bob, mediante el canal público, en cuáles ocasiones su filtro fue el correcto, pero sin decirle los estados de polarización que ella envió. Si Bob usó un filtro erróneo en alguno de los fotones que Alicia envió, el bit simplemente es descartado. En los casos correctos, se traspasa la información a ceros (0) y unos (1), los cuales son usados para la creación de la clave con la que encriptarán el mensaje en el canal público.

Pero, ¿qué pasa si hay una tercera persona; es decir, un intruso?

Llamemos a nuestro intruso Eve (evil). Aun si Eve interceptó el mensaje tanto en el canal cuántico como en él público, Eve no podrá engañar a Alicia o a Bob ya que su intervención sería detectada fácilmente. Esto se debe a que al medir la polarización de un fotón con el detector equivocado, la polarización del fotón se alterará, lamentablemente esto también impediría la comunicación entre Alicia y Bob, debido a que Eve alteró la polarización de los fotones por el camino.

Ejemplificando, según las teorías cuánticas, Eve tiene 50% de posibilidad de escoger el filtro correcto (al igual que Bob), pero Eve tendría que reenviar a Bob estos fotones para cubrir sus huellas. El problema para Eve sería que aunque Bob tuviera un 50% de probabilidades de concordar con Alicia en cada polarización, ¿qué pasaría cada vez que Eve usase el filtro incorrecto (ocurre en el 50% de los casos)?

Aun en estos casos, la mitad de los fotones pasará a través de los filtros de Bob, pero combinados resulta que el porcentaje de acierto entre Alicia y Bob se reducirá a 25% en presencia de Eve. En estos casos sería obvia la intrusión de una tercera persona y Alicia y Bob desecharían la transmisión.

Otro método para detectar estas intrusiones podría ser si Bob le transmite a Alicia los primeros 50 bits de su clave aleatoria. Si coinciden con los de Alicia entonces sabrán que Eve no los espió y que el canal no tiene ruido (el ruido es otro elemento que podría alterar la polarización de los fotones).

Si coinciden, podrán usar con seguridad el resto de los bits generados; en caso contrario, siempre sabrán que Eve estuvo de intermediaria en la comunicación o que el canal presenta otros problemas.

CONCLUSIÓN

Con esto concluimos nuestra introducción a esta tecnología del futuro, que aun tiene un largo camino que recorrer antes de ser introducida a las masas. El medio más factible para la comunicación cuántica es la fibra óptica, ya que para que el medio funcione de la forma correcta el canal de transmisión no puede tener ruido u otras interferencias. En la actualidad hay experimentos con esta tecnología en Washington y otros lugares importantes del mundo, en el Reino Unido han logrado romper la barrera de los 100 kilómetros de distancia usando fibra óptica. Los países más importantes del mundo están ansiosos por ser los primeros en poder implementar la computación cuántica, ya que les permitiría descifrar los secretos de los demás (algo muy solicitado en el gobierno de cualquier país) y enterarse de los planes de sus enemigos que usen los métodos criptográficos actuales. Aunque existe la duda de si estos gobiernos permitirán a los ciudadanos el uso de esta tecnología, ya que desde ahora existe el temor de que se use para proteger actividades criminales.

Por el momento, lo único que podemos hacer es prepararnos para responderle a la computación cuántica con la criptografía cuántica una vez que estén disponibles estas tecnologías.