CriptoCert Certified Crypto Analyst, una nueva certificación profesional criptográfica que nace en España

Con el reconocimiento del Centro Criptológico Nacional (CCN), nace en España CriptoCert Certified Crypto Analyst, una nueva certificación profesional criptográfica, de seguridad y protección de datos. Una iniciativa de CriptoCert, compañía recientemente creada en la que participan como fundadores tres solventes expertos de la cibeseguridad técnica –dos de Criptored y un tercero de DinoSec–. Su objetivo principal es atender la necesidad de disponer en la industria de profesionales con los conocimientos criptográficos necesarios, promoviendo la correcta utilización e implantación de la criptografía en todas las tecnologías y soluciones de seguridad, y su futura evolución en los próximos años.

La enseñanza de la criptografía y el entorno educativo

La criptografía, sin duda la rama más antigua de la seguridad informática, ha jugado en las últimas cuatro décadas un papel fundamental en el desarrollo de las nuevas tecnologías de la información, especialmente desde la irrupción de la cifra asimétrica o de clave pública, propuesta y creada, a finales de 1976, por los investigadores Whitfield Diffie y Martin Hellman, de la Universidad de Stanford. Unido al algoritmo DES, antiguo estándar de cifra ratificado por el NIST, un buen puñado de algoritmos de cifra simétrica y asimétrica comienzan sus andaduras desde finales de los años setenta, unos con menos fortuna que otros. Con ello se acrecienta la necesidad de enseñar y formar adecuadamente a los nuevos profesionales en estas técnicas de protección de la información, generalmente en las universidades y centros de investigación. En cuanto a esa enseñanza universitaria, en estas cuatro décadas la criptografía ha pasado de ser un temario obligatorio e indiscutible en las asignaturas de los ochenta y noventa, a perder parte de ese protagonismo a comienzos de este siglo XX, básicamente debido a la aparición de nuevas temáticas de gran interés en la seguridad (redes, protocolos, gestión, legislación, *hacking*, programación, análisis forense, etc.). Finalmente, ha vuelto a recuperar el protagonismo a finales de esta década de 2010, debido en este caso a la necesidad de proteger la información en la nube, la posibilidad del uso de cifrado homomórfico, nuevos sistemas basados en las cadenas de bloques (*blockchain*), protocolos avanzados de autenticación y la inevitable llegada de la criptografía postcuántica, habida cuenta del incesante desarrollo de nuevos computadores cuánticos desarrollados últimamente por grandes empresas y organizaciones.

Por otro lado, es menester destacar que existe una desigual formación profesional en criptografía entre los diferentes países de habla hispana. Alguno de ellos, como es el caso de España, con una gran profusión de asignaturas de criptografía en los grados de ingeniería, y algunas en los másteres, y en sentido contrario algunos países de Latinoamérica, en que dichas enseñanzas prácticamente no existen. Siendo conscientes de este escenario, Criptored apostó desde sus inicios en 1999 por una difusión masiva de la criptografía y la seguridad, destacando entre sus proyectos el MOOC Crypt4you, la enciclopedia visual intypedia, las píldoras formativas Thoth, el cuaderno de prácticas CLCript, la generación de software educativo para prácticas de criptografía, así como la publicación de libros electrónicos con más de 200.000 descargas, todos ellos contenidos de libre acceso desde su servidor web. Esos proyectos, y otros más como las conferencias TASSI, los congresos propios CIBSI y TIBETS celebrados ya en nueve ediciones en Latinoamérica, y las cuatro ediciones del congreso DISI en Madrid, con los mayores expertos mundiales como invitados, han tenido una excelente acogida. Destacan especialmente el MOOC Crypt4you con más de 1.250.000 accesos en siete años y el material multimedia subido al canal YouTube de la UPM, con dos millones de visitas, el 10% del total de visitas de dicha red social universitaria.

Con una media de un nuevo proyecto cada dos años, ¿qué nos tocaba hacer ahora desde Criptored para celebrar los 20 años de existencia y seguir difundiendo masivamente la criptografía? Simplemente dar un paso más; unirse a los más destacados expertos en la materia y crear una nueva certificación profesional en criptografía a través de la creación de una nueva compañía innovadora: **CriptoCert**.

Protagonismo de la criptografía en estos últimos años

Los últimos años han revelado diferentes hitos que es interesante destacar. Uno de los más significativos es la necesidad del uso de la criptografía en un amplio conjunto de tecnologías, protocolos, normativas (como por ejemplo los expertos en protección de datos y RGPD, o GDPR) y sistemas utilizados en el mundo real, que pasan desde las tan citadas criptomonedas y otros usos de las tecnologías *blockchain*, como los *smart contracts*, a arquitecturas criptográficas, nuevos algoritmos de protección (criptografía cuántica, postcuántica, etc.), auditorías criptográficas de software y hardware, programación segura de software, almacenamiento de datos, protección de las comunicaciones de los dispositivos IoT (Internet of Things), redes y comunicaciones inalámbricas, los sistemas de voto electrónico online (e-voting), etc.

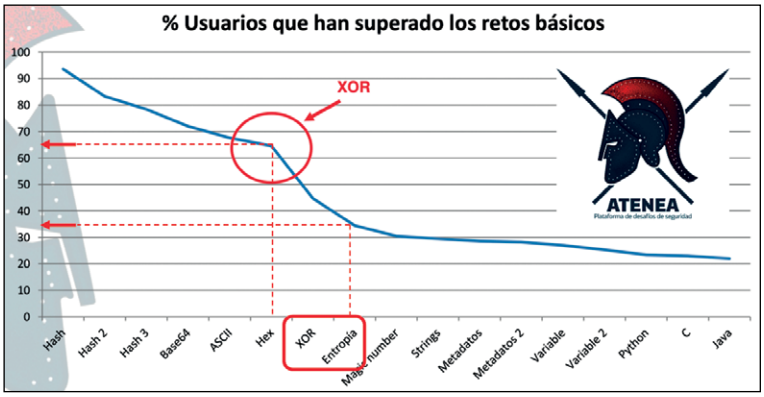

Fig. 1.- Dificultad y complejidad asociada a los retos de criptografía.

Este conjunto revela un matiz importante, considerando que las oportunidades laborales y comerciales en esta disciplina serán enormes durante la próxima década. Sin embargo, y en contraposición a estas oportunidades y al presente y futuro cercano para su aplicación, llama la atención la carencia formativa en esta disciplina entre los profesionales de la seguridad y de las nuevas tecnologías. Así, no resulta sencillo encontrar profesionales, por ejemplo en el mundo de la ciberseguridad, con una formación adecuada en esta especialidad criptográfica. Si esa búsqueda se extiende a otros sectores de la sociedad, por ejemplo, a los profesionales de TI (Tecnologías de la Información) o de las TIC (Tecnologías de la Información y las Comunicaciones), dicho índice es mucho menor. Este hecho podría llegar a justificar, por ejemplo, la falta de mecanismos adicionales de protección de seguridad de la información en los incidentes con más repercusión mediática asociados a la fuga masiva de datos personales. Ejemplos recientes significativos han sido el caso de Cambridge Analytica, Equifax o de los hoteles Marriott.

El uso de la criptografía en numerosos protocolos de comunicaciones, y en muchos otros escenarios prácticos, continúa progresando sin límites e invadiendo nuestras vidas. Así, durante el pasado año 2018, y previsiblemente de manera mucho más relevante durante este 2019, la protección del servicio de resolución de nombres en Internet, o DNS, debería consolidarse debido a su importancia y criticidad, mediante un uso más extendido de DNSSEC, DoH o DoT, tal como ha solicitado recientemente ICANN, máximo responsable de la jerarquía de nombres en Internet.

Por otro lado, y relacionado con los relevantes descubrimientos de seguridad de los últimos años relativos

a las comunicaciones inalámbricas, el pasado año se ratificó el estándar de seguridad Wi-Fi WPA3, que se hará realidad a lo largo de este año con la presencia de numerosos productos comerciales en el mercado con soporte para él. A las novedades de seguridad en el mundo Wi-Fi se une la siguiente generación del estándar de telefonía móvil que está empezando a ser implantada por los operadores de telecomunicaciones a nivel mundial, conocida como 5G. En breve se dispondrá de manera generalizada de dispositivos móviles en el mercado que ofrecerán soporte para ambas tecnologías que, como no podía ser de otro modo, hacen un uso extensivo de múltiples protocolos y mecanismos criptográficos.

Sin duda, la privacidad y la protección de las comunicaciones de los usuarios es una problemática social creciente a nivel mundial, debido a la extensa utilización de las aplicaciones de mensajería por millones de usuarios. En los últimos años igualmente se ha incrementado de forma exponencial el uso de soluciones de cifrado extremo a extremo (E2E) popularizadas por aplicaciones como WhatsApp o Signal, entre otras.

Durante los últimos dos o tres años, la importancia de la criptografía en numerosos aspectos cotidianos, tanto personales como profesionales, es más que notable. Así, de manera global, la necesidad de proteger todas las comunicaciones e intercambios de información a través de las tecnologías web, empleando HTTPS, es una tendencia que irremediablemente nos llevará a un Internet que solo hará uso de HTTPS y no de HTTP dentro de unos años. Esta evolución ha permitido la ratificación recientemente del protocolo TLS versión 1.3.

La necesidad de disponer de conocimientos criptográficos para su correcta aplicación en las tecnologías modernas se ha hecho ampliamente patente con los acontecimientos de estos últimos años, motivo por el que este año 2019 es el ideal para que una certificación profesional criptográfica vea la luz. Dada las necesidades de perfiles técnicos con este conocimiento y las carencias existentes, CriptoCert crea las dos primeras certificaciones técnicas profesionales a nivel mundial en español en el ámbito de la criptografía y la protección de datos y de la información.

Nuevas certificaciones profesionales en criptografía a nivel mundial creadas por CriptoCert

En este mes de abril verá la luz la certificación *CriptoCert Certified Crypto Analyst*, de momento solamente en español (aunque ya está en marcha un proyecto para ofrecerla en inglés próximamente), con el objetivo de capacitar y acreditar de manera rigurosa a profesionales mediante contenidos técnicos extensos, detallados y actualizados. Los alumnos tendrán a su disposición una extensa documentación de más de 800 páginas, que cubre los aspectos más significativos que permiten entender las bases y fundamentos actuales de la mayoría de componentes tecnológicos que hacen uso de la criptografía.

La ambición de esta innovadora iniciativa es extender los complejos conocimientos vinculados al mundo de la criptología a un mayor número de profesionales, para que dispongan de las capacidades de análisis y comprensión de aquellos elementos criptográficos presentes actualmente en infinidad de sistemas, aplicaciones, protocolos, comunicaciones, arquitecturas y dispositivos. El objetivo principal es promover, extender y facilitar la criptográfica y su aplicación para la protección de soluciones y entornos tecnológicos.

Entre estos contenidos se encuentran tanto la introducción al mundo de la seguridad de la información y de la criptografía, clásica y moderna, como los fundamentos matemáticos, de complejidad algorítmica, de teoría de números y de teoría de la información, necesarios para comprender los sistemas criptográficos más complejos actuales. El grueso del contenido, sin embargo, se centra en los diferentes algoritmos y sistemas criptológicos que son ampliamente empleados por las diferentes tecnologías que nos rodean en la actualidad: criptografía simétrica con multitud de sistemas de flujo y de bloque (como A5, RC4, Salsa20 o ChaCha20, y DES, 3DES o AES), criptografía asimétrica con algoritmos de referencia (como DH, RSA o ECC), funciones resumen o hash (como MD5, SHA1, SHA2 o SHA3), sistemas de autenticación (como MAC, HMAC y cifrado autenticado), y sus correspondientes ataques o criptoanálisis. Adicionalmente la documentación profundiza en otros aspectos como certificados digitales, claves criptográficas, algoritmos de derivación de claves, herramientas de cifrado, técnicas de esteganografía y estegoanálisis, criptografía cuántica y postcuántica, o firma digital.

Esta primera certificación se denomina *Analyst*, ya que pretende proporcionar a los profesionales aquellas capacidades para el estudio, la comprensión y el análisis de soluciones criptográficas. El objetivo de la misma, adicionalmente a la formación de los profesionales o empleados de una organización, se centra en acreditar sus conocimientos dentro de la industria (por ejemplo, respecto a terceros), lo que le facilitará el desarrollo de una carrera profesional y de habilidades en esta dirección. La evaluación de los conocimientos asociados a esta certificación se llevará a cabo mediante un examen *online* a distancia, con el objetivo de tener un muy amplio alcance a nivel mundial sobre toda la comunidad técnica hispanohablante (tanto en España e Iberoamérica, como en el resto del mundo), complementado con procedimientos y herramientas de supervisión que permitan asegurar la rigurosidad e integridad del proceso de certificación, para evitar la suplantación de los candidatos y poder así ratificar que los profesionales que obtienen la certificación disponen de los conocimientos y habilidades asociados.

En el año 2020 se espera publicar la certificación complementaria, *CriptoCert Certified Crypto Expert*, como una evolución de la certificación anterior, centrándose en aspectos más específicos y avanzados del mundo de la criptología, y con una especial componente práctica, que tendrá asociada la utilización de laboratorios. Esta segunda certificación se denomina *Expert*, ya que pretende identificar profesionales expertos en soluciones criptográficas, tanto desde un punto de vista ofensivo como defensivo. Obviamente para alcanzar este nivel de conocimientos será necesario obtener previamente la certificación *Analyst*.

En resumen, CriptoCert es una compañía española fundada en este año 2019, de ámbito global, focalizada en la promoción, educación, capacitación técnica y certificación de profesionales en el campo de la criptografía y protección de la información, y especialmente, en su aplicación en el mundo real. La iniciativa surge de la mano de tres reconocidos expertos en el campo de la seguridad informática y la criptografía. Por parte de la red temática Criptored, el doctor **Jorge Ramió** y el doctor **Alfonso Muñoz**, y por parte de la empresa DinoSec especializada en seguridad tecnológica y formación, el experto **Raúl Siles**, todos ellos con una larga trayectoria ampliamente reconocida, tanto a nivel nacional como internacional, y con numerosas menciones y premios a lo largo de su carrera profesional.

La necesidad de difusión de este tipo de conocimientos, y de disponer de certificaciones criptológicas como las planteadas por CriptoCert está reflejada en el interés mostrado por diferentes entidades privadas y organismos gubernamentales, reconociendo la calidad, relevancia y utilidad de las mismas. Especialmente reseñable es el reconocimiento de la certificación por el Centro Criptológico Nacional (CCN).

Esperamos que el esfuerzo, calidad y cariño volcado en esta iniciativa sea del agrado y de utilidad práctica para los profesionales del mundo de la ciberseguridad y tecnologías de la información. Para más información: https://www.criptocert.com ■

Temario de certificación CriptoCert Certified Crypto Analyst

1. Introducción a la seguridad.
2. Teoría de números, teoría de la información y complejidad algorítmica.
3. Introducción e historia de la criptografía.
4. Introducción a la criptografía moderna.
5. Criptografía simétrica.
6. Criptografía asimétrica.
7. Funciones hash.
8. Autenticación.
9. Firma digital.
10. Certificados digitales.
11. Claves criptográficas. Fortalezas, debilidades y gestión.
12. Algoritmos de derivación de claves.
13. Herramientas de cifrado.
14. Esteganografía y estegoanálisis.
15. Criptografía cuántica y postcuántica.

Dr. Jorge Ramió
Dr. Alfonso Muñoz
Raúl Siles
CRIPTOCERT