>> Jorge Dávila

E pur si muove! [1]

Después de la efervescencia generatriz de algoritmos criptográficos de la última década del siglo pasado, ha venido una calma –algo chicha– a principios de este siglo. Sin embargo, las cosas no han estado completamente quietas. La previsible llegada y generalización de la IoT general y de la OT industrial, así como la amenaza de un posible computador cuántico, han hecho que la administración norteamericana (el NIST) "toque a arrebato" y se desarrollen en el mundo lo que se llaman Criptografía Ligera y Criptografía Pos-cuántica. Va siendo hora de que echemos un vistazo en esta columna de qué va todo esto.

En 1633 el humanista italiano conocido como Galileo Galilei[3] (1564-1642) tuvo que agachar la cabeza ante la imponente y arrasadora iglesia católica, materializada en la organización teoterrorista conocida como la Inquisición o el Tribunal del Santo Oficio[4]. En aquella ocasión tuvo que abjurar de su teoría heliocentrista de que es la Tierra la que gira alrededor del Sol y no al revés. Dice la leyenda que al terminar el oficio, masculló aquello de "*Sin embargo se mueve*", como queriendo no resistirse del todo ante la obcecación de los que no querían perder su poder alienante frente a las masas y seguir determinando a capricho lo que era verdad y lo que no.

El control de las masas siempre ha sido algo a lo que los poderosos siempre han prestado mucha atención. Hoy en día hablamos de noticias falsas[5], de la posibilidad más que probable de que las "redes sociales" existan sólo para poder espiar a todo el mundo. Hoy es Tik Tok la que está en los titulares[6] pero, realmente, no creo que se salve ninguna de ellas.

Es cierto que esa aplicación de videos cortos es **increíblemente adictiva** y que ya la usan más de **1.000 millones de personas** en todo el mundo, lo que le podría llegar a suponer más de 18.000 millones de dólares en publicidad sólo en este año. Es cierto también, que se concentra peligrosamente en los más jóvenes y en las personas más vulnerables[7], por lo que en si misma constituye una peligrosa y amplia ventana de riesgo para todas las sociedades, occidentales y orientales, a medio y largo plazo.

Sin embargo, la manipulación de las masas[8], el poder determinar lo que piensan, lo que creen, el modo en que se comportan, lo que anhelan y desean, siempre ha sido el objetivo de muchos poderes; el político[9], el religioso[10], el cultural[11], el empresarial[12], etc., por lo que esta amenaza no se trata de nada realmente nuevo. Lo único nuevo es la magnitud del proceso, la cantidad de seres humanos a los que se puede alienar **con sólo una aplicación informática y mucha Internet**.

Según los medios de comunicación de todo tipo, hay frentes en los que parece focalizarse toda la actividad actual en los temas de informática o desarrollo digital. Por un lado está **1)** la muy manida "Inteligencia Artificial" y su vacuo charlatán conocido como chatGPT, y por otro, **2)** la "inminente" llegada del mesías de la computación en la forma de "Computador Cuántico". Sin embargo, hay otros frentes digitales que también se mueven y sus derroteros[13] pueden poner en riesgo o salvar la evolución de nuestra realidad más global y más cotidiana a medio y largo plazo.

La escasez de algoritmos criptográficos asimétricos, la opción de utilizar planteamientos matemáticos para elegirlos y la "amenaza cuántica", han ocupado en estos últimos años a los criptógrafos de todo el mundo.

Un microcontrolador es un circuito integrado programable, capaz de ejecutar las órdenes (comandos) grabadas en su memoria. Esos dispositivos están compuestos por varios bloques funcionales diseñados para atender a tareas específicas como son la unidad central de procesamiento, la memoria y los periféricos de entrada/salida.

Se dice que el primer microprocesador lo creó la compañía Intel y fue el **Intel 4004**[14] que trabajaba con valores de 4 bits y que fue lanzado al mercado en noviembre de 1971. Poco después, ese diseño fue seguido por el muy popular **Intel 8008**[15] y otros microprocesadores más potentes. Otras fuentes dicen que fueron los ingenieros de Texas Instruments **Gary Boone** y **Michael Cochran** los que crearon el primer microcontrolador, el **TMS 1000**[16], también en el año 1971, aunque no fue comercializado hasta 1974.

En aquellos años, ZiLOG fue un fabricante de microprocesadores, siendo su producto más conocido el **Zilog Z80** que trabajaba con registros de 8 bits. De hecho, ZiLOG Inc.[17] fue la primera compañía dedicada exclusivamente a la venta de microprocesadores. Fue fundada por Federico Faggin a finales del 1974, y su desarrolló más exitoso fue el microprocesador **Z80**[18] que se popularizó en los años 1980 por ser el alma de ordenadores muy populares como el **Sinclair ZX Spectrum**[19], **Amstrad**

[1] La expresión italiana "*E pur si muove!*" o "*Eppur si muove!*" que significa "*Y sin embargo gira*", literalmente: "*y sin embargo se mueve*".
[2] Ver https://en.wikipedia.org/wiki/Public-key_cryptography
[3] Ver https://en.wikipedia.org/wiki/Galileo_Galilei
[4] Ver https://es.wikipedia.org/wiki/Inquisición_española
[5] Ver https://en.wikipedia.org/wiki/Fake_news
[6] Ver https://www.elmundo.es/economia/2023/03/23/641ca8ad21efa078638b4599.html
[7] Ver https://www.diariodesevilla.es/salud/investigacion-tecnologia/Tiktok-peligrosos-efectos-invisibles-salud-mental-jovenes_0_1727528002.html
[8] Ver https://concepto.de/propaganda/
[9] Ver https://es.alphahistory.com/guerra-Fr%C3%ADa/propaganda-de-la-guerra-fría/
[10] Ver https://compolitica.com/iglesia-y-propaganda-dos-milenios-de-persuasion-desde-la-silla-de-san-pedro/
[11] Ver https://en.wikipedia.org/wiki/Reich_Ministry_of_Public_Enlightenment_and_Propaganda
[12] Ver https://en.wikipedia.org/wiki/Marketing
[13] Derrotero; De derrota 'camino, rumbo'. 1. Camino, rumbo, medio tomado para llegar al fin propuesto. 2. Conjunto de datos que indican el camino para llegar a un lugar determinado 3. Línea señalada en la carta de marear para el gobierno de los pilotos en los viajes. 4. Dirección que se da por escrito para un viaje de mar.
[14] Ver https://es.wikipedia.org/wiki/Intel_4004
[15] Ver https://es.wikipedia.org/wiki/Intel_8008
[16] Ver https://en.wikipedia.org/wiki/Texas_Instruments_TMS1000
[17] Ver https://en.wikipedia.org/wiki/Zilog
[18] Ver https://es.wikipedia.org/wiki/Zilog_Z80
[19] Ver https://es.wikipedia.org/wiki/Sinclair_ZX_Spectrum
[20] Ver https://es.wikipedia.org/wiki/Amstrad_CPC
[21] Ver https://en.wikipedia.org/wiki/Embedded_system
[22] Ver https://en.wikipedia.org/wiki/Arduino
[23] Ver https://en.wikipedia.org/wiki/Mbed

CPC[20] o de los ordenadores de sistema **MSX** presentado por Microsoft y ASCII Corporation en junio de 1983.

El Z80 Es uno de los procesadores de más éxito del mercado y prueba de ello lo son la infinidad de versiones clónicas que se han fabricado desde entonces, y aún hoy sigue siendo usado de forma extensiva en multitud de **sistemas embebidos**[21].

Los sistemas embebidos se fabrican en el rango de los millones de unidades con lo que se puede obtener muy significativas reducciones de costes a la vez que **se implantan en innumerables escenarios de todo el mundo**. Los sistemas embebidos suelen utilizar procesadores relativamente pequeños y lentos, con una memoria también pequeña y todo lo necesario para que funcionen de forma esencialmente autónoma. Los primeros equipos embebidos los desarrolló IBM en los años 1980 y, en general, se emplean en tareas de **procesamiento en tiempo real**.

Actualmente existen plataformas desarrolladas por distintos fabricantes que proporcionan herramientas muy cómodas para el diseño y desarrollo de aplicaciones y prototipos con sistemas embebidos a través de intuitivos entornos gráficos como son los casos de **Arduino**[22], **Mbed**[23], **Raspberry Pi**[24], **BeagleBone**[25], etc. Aunque este fenómeno emana de las décadas del final del Siglo XX, su popularidad no llega hasta que se empieza a hablar[26] de la **Internet de las Cosas**[27]. Aunque algunos puedan pensar que esto de la IoT es algo moderno, deberían saber que todo esto empezó en 1982 con una máquina expendedora de Coca-Colas ubicada en la Universidad de Carnegie Mellon[28], y de la cual Internet (la comunidad) quería saber si las latas estaban frías o no.

Son dos los nichos actuales en los que la IoT se ha ido desarrollando sigilosamente; uno de ellos es la **Domótica** o **Automatización del Hogar**[29], y por otro el **cuidado de ancianos**[30]. En la domótica, los dispositivos IoT incluyen sistemas para el control de la iluminación (intensidad y color), del acondicionamiento térmico (calefacción y refrigeración), del ambiente sonoro y visual (música y video ambiental), de los sistemas de seguridad perimetral y funcional de la casa (cámaras de vigilancia, sensores y actuadores de todo tipo), etc.

En principio, de esa automatización serían esperables beneficios a largo plazo como el **ahorro energético** al poder apagar automáticamente aquello que no sea necesario en cada momento[31]. Las casas inteligentes (*Smart* o *Automated Home*) contienen plataformas agregadoras que reúnen en ellas el control de numerosos dispositivos inteligentes especializados en funciones variopintas. Ejemplos de ello hay varios; por un lado tenemos el Apple's HomeKit[32] que permite poner todo lo importante de una casa a las órdenes del teléfono iPhone o de un Apple Watch; y con ello a las órdenes de cualquier aplicación nativa IOS como pueden ser asistentes como Siri, lo cual no es excepcional.

Hay plataformas que, como parte de su atractivo comercial, se pueden conectar a diferentes agentes domésticos digitales como son Echo Dot y Alexa[33] de Amazon, Home[34] de Google, HomePod[35] de Apple, y el SmartThings Hub[36] de Samsung. Además de los sistemas propietarios, también hay iniciativas de código abierto como son Home Assistant[37], OpenHAB[38] y Domoticz[39], entre otras.

Una de las justificaciones más eficaces para la automatización y monitorización del hogar está la **asistencia a ancianos** y **discapacitados** funcionales de algún tipo. Aquí se incluyen asistentes de voz para aquellos con problemas de vista o movilidad reducida, y aquellos sistemas de alerta que van directamente conectados a los implantes cloqueares de aquellos que tienen problemas auditivos. También se pueden conectar otros sensores que son sensibles a estados de emergencia médica (caídas, lipotimias, crisis glucémicas, etc.)

Además de todos estos usos "*para particulares*", no hay que olvidar que la IoT también ha colonizado los sistemas industriales a modo de evolución natural de los sistemas de automatización industrial anteriores. En este caso, es todo el sistema productivo industrial el que se pone a los pies de la nueva **OT** (**Operative Technology**)[40], que es como gustan llamar a la IoT industrial sus promotores. Para 2019 ya se estimaba que el número de artefactos IoT superaría los 9.100 millones de dispositivos[41].

Lo curioso de esta historia, es que **sus necesidades de seguridad**, en el sentido más amplio posible y en el de la ciberseguridad en concreto, es algo que **no se han tenido en cuenta**, **están pendientes**, y que ahora parecen saltar al candelero.

El primer cifrador civil se diseñó entre 1971 y 1973, y se llamaba **Lucifer**[42]. Su razón de ser fue un encargo que hizo el LLoyd's Bank de Londres a IBM[43] para poder proteger las comunicaciones digitales de lo que era, por aquel entonces, la joya tecnológica del sistema bancario: los "cajeros automáticos"[44].

El otro frente que tiene abierto la seguridad criptográfica actual es el de la amenaza cuántica. Sin entrar en si es realmente tal o una versión moderna del clásico sacamantecas del siglo XIX utilizado, esencialmente, para meter miedo, lo que si es cierto es que la Criptografía Asimétrica[2] lleva más de cuarenta años tentando a su suerte.

Convenientemente "tuneado" por la NSA, el algoritmo Lucifer se transformó en el muy popular **DES** (**Data Encryption Standard**)[45]; que en febrero de 1977 paso a ser el estándar de cifrado[46] de la administración norteamericana. En principio esto iba a ser así durante sólo cinco años, pero ese algoritmo fue renovado en su puesto hasta el 26 de mayo de 2002, momento en que dio paso al **AES**[47] como estándar actual de cifrado.

El desgaste de los cifradores

Estos casi cincuenta años transcurridos han demostrado la validez de estos cifradores, pero también su desgaste con el tiempo y su uso, debido a cambios tecnológicos que terminan favoreciendo su criptoanálisis. Nadie en 1977 podía imaginar la aparición de Internet y su implicación en la computación distribuida[48] utilizada en ataques por fuerza bruta[49]. En 1997 Rocke Verser, junto a miles de voluntarios conectados a Internet, lograron encontrar una clave DES en **tan sólo 96 días** después de haber empezado a buscarla, y ello con la única estrategia de probar con todas las claves posibles hasta encontrar la correcta (fuerza bruta).

Aunque son muchos los cifradores simétricos que se han creado y evaluado en el último medio siglo[50], el paso del tiempo, a la vez que los consagra, los debilita. Sus diseñadores

[24] Ver https://es.wikipedia.org/wiki/Raspberry_Pi
[25] Ver https://en.wikipedia.org/wiki/BeagleBoard
[26] Ver http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf y https://web.archive.org/web/20150311220327/http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf
[27] Red de objetos físicos (o grupos de tales objetos) con sensores, capacidad de procesamiento, software específico y otras tecnologías que se conectan entre si y que intercambian datos con otros dispositivos o sistemas a través de Internet u otras redes telemáticas. Ver https://en.wikipedia.org/wiki/Internet_of_things
[28] Ver https://www.cs.cmu.edu/~coke/history_long.txt
[29] Ver https://en.wikipedia.org/wiki/Home_automation
[30] Ver https://en.wikipedia.org/wiki/Home_automation_for_the_elderly_and_disabled
[31] Ver "*Socially Intelligent Interfaces for Increased Energy Awareness in the Home*" en https://arxiv.org/pdf/2106.15297.pdf
[32] Ver https://www.cnet.com/home/smart-home/apple-homekit-everything-you-need-to-know/
[33] Ver https://alexa.amazon.com/
[34] Ver https://home.google.com/welcome/
[35] Ver https://www.apple.com/homepod/
[36] Ver https://www.samsung.com/us/support/smart-home/smartthings/hubs/smartthings-hub/
[37] Ver https://en.wikipedia.org/wiki/Home_Assistant
[38] Ver https://en.wikipedia.org/wiki/OpenHAB
[39] Ver https://domoticz.com/
[40] Ver https://en.wikipedia.org/wiki/Operational_technology
[41] Ver https://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12
[42] Ver http://www.quadibloc.com/crypto/co0401.htm
[43] Ver https://www.ibm.com/ibm/history/ibm100/us/en/icons/cryptography/
[44] Ver https://www.theatlantic.com/technology/archive/2015/03/a-brief-history-of-the-atm/388547/
[45] Ver https://en.wikipedia.org/wiki/Data_Encryption_Standard
[46] Ver https://csrc.nist.gov/CSRC/media/Publications/fips/46/archive/1977-01-15/documents/NBS.FIPS.46.pdf

nunca pudieron imaginar las capacidades tecnológicas que acabaría teniendo el atacante, por lo que no pudieron incluir contramedidas. Tengamos en cuenta que **hoy existe Internet**, y que las **GPUs**[51] son los dispositivos de cálculo más potentes que un usuario común puede comprar y que éstas se fabrican en centenares de miles de ejemplares anuales. Las **granjas o factorías de GPUs** es algo que Bitcoin ya ha puesto en pie y a prueba estos últimos años y, por si fuera poco, alguien ha levantado la **amenaza cuántica**[52]. Por todo ello convendría ir pensando en los cifradores, simétricos y asimétricos de las próximas décadas. Hay que ampliar y mejorar la oferta.

Puestos a pensar en el futuro, los hay que imaginamos un escenario muchísimo más amplio que el actual, en el que la potencia computacional quizás no sea intensiva (pocos, grandes y muy caros ordenadores generales o especializados organizados en nubes), sino más bien extensiva (muchos, pequeños y baratos dispositivos computacionales con memoria organizados en "nieblas"). Es probable que la IoT y la OT tengan sus décadas de gloria y apogeo en el futuro medio y lejano, por lo que la excusa para un escenario extensivo ya está servida.

La senda de la Criptografía Ligera

Éste debe ser enfoque de la administración norteamericana cuando decidió iniciar la senda de lo que se conoce como la **Criptografía Ligera** (*Lightweight Cryptography*)[53]. En 2018, el NIST anunció un concurso[54], al estilo de los anteriores, centrado en la búsqueda de algoritmos que pudiesen englobarse dentro de la criptografía ligera; es decir, **que fuesen seguros y adecuados para ser utilizados en entornos con capacidades muy limitadas** (redes de sensores, dispositivos sanitarios personalizados, sistemas distribuidos de control, sistemas ciberfísicos, etc.).

En esa convocatoria se especificaron lo que ellos entendían eran los requisitos técnicos que deberían satisfacer dicho tipo de algoritmos, y al concurso se presentaron 57 candidatos[55] de 25 países. De ellos, 32 pasaron a una segunda fase[56] de selección gracias a sus buenas propiedades de seguridad.

La siguiente etapa habría sido la de seleccionar ocho finalistas que sean significativamente mejores que los actuales estándares del NIST tanto en software como en hardware, sin embargo, el 7 de febrero de este año, el NIST anunció[57] la selección de la **familia de cifradores Ascon**[58] para su estandarización como algoritmos criptográficamente seguros y ligeros. Son siete los miembros de la familia Ascon, y ofrecen varias funcionalidades que son útiles para desarrollar distintas tareas muy demandadas. La más importante es el **Cifrado Autenticado** (*authenticated encryption*) **con datos de integridad asociados** (AEAD).

Otro ejemplo prometedor de algoritmo criptográfico ligero es **Xoodyak**[59], diseñado por Joan Daemen y su equipo, basado en los conceptos de **esponjas criptográficas** y **construcciones duales**[60] que están relacionados con evoluciones de la esencia empleada en el último algoritmo hash (SHA3)[61] aprobado por la administración norteamericana.

Cualquier entorno IoT/OT está marcado por estrictos restricciones en la potencia consumible, la potencia de procesado, y la seguridad física de los mismos. Algunos de los algoritmos que están dentro de la oferta del NIST son **GIFT**, **AES**, y **SPECK**, entre otros[62].

El reto esencial de la Criptografía Ligera es análogo al del mitológico enfrentamiento entre David y Goliat[63]. La esencia de ésta es desarrollar algoritmos muy sencillos y fáciles de calcular, cuya complejidad (confusión y difusión) resultante sean suficientemente altas como para ganar a cualquier otro posible o futuro sistema computacional, sin límites de potencia y recursos, que pueda dedicarse a su criptoanálisis. Está por ver si esta heroicidad es realmente posible, pero como objetivo profesional es de lo más apetecible. Del éxito de esta misión depende nuestra tranquilidad ante toda futura IoT y todos los sistemas OT industriales por venir.

El reto esencial de la Criptografía Ligera es análogo al del mitológico enfrentamiento entre David y Goliat. Está por ver si esta heroicidad es realmente posible, pero como objetivo profesional es de lo más apetecible. Del éxito de esta misión depende nuestra tranquilidad ante toda futura IoT y todos los sistemas OT industriales por venir.

La amenaza cuántica

El otro frente que tiene abierto la seguridad criptográfica actual es el de la **amenaza cuántica**. Sin entrar en si esa amenaza es realmente tal o una versión moderna del clásico *sacamantecas*[64] del siglo XIX utilizado, esencialmente, para meter miedo; lo que sí es cierto es que **la Criptografía Asimétrica**[65] **lleva más de cuarenta años tentando a su suerte**. A diferencia de los cifradores simétricos, los asimétricos optaron desde el principio, justo después de ser imaginados[66] en 1976, por recurrir a **problemas matemáticos difíciles** que permitiesen construir **funciones netamente asimétricas**; es decir, (relativamente) fáciles de calcular en un sentido, pero computacionalmente imposibles en el sentido contrario.

En febrero de 1977 Ron Rivest, Adi Shamir y Leonard Adleman, propusieron utilizar la **exponenciación modular** con un **módulo compuesto especialmente elegido** en lo que, desde entonces, conocemos como algoritmo **RSA**[67]. En este caso, la dificultad que hace asimétrica la función es la **descomposición factorial** de ese módulo especialmente construido mediante una simple multiplicación.

Además del RSA, en 1985 se propuso otro tipo del algoritmo, el de **ElGamal**[68] y el protocolo de intercambio de claves sobre canales públicos, conocido como de **Diffie-Hellman-Merkle**[69]. En ambos casos, el problema matemático subyacente es la relativa sencillez de calcular una exponenciación modular y la imposibilidad computacional de calcular **logaritmos discretos**[70] en conjuntos de puntos suficientemente grandes.

Por último, también en 1985 se propuso el uso de las **Curvas Elípticas en Criptografía**[71]. Una curva elíptica es algo conocido de tiempo atrás en matemáticas, y podríamos decir que es una curva algebraica, no singular, suave y plana, con soluciones (x, y) que satisfacen la ecuación $y^2 = x^3+ax+b$, con ciertos parámetros a y b.

La sunción básica de este tipo de criptografías es que encontrar el logaritmo discreto de un elemento cualquiera (al azar) respecto a un punto conocido es imposible (Elliptic Curve Discrete Logarithm Problem o ECDLP).

[47] Ver https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
[48] Ver https://en.wikipedia.org/wiki/DESCHALL_Project y https://web.archive.org/web/20071231165331/http://www.interhack.net/pubs/des-key-crack/
[49] Ver https://en.wikipedia.org/wiki/Distributed.net
[50] Ver https://en.citizendium.org/wiki/Block_cipher
[51] Ver https://en.wikipedia.org/wiki/Graphics_processing_unit
[52] Ver https://en.wikipedia.org/wiki/Shor's_algorithm y https://en.wikipedia.org/wiki/Grover's_algorithm
[53] Ver https://csrc.nist.gov/Projects/Lightweight-Cryptography, https://www.sciencedirect.com/topics/computer-science/lightweight-cryptography
[54] Ver https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection
[55] Ver https://csrc.nist.gov/projects/lightweight-cryptography/round-1-candidates
[56] Ver https://csrc.nist.gov/projects/lightweight-cryptography/round-2-candidates
[57] Ver https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon
[58] Ver https://ascon.iaik.tugraz.at/ y https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf
[59] Ver https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Xoodyak-spec.pdf y https://keccak.team/xoodyak.html
[60] Ver https://keccak.team/sponge_duplex.html
[61] Ver https://en.wikipedia.org/wiki/SHA-3
[62] Ver https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9328432
[63] Ver https://es.wikipedia.org/wiki/Goliat_(personaje_bíblico)
[64] Ver https://en.wikipedia.org/wiki/Sacamantecas
[65] Ver https://en.wikipedia.org/wiki/Public-key_cryptography
[66] Ver Diffie W., Hellman, M.: "*New Directions in Cryptography*". 01 Nov 1976 - IEEE Transactions on Information Theory (IEEE) - Vol. 22, Iss: 6, pp 644-654, en https://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf

La seguridad de la criptografía sobre curvas elípticas depende de la habilidad para **calcular la multiplicación de dos puntos** (de la curva) y de la imposibilidad de calcular uno de ellos conociendo el otro y el resultado del producto; vamos, que **no sabemos "dividir" números/puntos en la curva**. El tamaño de la curva elíptica, medida por la cantidad de pares de números enteros que satisfacen su ecuación, determina la dificultad computacional para resolver el problema planteado.

La criptografía post-cuántica

En esencia, la **criptografía post-cuántica** (*post-quantum cryptography* o **PQC**)[72] se refiere a algoritmos criptográficos (normalmente asimétricos) que se piensa serían seguros frente a un ataque criptoanalítico utilizando un ordenador cuántico. El problema es que los algoritmos actuales se basan en problemas matemáticos (factorización de enteros, el problema del Logaritmo discreto, y el problema del logaritmo discreto sobre curvas elípticas) que podrían ser resueltos con un ordenador cuántico suficientemente potente ejecutando algoritmos especiales como el de Shor[73] y semejantes.

Para intentar resolver esta peligrosa carencia de algoritmos criptográficos asimétricos en general, y que sean resistentes a la amenaza cuántica, la administración norteamericana, a través del NIST, ha convocado otro concurso de ideas[74] que se conoce como proyecto de Estandarización de la Criptografía Post-Cuántica (*Post-Quantum Cryptography Standardization Project*)[75]. Después de cuatro rondas de selección y después de celebrar a finales de noviembre de 2022 la cuarta Conferencia de Estandarización PQC[76], el NIST anunció cuáles son los candidatos seleccionados[77].

Para el cifrado en general, como es el caso de las conexiones TLS, el NIST ha seleccionado el algoritmo conocido como **CRYSTALS-Kyber**[78]. Entre sus ventajas están sus relativamente pequeñas claves de cifrado que los comunicantes tienen que intercambiar, así como su velocidad de operación.

Kyber es un mecanismo seguro frente a ataques adaptativos de criptograma (IND-CCA2)[79], dedicado al **encapsulado de claves** (KEM)[80], y cuya seguridad se basa en la dificultad de resolver el problema de **Aprendizaje con Errores** (*learning-with-errors* o **LWE**)[81] sobre celosías modulares (modular lattices). Su propuesta incluye tres conjuntos diferentes de parámetros para ajustar el nivel de seguridad obtenido en cada caso. En concreto, Kyber-512 pretende tener una seguridad equivalente a la del AES-128, el Kyber-768 una seguridad semejante a la del AES-192, y el Kyber-1024 una seguridad pareja a la del AES-256.

Las recomendaciones actuales son las de utilizar Kyber **en el modo denominado "híbrido"**, es decir, combinado con sistemas "pre-cuánticos" (los de siempre) como, por ejemplo, el protocolo de Diffie-Hellman sobre curvas elípticas. Kyber ya ha sido integrado en librerías y sistemas industriales como, por ejemplo, en la librería criptográfica interoperable y reutilizable de Cloudflare (CIRCL)[82], que además incluye otros candidatos poscuánticos **SIDH**[83] y **SIKE**[84] que a fecha de hoy, **ya se sabe que son inseguros**.

Amazon por su parte soporta modos híbridos de funcionamiento en los que incluye Kyber en su servicio de gestión de claves de AWS; y ya el 2019 IBM anunció el uso de ese mismo algoritmo y otro conocido como **CRYSTALS-Dilithium** en un dispositivo de almacenamiento en cinta.

Como algoritmo de firmas digitales, NIST ha seleccionado tres algoritmos: **CRYSTALS-Dilithium**[85], **FALCON**[86] y **SPHINCS+**[87]. Los dos primeros son los más eficaces y NIST recomienda utilizar Dilithium como preferido y dejar FALCON para aplicaciones en las que sea necesario firmas más pequeñas que las generadas con Dilithium. Por su parte, SPHINCS+, genera firmas más grandes y es algo más lento que los otros dos, pero tiene interés como mecanismo de salvaguardia (backup) ya que está basado en una aproximación matemática distinta a la de los otros tres algoritmos recomendados (evitando así poner todos los huevos en la misma cesta).

La escasez de algoritmos criptográficos asimétricos, la opción de utilizar planteamientos matemáticos para elegirlos y la "amenaza cuántica", han ocupado en estos últimos años a los criptógrafos de todo el mundo. En el fondo se han "re-visitado" problemas que ya se sabía que eran difíciles y poco "eficientes" (por su velocidad y tamaño de las firmas), luego no hay grandes novedades. Sin embargo, es bueno que se mueva algo en la criptografía real, en la que se utiliza en los sistemas del día a día, ya que los últimos veinte años se ha estado viviendo de algoritmos diseñados en las últimas décadas del siglo pasado.

La corrección de los algoritmos criptográficos utilizados es una condición "necesaria pero no suficiente" para que podamos tener un sistema, un procedimiento, seguro. También debemos tener implementaciones y usos realmente seguros de dichos algoritmos. Si el criptoanalista no logra hincarle el diente al algoritmo, siempre podrá atacar a sus implementaciones concretas.

Sin embrago, es necesario plantearse lo que dijo Edgar Allan Poe, a través de uno de los protagonistas de su narración "*El escarabajo de oro*" (The Gold-bug, 1843)[88]; "***es, en realidad, dudoso que el genio humano pueda crear un enigma de ese género que el mismo ingenio humano no resuelva con una aplicación adecuada***".

Hay que tener en cuenta que **la corrección de los algoritmos criptográficos** utilizados es una condición "**necesaria pero no suficiente**" para que podamos tener un sistema, un procedimiento, seguro. También **debemos tener implementaciones y usos realmente seguros de dichos algoritmos**. Si el criptoanalista no logra, hincarle el diente al algoritmo, siempre podrá atacar (con bastante éxito en muchos casos) a sus implementaciones concretas. Huyamos de los becerros de oro, aunque sea mucho su brillo y mucha su popularidad en los grandes medios. La criptografía es una actividad difícil, poco grata, pero absolutamente necesaria; por lo que **sólo se puede hacer si se hace bien**. ■

[67] Ver https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[68] Ver https://en.wikipedia.org/wiki/ElGamal_encryption
[69] Ver https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
[70] Ver https://en.wikipedia.org/wiki/Discrete_logarithm
[71] Ver https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
[72] Ver https://en.wikipedia.org/wiki/Post-quantum_cryptography
[73] Ver https://en.wikipedia.org/wiki/Shor's_algorithm
[74] Ver https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[75] Ver https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization
[76] Ver https://csrc.nist.gov/events/2022/fourth-pqc-standardization-conference
[77] Ver https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022
[78] Ver https://pq-crystals.org/kyber/
[79] Ver https://en.wikipedia.org/wiki/Ciphertext_indistinguishability
[80] Ver https://en.wikipedia.org/wiki/Key_encapsulation_mechanism
[81] LWE es un modo de esconder un valor secreto añadiéndole ruido y haciendo que éste sea muy significativo. Ver https://en.wikipedia.org/wiki/Learning_with_errors y https://dl.acm.org/doi/pdf/10.1145/2535925
[82] Ver https://blog.cloudflare.com/introducing-circl/
[83] SIDH = *Super singular Isogeny-based Diffie-Hellman protocol*. (¡algoritmo inseguro!) Ver https://en.wikipedia.org/wiki/Supersingular_isogeny_key_exchange
[84] SIKE = *Super singular Isogeny-based Key Encapsulation protocol*. (¡algoritmo inseguro!) Ver https://sike.org/
[85] Ver https://pq-crystals.org/dilithium/
[86] Ver https://falcon-sign.info/
[87] Ver https://sphincs.org/
[88] Ver https://en.wikipedia.org/wiki/The_Gold-Bug

Jorge Dávila
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es