M1AC2. Actividad colaborativa 2

Criptografía cuántica

¿Una amenaza real?

GRUPO 1

1. Ane Aretxabaleta Vázquez (Responsable)
2. Cesar Farro (Responsable)
3. Alejandra Montero Fuentes
4. Javier Morillas Domínguez
5. Julián Alonso Ubierna
6. Guadalupe De Jesús Rosales Salinas
7. Alejandro Cortés Rivera

Criptografía de clave pública/clave secreta, & ordenador cuántico. Impacto de un ataque con un ordenador cuántico a los esquemas de la criptografía actual

ANTECEDENTES

Tanto la Criptografía Clásica como la Criptografía Moderna tienen como **objetivo** principal el **cifrado de información**, por medio de métodos matemáticos simples o complejos, para que pueda ser transmitida a un receptor y que solo éste sea capaz de descifrarla.

En la actualidad, los protocolos de comunicaciones utilizados se basan en cifrado de clave pública, firmas digitales, etc. Algunos de los métodos de implementación más conocidos serían RSA o intercambio claves Diffie-Hellman en los que la **seguridad de cada uno de ellos depende de problemas teóricos numéricos.**

FUNCIONAMIENTO CIFRADO SIMÉTRICO

Un **algoritmo de clave secreta**, o algoritmo simétrico, es un algoritmo criptográfico que usa la misma clave para cifrar y descifrar datos. El algoritmo más conocido es el Estándar de encriptación avanzada (AES).

Un ejemplo muy simple de cómo podría funcionar un algoritmo de clave secreta podría ser sustituir la letra en el alfabeto antes de la letra objetivo para cada carácter del mensaje. El texto resultante, "gdkkn", por ejemplo, no tendría sentido para alguien que no supiera el algoritmo utilizado (x-1), pero las partes involucradas en el intercambio lo entenderían como "hola".

El problema con las claves secretas o simétricas es cómo obtener de forma segura las claves secretas para cada extremo del intercambio y mantenerlas seguras después de eso. Por esta razón, a menudo se usa un sistema de claves asimétricas junto con una infraestructura de clave pública (PKI).

FUNCIONAMIENTO CIFRADO ASIMÉTRICO

La criptografía asimétrica se basa en el uso de dos claves: la pública (que está vinculada a la privada, pero que se podrá difundir sin ningún problema a todas las personas interesadas en realizar algún envío de información cifrada al receptor) y la privada (que únicamente la conoce el receptor y no debe de ser revelada nunca). Son utilizados para establecer una comunicación segura por un canal inseguro. Este tipo de sistemas criptográficos usa algoritmos bastante complejos que generan a partir de la frase de paso

(la contraseña) la clave privada y pública que pueden tener un tamaño de 2048bits, por lo que el tiempo necesario para la operación de cifrado y descifrado es superior.

El modo de funcionamiento es proporcionar nuestra clave pública a todo aquel que nos quiera enviar un mensaje confidencial, de tal manera que el emisor lo cifra con la clave pública, y el mensaje sólo puede ser descifrado con la clave privada (que como se ha mencionado anteriormente sólo debería conocer el receptor). Para que la comunicación pueda ser bidireccional, este mismo proceso debería realizarse con dos pares de claves, o una por cada comunicador.

COMPUTACIÓN CUÁNTICA

Una definición directa sería que los ordenadores cuánticos trabajan con QUBITS (unidad de información cuántica), en la que no solo se le aplica un estado sino que se le aplica el concepto onda partícula, lo que puede hacer que un QUBIT se encuentre en varios estados a la vez. Los QUBITS pueden estar relacionados entre sí, por una propiedad quántica denominada **entrelazamiento**, que permite propagar la propiedad de un QUBITS de tener 0 y 1 a su vez combinado y trabajando en el mismo instante con todos los QUBITS con los que esta entrelazado. Es decir, una operación que afecta a unos pocos QUBITS se propagaría en todos los demás. Esto cambia disruptivamente la **capacidad de procesamiento en el tiempo**.

Un ordenador cuántico permite procesar muchísimas más operaciones que un ordenador normal, por lo que el problema del espacio en la computación actual desaparece ya que con menor tamaño se puede procesar muchas más información para resolver problemas complejos. Fue en 1994 cuando Peter Shor demostró que un ordenador cuántico podría factorizar con rapidez grandes números enteros.

VENTAJAS… o ¿AMENAZAS?

Las ventajas que suponen el procesamiento con la computación cuántica pueden suponer importantes amenazas a la seguridad de la información actual. Las principales ventajas serían las siguientes:

- Con un ordenador cuántico se **mejora el tiempo de procesamiento**, reduciendo el tiempo invertido en probar una posible combinación para romper el cifrado.

- Uno de los mayores avances con los ordenadores cuánticos es la posibilidad de **calcular factores de números** (tan grandes como se deseen) de una manera muy sencilla (algoritmo de Shor), además de curvas elípticas o logaritmos discretos. Con los ordenadores actuales es algo muy complejo de calcular y por

eso son métodos muy utilizados en los algoritmos de cifrado actuales, que quedarían en evidencia con estos ordenadores cuánticos.

Un ordenador cuántico sería capaz de romper la mayoría de los actuales algoritmos de cifrado al ser capaz de factorizar a una velocidad muchísimo mayor que los convencionales. Un ataque de fuerza bruta (probar todas las claves posibles a gran velocidad hasta dar con la correcta) sería sencillo con una máquina de estas características, por lo que es probable que la computación cuántica sea el final de la criptografía asimétrica actual basada en la factorización de números enteros y el cálculo de logaritmos discretos, como lo son curvas elípticas, Diffie-Hellman y RSA.

En la seguridad de la información, específicamente en la criptografía, se verán cambios tanto en la capacidad de dotar de mayor integridad a la actual (a los datos enviados en una comunicación), como en la capacidad para realizar criptoanálisis sobre algoritmos de cifrado actuales, con el impacto que esto conllevaría en campos como la economía, las finanzas y la seguridad militar, es por eso la importancia del estudio de la Criptografía Cuántica.

CONCLUSIONES

Muchos algoritmos de cifrado se basan en que la factorización de grandes números es una operación muy costosa en ordenadores tradicionales, mientras que no lo es en ordenadores cuánticos (ganancia exponencial); y en estos últimos se pueden ejecutar algoritmos de factorización. Con estas premisas parece que para muchos algoritmos de cifrado (de uso muy frecuente) el criptoanálisis cuántico es una amenaza real.

En el momento que consigan estabilizar y hacer funcionar el suficiente número de QUBITS trabajando en conjunto, se conseguirán resolver problemas de factorización que llevarían años en minutos. Se podría decir que la capacidad de cómputo matemático de un ordenador cuántico es de 1 a 1000000 (por mencionar una cantidad) en comparación del ordenador actual más potente.

La competencia no sería honesta, es como si compitiera un "Jet supersónico" contra un papalote (cometa), o como si se quisiera ganar a una bala. Tal como se refleja en las películas de acción (MATRIX). Esto es solamente una analogía para expresar el problema real, **muchos de los sistemas criptográficos quedarían obsoletos.** El principio de Kerckhoffs dice que "la seguridad debe recaer solo en la seguridad de la clave" en relación a que no pueda descifrarse o que por coste y tiempo de cómputo sea matemáticamente INVIABLE. Con un ordenador cuántico lo actualmente inviable podría

convertirse en POSIBLE, por lo que se tendrían que hacer toda una serie de cambios para garantizar que siga siendo inviable. Con estas expectativas de futuro, la preocupación debe ser mundial.

En resumen, la llegada de ordenadores cuánticos impactará no solo a los sistemas criptográficos actuales, sino a toda la humanidad. Será necesario que se realicen cambios físicos y lógicos de infraestructura para soportar la nueva "Revolución Cuántica".

BIBLIOGRAFÍA

- https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf
- https://www.xataka.com/
- https://www.lavanguardia.com/tecnologia/20170521/422764114392/computacion-cuantica-ordenadores-qubits.html https://ciberseguridad.blog/la-criptografia-post-quantum/
- https://es.wikipedia.org
- https://www.youtube.com/
- https://www.redeszone.net/2018/06/05/openvpn-seguridad-criptografica-post-quantum/
- https://www.t-systems.com/mx/es/noticias-y-eventos/editorial/seguridad/ict/post-quantum-cryptography-790560
- https://www.20minutos.es/noticia/3430406/0/duda-resuelta-fisica-cuantica-responde-incognita-antes-huevo-gallina/
- https://www.pandasecurity.com/spain/mediacenter/seguridad/los-ordenadores-cuanticos-ciberseguridad/
- http://www.criptored.upm.es/crypt4you/temas/cuantica/leccion2/leccion02.html
- https://pdfs.semanticscholar.org/86a2/9ccc18f226ad8e153b714f78736d4f3e6365.pdf
- https://en.wikipedia.org/wiki/Quantum_key_distribution
- https://www.quintessencelabs.com/wp-content/uploads/2015/08/CSA-What-is-Quantum-Key-Distribution-QKD-1.pdf
- https://www.nature.com/articles/srep35032
- https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/
- https://www.cs.nmsu.edu/~istrnad/cs478/presentations/QuantumCryptography.pdf
- https://www.researchgate.net/publication/228575112_Quantum_Key_Distribution_Protocols_A_Survey
- https://spectrum.ieee.org/computing/software/cryptographers-take-on-quantum-computers
- https://spectrum.ieee.org/computing/networks/qa-with-postquantum-computing-cryptography-researcher-jintai-ding
- https://en.wikipedia.org/wiki/Post-quantum_cryptography
- https://csrc.nist.gov/projects/post-quantum-cryptography