INTRODUCCIÓN

Los telegramas fueron durante un tiempo el instrumento imprescindible de una sociedad que había encontrado en ellos una nueva vía para favorecer las comunicaciones personales, el progreso de las finanzas y las gestiones políticas, administrativas y militares. Desde su aparición, en la segunda mitad del siglo XIX, los telegramas secretos, cifrados o encriptados eran habituales en las comunicaciones oficiales. El Gobierno Civil era el origen y destino de un flujo continuo de instrucciones, informes, solicitudes y respuestas que lo convertían en el principal activo en la periferia al servicio de la Administración Central del Estado. Una abrumadora cantidad de mensajes, urgentes en su mayoría, y confidenciales, en mayor o menor medida, fueron cobrando protagonismo en los fondos generados por las diversas instituciones del gobierno. No son muchos los telegramas cifrados que han resistido el paso del tiempo en los fondos del Gobierno Civil de Málaga —no así sus contenidos— pero, en octubre de 2017, el Laboratorio de Criptografía y Seguridad de la Información de la Universidad de Málaga recibía un lote de catorce telegramas encriptados procedentes del Archivo Histórico Provincial de Málaga (AHPMA), datados en torno a 1940. El envío se producía como respuesta a la decidida búsqueda de documentos encriptados, aún sin descifrar, que se había iniciado meses atrás, motivada por la considerable cantidad de este tipo de material que todavía se puede encontrar entre los fondos documentales distribuidos por todo el país.

La llegada de los telegramas, identificados bajo la signatura 77145/07, sección Gobierno Civil, del AHPMA, inició de inmediato un proceso de criptoanálisis. Como suele ser habitual, se requería el conocimiento de las técnicas criptográficas aplicadas en la época y del contexto histórico y social en el que fueron utilizados. Las particularidades de este expediente, unidas a la innegable motivación por descifrar los mensajes, pronto dieron sus frutos. A finales de ese mismo año, muy cerca de la inaplazable interrupción navideña en el calendario académico, los telegramas estaban descifrados y el sistema de cifrado utilizado reconstruido por completo. El

cifrado de cinta móvil conocido como "Clave[14] PILAR" volvía a ver la luz casi 80 años después de ser aplicado en las comunicaciones oficiales de la Dirección General de Seguridad en Madrid con el Gobierno Civil de Málaga.

Desde ese instante, comenzaron los esfuerzos por poner en valor los resultados del criptoanálisis que se trasladaron al AHPMA, completando así la información del expediente que contenía estos telegramas. La dirección del Archivo decidió entonces incluirlos en una de las actividades divulgativas que, con periodicidad mensual, organiza en su sede de la calle Martínez de la Rosa: "el documento del mes". Una vitrina con los telegramas, acompañados de los mensajes descifrados y una reconstrucción de la Clave Pilar, dieron forma a la exposición del documento del mes de junio de 2018[15]. Por la novedosa aportación que suponía, fue inaugurada por la Delegada territorial de Cultura en Málaga de la Junta de Andalucía, con el habitual seguimiento de la prensa local, provincial y nacional. No era la primera vez que esta actividad divulgativa, compartida por los Archivos Históricos Provinciales de Andalucía, mostraba documentos de esta naturaleza. En enero de 2014, el Archivo Histórico Provincial de Cádiz expuso una carta cifrada[16] en 1958 con la Clave ESPAÑA, Grupo B, con su correspondiente descifrado, enviada por el Gobierno Civil de Cádiz a la Dirección General de Seguridad en Madrid, con motivo de una visita del jefe del Estado. Todos los documentos se encontraban en el mencionado archivo y, por tanto, no hubo necesidad de realizar un criptoanálisis. Más tarde, en septiembre de 2016, el Archivo Histórico Provincial de Almería expuso un cifrado de cinta móvil, del mismo tipo que el encontrado en Málaga, utilizado en 1945 para las comunicaciones entre la Dirección General de Prisiones y la Prisión de El Acebuche[17].

14. En la época a la que pertenece este sistema, en lugar de la denominación "Sistema de cifrado", "Sistema de encriptado" o "Sistema criptográfico", se utilizaba el término "Clave". Así, "Clave PILAR" es la denominación de un Sistema de encriptado completo y no una clave o contraseña que podría emplearse para descifrar un mensaje concreto [46].
15. Los documentos de la exposición están accesibles en: https://www.juntadeandalucia.es/cultura/archivos/web_es/contenido?id=4c4ad182-67c5-11e8-b0c7-000ae-4865a5f&idActivo=&idContArch=efc4b78f-79de-11dd-8f74-314 50f5b9dd5&idArchivo=cfa8cd88-58a4-11dd-b44b-31450f5b9dd5
16. Los documentos están accesibles en https://dialnet.unirioja.es/servlet/articulo?codigo=7671358
17. La exposición quedó recogida en el periódico digital Noticias de Almería.com, en el siguiente enlace: https://www.noticiasdealmeria.com/noticia/121553/capital/exponen-la-clave-de-los-mensajes-cifrados-que-recibia-el-director-de-la-prision-de-almeria-durante-el-franquismo.html

En cambio, los documentos expuestos en junio de 2018 en el AHPMA han supuesto un interesante hallazgo desde el punto de vista criptográfico al revelar un conjunto de catorce telegramas cifrados con un mismo sistema, la Clave PILAR, de fecha anterior a los mencionados, y dando como resultado principal la reconstrucción del sistema de cifrado completo. Diversos estudios han recogido los numerosos sistemas de encriptado utilizados en España a lo largo de la historia. La Clave PILAR no aparece en estos catálogos, cuya actualización más reciente data de 2016 y puede considerarse la referencia más completa realizada desde el ámbito civil, aunque la mayor parte de los criptosistemas que lo componen sean de uso militar [49]. En consecuencia, ha sido necesario el criptoanálisis y la reconstrucción de todo el sistema de cifrado para, por un lado, descifrar completamente los telegramas y, por otro, completar el catálogo con esta nueva Clave.

Los aspectos más relevantes del proceso de criptoanálisis que permitió la reconstrucción de la Clave PILAR fueron presentados en septiembre de 2018 en el congreso nacional de referencia en materia criptográfica la Reunión Española de Criptología y Seguridad de la Información[18], RECSI 2018, que celebraba en Granada su decimoquinta edición, donde fue seleccionado como mejor trabajo de investigación. Más tarde, en 2019, estos resultados junto con una breve discusión en torno a la ubicación histórica y el significado de los mensajes fueron publicados en la revista *Cryptologia*[19][41].

Tras un período pandémico que ha alterado inexorablemente todas las planificaciones, se presenta este libro que trata de completar la información publicada sobre el proceso criptoanalítico empleado en la reconstrucción de la Clave PILAR y sobre los telegramas cifrados que se pueden encontrar en los fondos del Gobierno Civil de Málaga. En el libro se describen, por una parte, los detalles matemáticos que han permitido, en esta ocasión, obtener éxito en el desafío criptográfico planteado sobre la Clave PILAR. Se profundiza en otros aspectos relacionados con la información que

18. La RECSI es un congreso nacional bienal que reúne a todos los investigadores en criptografía y seguridad de la información del país. Toda la información sobre la edición celebrada en Granada en 2018 se encuentra disponible en https://nesg.ugr.es/recsi2018/.
19. Publicada por la editorial Talylor & Francis, *Cryptologia* es un referente internacional en todos los aspectos relacionados con la Historia de la Criptografía.

ha revelado el criptoanálisis, que sobrepasa el mero descifrado de los mensajes utilizados para transmitir instrucciones de diversa índole desde Madrid, tal como queda recogido en la segunda parte. Por otro lado, los expedientes consultados han revelado telegramas encriptados con otros métodos que, si bien no han requerido un criptoanálisis, han resultado de gran utilidad para conocer más detalles sobre los sistemas utilizados y la operativa empleada en los procesos de cifrado y descifrado. Telegramas remitidos por el Servicio Nacional de Prensa, y otros, relacionados con registros domiciliarios en la ciudad de Antequera, son muestras de lo que albergan los mencionados fondos.

De manera particular, este libro pretende ser una muestra de transversalidad en la que, a través de la criptografía, la ingeniería de telecomunicación proporciona detalles significativos sobre la historia y la evolución de la sociedad de una provincia y de un país. No en vano, podría considerarse que cada momento, cada época, en la historia de las civilizaciones viene determinado por el punto de encuentro entre el estado del arte de la criptografía y de las comunicaciones, hoy, las telecomunicaciones. Las técnicas criptográficas se han ido desarrollando como consecuencia de la necesidad que arrastra el ser humano de comunicarse y de proteger sus comunicaciones; pero, al mismo tiempo, el modo de comunicarse, muy dependiente de la tecnología de cada momento, ha ido determinando la forma en la que las personas se han relacionado y ha obligado también a una continua y progresiva evolución de la criptografía. A un paso de poder aplicar la computación cuántica, que amenaza la criptografía moderna; cuando las *blockchains*[20] son ya una realidad que se extiende mucho más allá de las criptomonedas; cuando el acceso a Internet no tiene secretos para la mayor parte de la población; cuando se ha perdido la cuenta de la generación de comunicaciones móviles que estamos utilizando, porque hemos creado una feroz dependencia del smartphone y de las innumerables redes sociales —las hay para todo— a las que dan acceso; y cuando estamos a punto de que se cumpla el plazo anunciado por las principales compañías operadoras de telecomunicación de Europa sobre el cierre

20. *Blockchain* (cadena de bloques, en español) es un sistema que garantiza la integridad de los datos sobre los que se aplica, esto es, que no sean alterados accidental o maliciosamente sin que se generen evidencias de ello. Aunque es conocido por dar soporte a criptomonedas como el bitcoin, actualmente tiene aplicaciones en todos los campos en los que la protección de datos es una preferencia o una necesidad, como los datos médicos de los pacientes, los procesos electorales o la gestión de las cadenas de suministros [6].

de las centrales de telefonía fija, para dar paso a la *voz sobre IP*[21], aparece este libro sobre telegramas. Lejos de ser anacrónico, supone una oportunidad para revisar la notable influencia de los avances de la telecomunicación en la sociedad, en la que provoca cambios sustanciales en el modo de relacionarse o en la estructura de las Administraciones; pero, al mismo tiempo, mantiene intactos los patrones más elementales de comportamiento, las mismas necesidades básicas, las mismas preocupaciones, los mismos problemas y amenazas. En definitiva, un modo de poner de manifiesto el alto poder de adaptación del ser humano sustentado en gran medida por las mismas debilidades y fortalezas que se mantienen inalteradas con el paso del tiempo y la evolución de la tecnología. La criptografía es una prueba de ello. Se adapta, cambia de forma, utiliza nuevas técnicas, pero mantiene los mismos objetivos. Se revela así un paralelismo perfecto entre la época de los telegramas y el momento actual: el uso generalizado de la mensajería instantánea, en forma de telegrama o a través de un smartphone; la imperiosa necesidad de garantizar el secreto de los mensajes y la permanente preocupación por la posible interceptación de nuestras comunicaciones, hoy bajo el paraguas de la ciberseguridad; la obsesión de algunos por acceder a información ajena; la destreza de unos frente a la torpeza de otros a la hora de aplicar las medidas de seguridad, antes y ahora; o las decisiones políticas frente a los informes de los expertos.

La historia de la criptografía es un reflejo, una proyección, de la historia de la humanidad. Una pequeña muestra de esa historia es la que la primera parte de este libro trata de mostrar describiendo el contexto en el que se desarrolla la criptografía que, de manera particular, fue aplicada a los telegramas recibidos por el Gobierno Civil de Málaga. Tres factores principales son tenidos en cuenta en este contexto histórico que mantiene el foco en el siglo XIX y la primera mitad del XX: las telecomunicaciones, en las que la radiotelegrafía sin hilos generó nuevas oportunidades, con sus ventajas e inconvenientes; la criptografía, como hilo conductor de todo este proceso, analizada desde una perspectiva global para descender hasta los detalles de los sistemas característicos utilizados por las distintas Administraciones españolas; y el Gobierno Civil de Málaga, como centro estra-

21. *La voz sobre IP* es una tecnología que permite transmitir voz digitalizada a través de redes de datos que utilizan el protocolo IP (Internet protocol). Esto permite proporcionar el servicio de telefonía sin necesidad de utilizar centrales de conmutación específicas

tégico de la Administración del Estado y, por tanto, con especial atención a las relaciones con otros organismos como la Dirección General de Seguridad en la capital de España o el Servicio Nacional de Prensa. Este contexto histórico en el que se destaca la influencia y relevancia de las telecomunicaciones en el progreso de la sociedad queda perfectamente representado en la ciudad de Málaga mediante dos edificios singulares y emblemáticos. El primero de ellos, la sede actual del Rectorado de la Universidad de Málaga que ocupa el inmueble que fue, desde 1925 a 1986, la Casa de Correos y Telégrafos de la ciudad. Puede que no sea casual, entonces, que la Universidad se asiente sobre la telecomunicación, al menos en lo que se refiere a sus sedes. El otro edificio es el Palacio de la Aduana, hoy reconvertido en Museo de la ciudad, que albergó la sede del Gobierno Civil, más tarde, Subdelegación del Gobierno, desde 1836 hasta 2007 y la primera oficina telegráfica desde 1857 a 1925.

La segunda parte del libro contiene el criptoanálisis detallado de los telegramas cifrados con la Clave PILAR. Los resultados del análisis preliminar permiten establecer las bases del posterior proceso matemático que queda descrito a continuación junto con sus resultados, esto es, el contenido de los mensajes, la recuperación del sistema de cifrado y la descripción de tres sistemas de cifrado aplicados a telegramas de diversa naturaleza. La última parte del libro contiene una serie de conclusiones y reflexiones sobre la información que se infiere a partir de los datos recuperados de los documentos encriptados.