LIBRO ELECTRÓNICO DE SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA

PRÓLOGO DE LA SEXTA EDICIÓN v4.1 EN INTERNET
Madrid, 1 de marzo de 2006

Estimados amigos y amigas:

Con un nivel de descargas de la versión anterior 4.0 que se han acercado nuevamente a las 40.000 durante un año, a estas alturas las palabras sobran.

En esta sexta edición nuevamente he contado con la inestimable colaboración del Dr. Josep María Miret Biosca, profesor de la Universitat de Lleida, en el capítulo dedicado a curvas elípticas que se ha reestructurado. En cuanto a los demás capítulos, todos han sido revisados y en su gran mayoría actualizados. Las mayores novedades las encontrará en el capítulo de cifra simétrica con el algoritmo AES y en el capítulo de cifra asimétrica con una profundización en la generación de claves y debilidades en RSA.

Se han aumentado los enlaces a páginas Web y en el último capítulo se recogen todos estos sitios Web con una breve descripción del contenido de la página.

Así, esta versión 4.1 cuenta con un total del 1.106 diapositivas, casi una centena más que la versión anterior.

Espero que este libro electrónico le sea de utilidad en su aprendizaje de la criptografía, una apasionante rama de la seguridad informática en la que está principalmente enfocado.

Muchas gracias a todos
El autor
Madrid, 1 de marzo de 2006

PRÓLOGO DE LA QUINTA EDICIÓN v4.0 EN INTERNET
Madrid, 1 de marzo de 2005

Estimados compañeros de ruta:

Permítanme esta licencia en la forma de saludo del prólogo de esta quinta edición. La razón de este trato tan personal radica en la certeza de que muchos de aquellos amigos/as que ya han leído, estudiado e incluso impartido clases y conferencias con esta documentación, se descargarán la nueva edición y seguirán profundizando en estos temas apasionantes de la criptografía y la protección de la información, al igual que debo hacerlo yo –no queda otro remedio en esta cambiante especialidad- de cuando en cuando.

Como corresponde a cualquier nueva versión, los capítulos han sido actualizados y además se ha incluido uno nuevo sobre la cifra con curvas elípticas, gracias a la colaboración del Dr. Josep María Miret Biosca, profesor de la Universidad de Lleida; a quien desde este prólogo agradezco su excelente predisposición para entregarme sus notas sobre este tema y que en

próximas ediciones actualizará. Además, a diferencia de la versión v3.2, los archivos tienen cada uno un nombre relacionado con el tema que trata para una búsqueda más rápida.

Como novedad docente, he creído oportuno incluir en algunas diapositivas enlaces a páginas Web, de forma que pinchando en el icono correspondiente podamos acceder directamente a ese sitio y contrastar información. Además, en tanto la teoría en ingeniería poco o nada vale si no va asociada con unas prácticas, al final de los capítulos que así lo requieren, se han añadido diversos ejercicios prácticos para realizarlos con programas y aplicaciones de tipo freeware.

De esta forma, la versión v4.0 cuenta con un total del 1.030 diapositivas, una centena más que la versión anterior. Además, puede descargar un documento en Word de 106 páginas sobre criptografía clásica desde http://www.criptored.upm.es/descarga/CriptoClasica.zip

Nuevamente, mil gracias a todos y todas por hacer de este libro electrónico un verdadero *boom* editorial en Internet , lo cual no deja de sorprenderme al constatar que de la versión v3.2 que con fecha de hoy ha quedado ya obsoleta, las descargas en un año han llegado a la nada despreciable cifra de 40.000.

Dr. Ingeniero de Telecomunicación Diplomado por la Universidad Politécnica de Madrid.
Profesor titular del Departamento de Lenguajes, Proyectos y Sistemas Informáticos de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid.
Es profesor y coordinador de la asignatura de Seguridad Informática que se imparte desde el año 1994 como asignatura optativa de tercer curso en la titulación de Ingeniero Técnico en Informática de Gestión del Plan de Estudios 1992.
Desde el año 2005 es el coordinador de una nueva asignatura de libre elección Gestión, Auditoría, Normativas y Legislación en Seguridad Informática, cuya particularidad es que los docentes serán conferenciantes invitados de diversos organismos, empresas e instituciones, expertos en el tema.
Es el creador y coordinador de CriptoRed, la Red Temática Iberoamericana de Criptografía y Seguridad de la Información, en la que participan más de 550 expertos e investigadores de 160 universidades y centros de investigación, así como empresas de sector de las NTIs, desde cuyo servidor se descargan más de 25.000 documentos mensualmente.
Fue partner de la Red ECET, European Computer Education and Training (2001-2004), y a partir de 2005 de Red ETN DEC European Thematic Network for Doctoratal Education in Computing, cuyo objetivo es el análisis de los estudios de doctorado.
Desde el año 2000 viene impartiendo diversas conferencias y escribiendo documentos en los que hace ver la necesidad de crear un espacio docente para la introducción de las asignaturas relacionadas con la seguridad informática en los planes de estudios universitarios y la creación de una Ingeniería en Seguridad Informática.
Es miembro del Subcomité de Seguridad de Tecnologías de la Información (SC 27) del Comité Técnico de Normalización de Tecnología de la Información (CTN 71) de AENOR.
Es miembro del comité de revisores de IEEE América Latina.
Ha participado en numerosos congresos en calidad de conferenciante invitado, moderador de sesión, miembro del comité organizador o miembro del comité de programa.
A fecha de enero de 2006, ha impartido diversos cursos, charlas y conferencias sobre criptografía, seguridad informática y la red temática en: Argentina, Bolivia, Brasil, Bulgaria, Chile, Colombia, Costa Rica, Cuba, España, México, Panamá, Perú, República Dominicana, Uruguay y Venezuela.

✉ jramio@eui.upm.es
Web personal: http://www.lpsi.eui.upm.es/~jramio
Web asignatura SI: http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm
Web asignatura GANLESI: http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm
Web CriptoRed: http://www.criptored.upm.es/