



# INTRODUCCIÓN A LA CRIPTOGRAFÍA

## 2ª edición actualizada

**Autor:** Pino Caballero Gil

**Editorial:** Ra-Ma

**Año 2002 –133 páginas –ISBN: 84-7897-520-9**

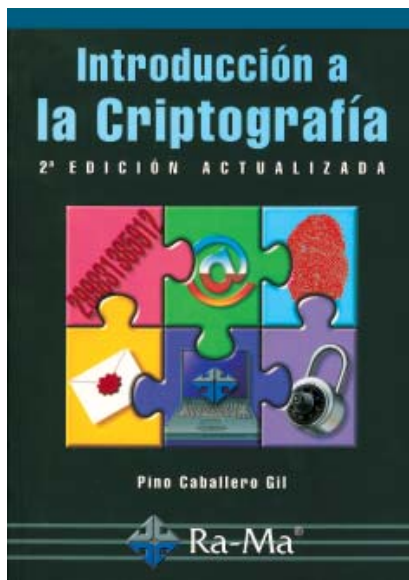
**www.ra-ma.es**

Decía un insigne orador (creo recordar que el psiquiatra Vallejo Nájera) que la preparación de una conferencia de una hora le llevaba diez minutos, mientras que si su duración era de diez minutos en su preparación invertía una hora. Y la frase, en el fondo, es mucho más que una divertida ocurrencia. En efecto, como todo el mundo conoce, la síntesis es un proceso intelectual complejo y laborioso, y estructurar en un escaso espacio (temporal o espacial) una materia, incluyendo sólo lo sustancial y haciéndolo comprensible por los más de los oyentes o lectores es una tarea nada trivial.

Pero además, si la materia a tratar es la criptografía la tarea citada presenta aún mayores dificultades. Y es que, de hecho, de los varios campos de que conforman la seguridad de las Tecnologías de la Información, sin ningún género de dudas es la criptografía el más complejo, doctrinal y extenso de todos. Por ello, es también la materia que más dificultades expositivas presenta, estando su tratamiento reservado a aquellos que aúnan acreditadas dotes didácticas con un conocimiento profundo de la disciplina. Pues bien, todo ello se conjuga en la profesora de la Universidad de La Laguna **Pino Caballero Gil** –autora del libro que en esta ocasión reseñamos–, cuya trayectoria profesional desde que concluyó sus estudios (primero como investigadora en el CSIC y luego como docente e investigadora) ha estado centrada en la disciplina aludida, en la que está públicamente reconocida como una reputada experta.

La obra en cuestión, de título **Introducción a la Criptografía**, está editada por **Ra-Ma** en el pasado año y, como atinadamente sugiere su nombre, es una primera aproximación a esta materia, que ha estado tan vinculada desde la antigüedad a la seguridad. No obstante, y contrariamente a lo que a menudo sucede con las obras adjetivadas de introducción, en ésta el carácter introductorio no menoscaba el número de aspectos tratados, que son prácticamente todos los relevantes en el presente, ni mucho la amplitud de miras con que se exponen. Es en este difícil arte de concentrar los conceptos fundamentales en su punto justo, –que permite conjugar una visión totalizadora en un manual compacto– donde radica el principal activo del libro.

Por otro lado, es de celebrar un hecho singular en la bibliografía de la seguridad en nuestro país, y es que se trata de la segunda edición de la obra, lo



que constituye todo un aval para la misma –y por ende para su autora–, además de ser un motivo de satisfacción para todos cuantos nos hemos esforzado desde hace años en elevar la disciplina al lugar que hoy va alcanzando en nuestro país.

La obra se articula en cuatro capítulos que se despliegan en 115 densas (aunque, como se ha comentado, en absoluto ilegibles) páginas en las que se comprenden desde los fundamentos teóricos hasta algunas aplicaciones criptográficas actuales. A menudo, estas páginas se ven jalonadas por notas sombreadas que contribu-

yen poderosa y atinadamente a centrar la atención en conceptos o aspectos relevantes. Además, no es posible ignorar las doce páginas de bibliografía (completísima, como cabe suponer en una profesora universitaria), en la que se pueden hallar prácticamente todas las referencias a las aportaciones más relevantes de la materia.

Comienza el manual con un breve capítulo, de sólo quince páginas, de título: **Criptografía teórica**, en el que se repasan las bases mínimas de la disciplina, principalmente la teoría de la información, pues otros fundamentos de la misma o se tratan posteriormente en el momento en que se precisan (por ejemplo, los conceptos necesarios de la teoría de números, contemplados durante la exposición del RSA, Rabin, o Merkle-Hellman) o bien se soslayan por no ser imprescindibles en el resto del libro (como ocurre con la teoría de complejidad algorítmica, o ciertos aspectos de la estadística, necesarios si la obra hubiese sido un tratado exhaustivo). Esta elección contribuye a hacer del capítulo un compendio mínimo, y por tanto de lectura menos pesada de lo que es costumbre en otros títulos, que tienden a englobar todos los fundamentos en un único y extenso capítulo, que resulta a la postre irremediablemente agotador para el lector.

El capítulo segundo: **Criptografía de clave secreta**, comienza exponiendo con concisión la criptografía clásica (cifrados de sustitución mono y polialfabéticos, homofónicos y poligráficos) y con más brevedad aun su criptoanálisis (método de Kasiski e índice de coincidencia), para seguidamente detenerse en los cifrados en bloque, con especial atención al DES –evidentemente por su carácter ejemplarizante de los restantes métodos en bloque–, para continuar con su sucesor, el Rijndael (base del nuevo estándar estadounidense AES), y, a modo de

cita, con el IDEA y el RC-5. El cifrado en flujo se aborda en el apartado siguiente, donde tras contemplar la pseudoaleatoriedad de las secuencias cifrantes, se detiene en los generadores de éstas (registros de desplazamiento, filtrado y combinadores no lineales). Por último se concluye con un apartado consagrado al intercambio de claves (clásico, mediante claves jerárquicas, y más moderno, mediante negociación de Diffie-Hellman), aunque el apartado lleve por nombre el más extenso y equívoco de Gestión de Claves, que obviamente desborda lo tratado.

En el capítulo siguiente: **Criptosistemas de clave pública**, como prólogo se introducen las transformaciones que fundamentan los sistemas asimétricos: las funciones irreversibles con trampa, y las ideas de los autores de aquellos sistemas, Diffie y Hellman. El apartado que sigue, consagrado al algoritmo RSA, es lo suficientemente amplio como para adentrarse en la elección de los primos  $p$  y  $q$  –con los consiguientes test de primalidad–, cuyo producto genera la base de la aritmética modular, así como diversos ataques a este criptosistema. Acertadamente, menor extensión se reserva para los algoritmos de Rabin, El Gamal y Merkle-Hellman (cuya inclusión, hoy en día, no deja de ser cuestionable), mientras que con algo más de detenimiento se estudia el sistema de McEliece. Pero posiblemente uno de los apartados más logrados sea el dedicado a los criptosistemas basados en curvas elípticas, magníficamente expuestas, que en pocas páginas permite hacerse una completa idea, en primer lugar de las mismas, y después de sus aplicaciones en el cifrado. Para finalizar, un último apartado se dedica a presentar las ventajas e inconvenientes de los sistemas expuestos.

Finalmente, el capítulo cuatro, **Aplicaciones criptográficas**, recoge los usos de la criptografía en la autenticación, firma digital y protocolos criptográficos. En el primero de ellos, tras una muy interesante presentación de los retos a los que se enfrenta la autenticación, se esbozan, tan sólo, algunos esquemas básicos de la misma. En cuanto a la firma y después, nuevamente, de un sugestivo prólogo de sus requisitos, se estudian concisamente los esquemas del RSA, El Gamal y Fiat-Shamir, para terminar con un estudio de las funciones resumen (*hash*) y los certificados digitales. No se entiende, sin embargo, que el DSS, sólo merezca una mención de una línea, pues su importancia actual hubiese debido destinarle, al menos, el espacio dedicado a los restantes esquemas reseñados. Finalmente, un último apartado, de protocolos criptográficos, recoge un selecto grupo de éstos como, por ejemplo, los de firma de contratos, conocimiento nulo o votaciones electrónicas, ejemplificadores de la versatilidad, potencia y aplicaciones de la criptografía.

En resumen, una obra muy notable que merece formar parte del fondo bibliográfico de todos los concernidos por la seguridad, o simplemente interesados en la pujanza de esta ancestral disciplina que vive días de gloria como nunca antes lo había conocido. ■

**ARTURO RIBAGORDA GARNACHO**

Catedrático y Director del Dpto. de Informática

**UNIVERSIDAD CARLOS III DE MADRID**

arturo@inf.uc3m.es