Prólogo

Es sabido que la necesidad de transmitir y recibir información secreta o confidencial es tan antigua como la Humanidad. Desde siempre, el Hombre ha tenido necesidad de dar a conocer determinada información a sus amigos y aliados y, a la vez, mantenerla en secreto para sus enemigos y adversarios. Fruto de esta necesidad fue el nacimiento de lo que hoy llamamos *criptología*, esto es, la ciencia que se encarga de proporcionar los métodos para el intercambio seguro de información, de modo que solo aquellos autorizados a conocerla sean los que puedan tener acceso a la misma.

Para la transmisión de esta información secreta se recurre a las dos partes en que se divide la criptología: la criptografía y el criptoanálisis. La primera lleva a cabo el diseño de métodos y protocolos que son capaces de transformar, mediante el uso de claves, la información original en otra ilegible, el texto cifrado. Una vez transmitida la información cifrada, solo quien posea la clave correspondiente será capaz de recuperar dicha información.

Por su parte, el criptoanálisis permite garantizar que los sistemas de cifrado o criptosistemas utilizados son seguros, esto es, imposibles de vulnerar sin el conocimiento de la clave necesaria o, dicho de otro modo, un criptoanalista tiene como objetivo estudiar hasta qué punto es posible vulnerar la seguridad de un criptosistema propuesto.

En este texto nos ocuparemos de un tipo especial de criptosistemas, los que emplean como fundamento las curvas elípticas. La criptografía basada en curvas elípticas fue propuesta hace treinta años por Neal Koblitz y Victor Miller, y desde entonces su popularidad y utilización han ido creciendo de

forma continua, y ha dado lugar no solo a sistemas de cifrado sino también a protocolos como los de firmas digitales, algoritmos para la factorización de números enteros, etc.

Las propiedades y posibilidades de utilización de la criptografía con curvas elípticas han sido menos estudiadas que otras opciones criptográficas, lo que ha motivado su menor implantación en el entorno de las soluciones de seguridad hasta hace solo unos pocos años, cuando su irrupción en el mundo de la seguridad ha modificado los planteamientos y desarrollos posteriores. De hecho, algunos estudios realizados (principalmente en el Instituto Nacional de Estandarización y Tecnología norteamericano y en los laboratorios RSA) demuestran que el uso de curvas elípticas en protocolos criptográficos ofrece mejores prestaciones que otras propuestas.

La ventaja de las curvas elípticas en criptografía puede resumirse diciendo que proporcionan una seguridad equivalente a la de otros sistemas propuestos (como el RSA, por ejemplo) pero con longitudes de claves mucho más pequeñas, lo que las convierte en el método idóneo para su uso en dispositivos con poca capacidad de cálculo como tarjetas inteligentes o algunos modelos de tabletas y de teléfonos móviles. Por ello, no es de extrañar que los criptosistemas basados en este tipo de curvas se estén mostrando cada vez más útiles, su importancia vaya aumentando, y se espere que lo siga haciendo cada vez más en el futuro, a medida que se incrementen los requisitos de seguridad.

Todas las razones anteriores son las que nos han llevado a la publicación de este libro, que pretende paliar, en parte, la escasez de obras en español sobre el uso de las curvas elípticas en criptografía. La obra se dirige a lectores familiarizados con la criptología, pero que aún no se han adentrado en el campo de las curvas elípticas, posiblemente por considerarlo más difícil que otros modelos criptográficos o por no poseer el suficiente bagaje de conocimientos como para profundizar en él.

Así, la obra consta de once capítulos y dos apéndices, que pretenden acercar al lector a este campo de la criptografía que ha probado tener un enorme futuro. El libro comienza con dos capítulos que contienen una introducción general a los principales conceptos relacionados con la criptología y sus dos ramas: la criptografía y el criptoanálisis, para pasar a definir y justificar la necesidad de abordar el tema fundamental de la obra, la criptografía basada en curvas elípticas.

A partir de aquí, se presenta una visión monográfica de cómo estas curvas pueden ser empleadas para cifrar y descifrar información. A la vez se abordan y detallan temas colaterales, pero de indudable relevancia, como son las cuestiones relacionadas con la seguridad de estos criptosistemas y la generación de las curvas elípticas para su uso criptográfico, un aspecto cuya importancia ha crecido enormemente a raíz de las noticias y revelaciones en la prensa acerca de la dudosa forma de generar estas curvas que algunas instituciones y estándares han propuesto. Como aplicación inmediata se presenta el esquema de cifrado híbrido definido con curvas elípticas más extendido en la actualidad: ECIES.

A continuación, y dado que uno de los principales atractivos del uso de las curvas elípticas en las aplicaciones criptográficas es la posibilidad de implementar de modo eficiente diferentes protocolos en tarjetas inteligentes, se lleva a cabo una introducción al lenguaje Java, un análisis de las principales bibliotecas criptográficas desarrolladas en este lenguaje para este tipo de criptografía y se comenta la disponibilidad de funcionalidades relacionadas con la criptografía de curvas elípticas en las distintas versiones de Java Card.

Más adelante, se introducen los emparejamientos bilineales, una de las primitivas que está teniendo mayor influencia en muchos protocolos criptográficos dado que, pese a su complejidad conceptual, permite simplificarlos. Con el fin de proporcionar al lector un primer acercamiento a esta primitiva, se define y se muestran solo algunos ejemplos elementales de uso.

Por otra parte, creemos que en un libro dedicado a la protección de la información mediante técnicas criptográficas basadas en curvas elípticas, es importante conocer los algoritmos más utilizados en la implementación de la operación básica empleada, la multiplicación escalar, en dispositivos físicos (que muchas veces disponen de recursos computacionales escasos y de poca capacidad de memoria), así como conocer las principales amenazas a las que están expuestos. En este sentido, se incluyen sendos capítulos dedicados a describir tales algoritmos y a los principales ataques físicos a las implementaciones de los criptosistemas de curva elíptica.

Finalmente, se incluyen dos apéndices donde se tratan, de forma escueta, las características generales de las tarjetas inteligentes y de su principal lenguaje de programación: Java Card.

El libro incluye la lista de las más de trescientas referencias que se han citado a lo largo de los capítulos con el fin de facilitar al lector interesado la ampliación de los contenidos abordados. La obra concluye con el glosario de los términos empleados y un índice alfabético de los principales conceptos tratados en el libro.

Deseamos que la lectura de esta obra permita al lector adentrarse en esta reciente faceta de la criptografía, de modo que las curvas elípticas pasen a formar parte del acervo criptográfico habitual, al igual que términos como RSA, firma electrónica, certificado digital, etc.

Presentación

El libro presenta una introducción a la criptografía basada en curvas elípticas. Este planteamiento general supone abordar temas propios de la criptografía, es decir, de la ciencia que se encarga de proteger la información y asegurar su confidencialidad, integridad y privacidad, mediante el uso de unas herramientas matemáticas conocidas como *curvas elípticas*.

Así pues, se presentarán dichas curvas y se abordarán tanto los criptosistemas de clave pública que las utilizan como otros procedimientos criptográficos que permiten, por ejemplo, el acuerdo de claves y llevar a cabo la firma digital de documentos. En todos estos casos, la seguridad de tales protocolos se basa en la dificultad computacional de resolver eficientemente el problema matemático subyacente, esto es, el problema del *logaritmo elíptico,* también conocido como *logaritmo discreto aditivo*. El atractivo de este tipo de criptosistemas y protocolos estriba en que son necesarias claves con longitudes mucho menores que las utilizadas en otros criptosistemas de clave pública (basados en los problemas de la factorización o del logaritmo discreto, por ejemplo), para conseguir un nivel de seguridad equivalente.

El uso de dispositivos electrónicos con capacidades limitadas de cálculo y almacenamiento está creciendo exponencialmente en los últimos años, y es previsible que lo siga haciendo. Así, es claro que cada vez se usan más, por ejemplo, las tarjetas inteligentes (tarjetas de identificación y pago, de transporte, de telefonía, etc.), y está aumentando la utilización de diferentes dispositivos que llevamos puestos (relojes o pulseras inteligentes, sensores

de ritmo cardíaco, etc.). Es sabido que los recursos de que se dispone en estos casos son mucho menores que los de un ordenador, por lo que resulta innegable la utilidad de disponer para ellos de criptosistemas que utilicen claves cortas. Se trata, en definitiva, de emplear procedimientos que protejan la información almacenada en estos dispositivos y que garanticen la privacidad de los datos de sus propietarios.

Además de proporcionar una introducción a los conceptos básicos de la criptografía basada en curvas elípticas, el libro se complementa con una visión monográfica de cómo se pueden emplear dichas curvas para cifrar y descifrar información, su uso en los protocolos para el acuerdo de claves y los esquemas de firmas digitales. También se tratan los aspectos relacionados con la seguridad y la generación de estas curvas, cuya importancia ha crecido enormemente a raíz de las noticias y revelaciones en la prensa acerca de la dudosa forma de generar estas curvas. Se incluyen, además, otros aspectos prácticos como son los dedicados a la implementación de esta criptografía en ordenadores personales y tarjetas inteligentes, y a los ataques físicos a los que están sometidos actualmente los sistemas que implementan criptografía basada en curvas elípticas.

El principal objetivo de este libro es proporcionar un acercamiento a los principales conceptos relacionados con la criptografía basada en curvas elípticas, destacar su importancia actual y los diferentes campos de aplicabilidad que ofrece, así como mencionar a modo de ejemplo algunas de las aplicaciones a que esta criptografía ha dado lugar desde su propuesta original a mediados de los años ochenta del siglo xx.

El libro va dirigido a un público interesado en las actuales y futuras tendencias en criptografía, no necesariamente experto en la materia. Hemos intentado que su estructura y contenido resulten de utilidad para lectores procedentes de cualquiera de los campos relacionados con la seguridad de la información, como ingenieros o estudiantes de ciencias, pero también para todos aquellos interesados en los sistemas y métodos para la protección de datos personales mediante sistemas de cifrado y descifrado.

La criptografía está estrechamente ligada con las Matemáticas, la Tecnología de las Comunicaciones y la Ciencia de la Computación, por lo que hemos procurado dar una visión global del tema sin profundizar excesivamente en conceptos que no sean estrictamente necesarios. Se trata, en definitiva, de presentar un texto básico pero autocontenido

que permita al lector acercarse a esta moderna faceta de la criptografía. En el libro intentamos explicar esta criptografía de forma relativamente sencilla, evitando, cuando ha sido posible, un excesivo rigor matemático. No hemos profundizado en las aplicaciones de las curvas elípticas porque su inclusión requeriría el estudio de determinadas herramientas matemáticas que sobrepasan los aspectos incluidos en este libro.

La obra contiene algunos capítulos que pueden considerarse estándares sobre curvas elípticas y que el lector puede encontrar en otros libros (fundamentalmente en lengua inglesa) dedicados al mismo tema; no obstante, hemos de señalar que pretendemos huir del enfoque tradicional en el que los conceptos matemáticos se presentan y definen en capítulos independientes, que luego se utilizan en otros capítulos del libro. En nuestro caso hemos introducido los conceptos matemáticos necesarios en el momento que hacían falta, tratando de evitar los aspectos abstractos que suelen acompañarlos. Los restantes capítulos y los dos apéndices abordan temas que, en nuestro conocimiento, no se han incluido en libros publicados en los últimos años.