

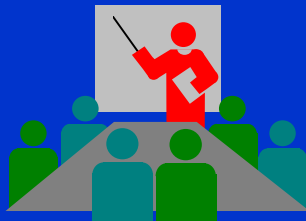
Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1

Sexta edición de 1 de Marzo de 2006

Capítulo 1. Presentación del Libro Electrónico



v 4.1



Material Docente de
Libre Distribución

Libro electrónico con: 1.106 diapositivas

Este archivo tiene: 33 diapositivas

Ultima actualización: 01/03/06

Dr. Jorge Ramió Aguirre

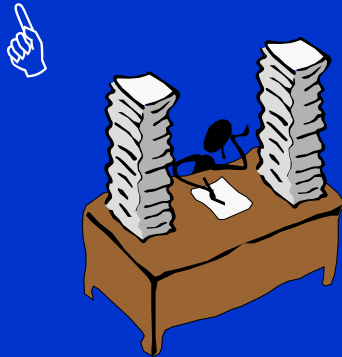
Universidad Politécnica de Madrid

Colaboración del Dr. Josep María Miret Biosca
(U. de Lleida) en capítulo 20: Curvas Elípticas

Este archivo forma parte de un curso completo sobre Seguridad Informática y Criptografía. Se autoriza el uso, reproducción en computador y su impresión en papel, sólo con fines docentes y/o personales, respetando los créditos del autor. Queda prohibida su comercialización, excepto la edición en venta en el Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España.

Los derechos de autor en el freeware

Este libro electrónico es el resultado de miles de horas de trabajo. Recuerde que freeware no le da derecho para **apropiarse** del trabajo de otros, sino **compartirlo**.



ISBN: 84-86451-69-8 (2006)
Versión 4.1 impresa - EUI - UPM
Depósito Legal: M-10039-2003

Este documento electrónico puede ser descargado libre y gratuitamente desde Internet para su ejecución e impresión, solamente para fines educativos y/o personales, respetando en todo caso su integridad y manteniendo siempre los créditos del autor en el pie de página.

Si lo desea, puede utilizar partes del libro como material de apoyo didáctico para docencia sin solicitar autorización previa ni incluir los créditos de autor.

Queda por tanto prohibida su venta, excepto a través del Departamento de Publicaciones de la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España.

Temas del curso

Página de diapositiva

Capítulo 01: Presentación del Libro Electrónico	1
Capítulo 02: Una Breve Introducción a la Criptografía	34
Capítulo 03: Introducción a la Seguridad Informática	49
Capítulo 04: Calidad de Información y Programas Malignos	105
Capítulo 05: Introducción a la Gestión de la Seguridad	132
Capítulo 06: Teoría de la Información	178
Capítulo 07: Teoría de los Números	237
Capítulo 08: Teoría de la Complejidad Algorítmica	312
Capítulo 09: Sistemas de Cifra Clásicos	343
Capítulo 10: Introducción a la Cifra Moderna	384
Capítulo 11: Sistemas de Cifra en Flujo	419

Temas del curso

Página de diapositiva

Capítulo 12: Cifrado Simétrico en Bloque	472
Capítulo 13: Cifrado Asimétrico con Mochilas	591
Capítulo 14: Cifrado Asimétrico Exponencial	621
Capítulo 15: Funciones Hash en Criptografía	710
Capítulo 16: Autenticación y Firma Digital	744
Capítulo 17: Certificados Digitales y Estándar PKCS	807
Capítulo 18: Aplicaciones de Correo Seguro	828
Capítulo 19: Protocolos y Esquemas Criptográficos	928
Capítulo 20: Introducción a la Cifra con Curvas Elípticas	998
Capítulo 21: Bibliografía, Enlaces, Tablas, Software y Documentos	1.028
Total diapositivas de la versión 4.1	1.106

Resumen del Contenido

	Página
Capítulo 01: Presentación del Libro Electrónico	1
Capítulo 02: Breve Introducción a la Criptografía	34
- <i>Definición de criptografía</i>	39
- <i>Confidencialidad e integridad</i>	40
- <i>Clasificación de los criptosistemas</i>	41
- <i>Criptosistemas simétricos</i>	43
- <i>Criptosistemas asimétricos</i>	44
- <i>Sistema de cifra híbrido</i>	48
Capítulo 03: Introducción a la Seguridad Informática	49
- <i>Definiciones</i>	53
- <i>Principios de la seguridad informática</i>	62
- <i>Amenazas del sistema</i>	66
- <i>Debilidades del sistema</i>	73
- <i>Elementos de la seguridad informática</i>	75
- <i>Esquema de un criptosistema</i>	79
- <i>Recomendaciones de Bacon</i>	87
- <i>Recomendaciones de Kerkchoffs</i>	88

Resumen del Contenido

- <i>Fortaleza y tipos de ataques</i>	89
- <i>Cifrado en bloque vs cifrado en flujo</i>	91
- <i>Confidencialidad vs integridad sistemas simétricos y asimétricos</i>	93
Capítulo 04: Calidad de Información y Programas Malignos	105
- <i>Concepto e importancia de la información</i>	106
- <i>Vulnerabilidad de la información</i>	110
- <i>Acciones contra los datos</i>	112
- <i>Ataques y delitos informáticos</i>	117
- <i>Ataques y delitos recientes</i>	123
- <i>Introducción a los virus informáticos</i>	124
Capítulo 05: Introducción a la Gestión de la Seguridad	132
- <i>Protección lógica y física de los datos</i>	133
- <i>Análisis de riesgo</i>	135
- <i>Políticas de seguridad</i>	145
- <i>Modelos de seguridad</i>	149
- <i>Criterios y normativas de seguridad</i>	153
- <i>Leyes de seguridad informática en España LOPD</i>	154
- <i>Norma ISO 17799</i>	161
- <i>Planes de contingencia</i>	164
- <i>Acciones en un SGSI y PDCA</i>	165

Resumen del Contenido

- <i>Recuperación ante desastres</i>	171
Capítulo 06: Teoría de la Información	178
- <i>Cantidad de información</i>	183
- <i>Definición logarítmica de la cantidad de información</i>	190
- <i>Grado de indeterminación de la información</i>	191
- <i>Entropía de los mensajes</i>	196
- <i>Codificador óptimo</i>	199
- <i>Entropía condicional</i>	202
- <i>La ratio del lenguaje</i>	205
- <i>Redundancia del lenguaje</i>	209
- <i>Secreto en un sistema criptográfico</i>	215
- <i>La distancia de unicidad</i>	223
- <i>Esquema de un cifrador aleatorio</i>	224
- <i>Cantidad de trabajo en criptoanálisis</i>	230
Capítulo 07: Teoría de los Números	237
- <i>Propiedades de la congruencia y operaciones</i>	240
- <i>Conjunto completo de restos</i>	243
- <i>Homomorfismo de los enteros</i>	244
- <i>Divisibilidad de los números</i>	246

Resumen del Contenido

- <i>Inversos en un cuerpo</i>	249
- <i>Conjunto reducido de restos</i>	255
- <i>Función de Euler</i>	257
- <i>Teorema de Euler</i>	263
- <i>Algoritmo extendido de Euclides</i>	269
- <i>Cálculo de inversos con el Algoritmo extendido de Euclides</i>	271
- <i>Teorema del resto chino</i>	275
- <i>Algoritmo de exponenciación rápida</i>	287
- <i>Distribución de números primos</i>	291
- <i>Raíz primitiva de un cuerpo</i>	292
- <i>Cálculos en campos de Galois</i>	302
Capítulo 08: Teoría de la Complejidad Algorítmica	312
- <i>Número de operaciones bit</i>	314
- <i>La función $O(n)$</i>	316
- <i>Algoritmos de complejidad polinomial P</i>	319
- <i>Algoritmos de complejidad no determinista NP</i>	321
- <i>El problema de la mochila</i>	326
- <i>El problema de la factorización</i>	330
- <i>El problema del logaritmo discreto</i>	333
- <i>Logaritmo discreto con valores de α</i>	336

Resumen del Contenido

Capítulo 09: Sistemas de Cifra Clásicos	343
- <i>Clasificación histórica de la criptografía clásica</i>	346
- <i>Herramientas de la criptografía clásica</i>	348
- <i>Clasificación de los sistemas de cifra clásica</i>	349
- <i>Cifrador escítala</i>	351
- <i>Cifrador de Polybios</i>	353
- <i>Cifrado por sustitución del César y criptoanálisis</i>	354
- <i>Cifrador monoalfabeto afín y criptoanálisis</i>	357
- <i>Cifrador polialfabético de Vigenère</i>	359
- <i>Criptoanálisis de Vigenère por método de Kasiski</i>	361
- <i>Regla AEO de ataque por Kasiski</i>	364
- <i>Índice de Coincidencia IC</i>	365
- <i>Cifrador poligrámico de Playfair</i>	365
- <i>Cifrador poligrámico con matrices de Hill</i>	368
- <i>Criptoanálisis de Hill por el método de Gauss Jordan</i>	372
- <i>Cifrador de Vernam</i>	375
Capítulo 10: Introducción a la Cifra Moderna	384
- <i>Clasificación de los criptosistemas modernos</i>	386
- <i>Introducción al cifrado en flujo</i>	387
- <i>Introducción al cifrado en bloque</i>	391

Resumen del Contenido

- <i>Funciones unidireccionales con trampa</i>	396
- <i>Cifrado con clave pública de destino</i>	399
- <i>Cifrado con clave privada de origen</i>	405
- <i>Comparativa entre cifrado simétrico y asimétrico</i>	408
Capítulo 11: Sistemas de Cifra en Flujo	419
- <i>Cifrador de flujo básico</i>	420
- <i>Rachas de dígitos</i>	422
- <i>Autocorrelación fuera de fase</i>	424
- <i>Postulados de Golomb G1, G2, G3</i>	427
- <i>Generador de congruencia lineal</i>	436
- <i>Registros de desplazamiento</i>	440
- <i>Introducción a los autómatas celulkares</i>	441
- <i>Generadores no lineales: NLFSR</i>	442
- <i>Generadores lineales: LFSR</i>	444
- <i>Ataque de Berlekamp-Massey</i>	455
- <i>Complejidad lineal</i>	459
- <i>Operaciones con dos registros y filtrado no lineal</i>	460
- <i>Algoritmos de cifra A5/1 y A5/2</i>	463
Capítulo 12: Cifrado Simétrico en Bloque	472
- <i>Cifradores tipo Feistel</i>	474

Resumen del Contenido

- *Cifradores de bloque más conocidos* 477
- *Data Encryption Standard DES* 485
- *Cajas S en DES* 496
- *Modos de cifra ECB, CBC, CFB* 508
- *Cifrado múltiple y ataque meet-in-the-middle* 516
- *Triple DES* 520
- *International Data Encryption Standard IDEA* 522
- *Algoritmos RC2, RC5, SAFER, Blowfish, CAST, Skipjack* 539
- *Desafíos al DES: DES Challenge I, II y III* 555
- *AES, algoritmo Rijndael* 549
- *Esquema general del AES y sus funciones* 557
- Capítulo 13: Cifrado Asimétrico con Mochilas** **591**
- *El problema de la mochila* 592
- *Mochila simple o supercreciente* 597
- *Mochila de Merkle y Hellman* 600
- *Criptoanálisis a mochilas, Shamir y Zippel* 610
- Capítulo 14: Cifrado Asimétrico Exponencial** **621**
- *Cifrado exponencial con clave de destino y de origen* 624
- *Intercambio de clave de Diffie y Hellman* 629
- *Algoritmo de cifra RSA* 638

Resumen del Contenido

- <i>Uso del Teorema del Resto Chino en RSA</i>	642
- <i>Ataque por factorización de n</i>	645
- <i>Elección de números primos seguros</i>	650
- <i>Claves privadas parejas</i>	653
- <i>Claves públicas parejas</i>	659
- <i>Números N no cifrables</i>	662
- <i>Distribución de números no cifrables</i>	666
- <i>Ataque al secreto de N por cifrado cíclico</i>	673
- <i>La paradoja del cumpleaños</i>	676
- <i>Ataque a la clave privada por paradoja del cumpleaños</i>	677
- <i>La otra historia de RSA</i>	683
- <i>Algoritmo de cifra de Pohlig y Hellman con clave secreta</i>	684
- <i>Algoritmo de cifra de ElGamal</i>	687
- <i>Elección del tamaño del bloque para cifras de mensajes</i>	692
- <i>Fortaleza y resumen de la cifra exponencial</i>	694
Capítulo 15: Funciones Hash en Criptografía	710
- <i>Uso de las funciones hash en criptografía</i>	711
- <i>Propiedades de las funciones hash</i>	714
- <i>Funciones hash más conocidas</i>	717
- <i>Algoritmo de resumen Message Digest 5 MD5</i>	718

Resumen del Contenido

- <i>Algoritmo de resumen Secure Hash Algorithm SHA-1</i>	728
- <i>Comparativas entre MD5 y SHA-1</i>	733
- <i>Últimos ataques a las funciones hash</i>	738
Capítulo 16: Autenticación y Firma Digital	744
- <i>Los problemas de la integridad</i>	746
- <i>Escenarios integridad</i>	748
- <i>Autenticación con sistemas simétricos</i>	751
- <i>Autenticación con MAC o Checksum</i>	753
- <i>Autenticación con HMAC</i>	756
- <i>Autenticación de Needham y Schroeder</i>	761
- <i>Autenticación con Kerberos</i>	765
- <i>Características de la firma digital</i>	775
- <i>Firmas digitales simétricas</i>	776
- <i>Firmas digital de Desmedt</i>	777
- <i>Autenticación con sistemas asimétricos</i>	779
- <i>Firma digital RSA</i>	780
- <i>Vulnerabilidades de la firma RSA</i>	784
- <i>Firma digital ElGamal</i>	786
- <i>Estándares de firma digital</i>	791
- <i>Firma digital DSS Digital Signature Standard</i>	792

Resumen del Contenido

- Seguridad de la firma digital DSS	798
- Mensajes sin firma en DSS	799
- Firmas simétricas versus asimétricas	801
Capítulo 17: Certificados Digitales y Estándar PKCS	807
- Certificado digital X.509	809
- Introducción a las Autoridades de Certificación	812
- Certificado digital para correo de Verisign	816
- Certificado de Verisign en Outlook Express	818
- Estándar PKCS Public Key Cryptography Standards	822
- PKCS #1 RSA Cryptography Standard	824
Capítulo 18: Aplicaciones de Correo Seguro	828
- Private Enhanced Mail PEM	830
- Pretty Good Privacy PGP	834
- Cifrado local o convencional	839
- Generación de claves asimétricas y anillos de claves	843
- Estructura del anillo de claves privadas	845
- Estructura del anillo de claves públicas	847
- Gestión del anillo de claves públicas	849
- Cifrado con clave pública de destino	852
- Descifrado con clave privada de destino	854

Resumen del Contenido

- <i>Firma digital RSA</i>	856
- <i>Formato de un mensaje PGP</i>	858
- <i>Algoritmos en nuevas versiones de PGP</i>	860
- <i>Instalación de PGP versión 6.5.1</i>	862
- <i>Generación de claves PGP 6.5.1 con PGPkeys</i>	873
- <i>Gestión de claves PGP 6.5.1</i>	883
- <i>Operaciones con el portapapeles en la versión 6.5.1</i>	889
- <i>Características PGP Versión 7.0.3</i>	895
- <i>Cifrado en modo SDA con PGP 7.0.3</i>	901
- <i>Borrado físico de archivos con PGP 7.0.3</i>	903
- <i>Características PGP Versión 8.0</i>	904
- <i>Operación wipe free space con PGP 8.0</i>	909
- <i>Recomendaciones con las claves PGP</i>	911
- <i>GnuPG Gnu Privacy Guard</i>	912
- <i>Correo seguro a través de S/MIME</i>	913
Capítulo 19: Protocolos y Esquemas Criptográficos	925
- <i>Definición y ejemplos de protocolos criptográficos</i>	926
- <i>Protocolo de firma ciega de Chaum</i>	932
- <i>Transferencia inconsciente o trascordada de Rabin</i>	935
- <i>El problema del lanzamiento de la moneda</i>	943

Resumen del Contenido

- *Solución según el esquema de Blum* 945
- *Restos cuadráticos y enteros de Blum* 947
- *Algoritmo de Blum* 952
- *La firma de contratos* 955
- *Firma de contratos según algoritmo de Even* 959
- *Correo electrónico certificado* 962
- *Protocolo de póquer mental* 967
- *Protocolo de póquer mental con RSA* 969
- *Canal subliminal* 972
- *Transferencia con conocimiento nulo* 974
- *Esquema de transferencia con conocimiento nulo de Koyama* 975
- *Voto electrónico y esquema electoral* 979
- Capítulo 20: Introducción a la Cifra con Curvas Elípticas** **998**
- *Introducción a las curvas elípticas* 1.000
- *Conjunto y suma de puntos de una curva elíptica* 1.002
- *Curvas elípticas sobre cuerpos finitos* 1.006
- *Criptosistemas con curvas elípticas* 1.008
- *Criptosistema de ElGamal elíptico* 1.009
- *ElGamal elíptico versus ElGamal multiplicativo* 1.014
- *Tamaños de la clave* 1.015

Resumen del Contenido

- <i>Dificultad del PLDE</i>	1.016
- <i>Firma digital con curvas elípticas ECDSA</i>	1.017
- <i>Curvas elípticas criptográficamente útiles</i>	1.021
- <i>ECC challenge</i>	1.022
- <i>Software libre para usar curvas elípticas</i>	1.025
Capítulo 21: Bibliografía, Enlaces, Tablas, Software y Documentos	1.028
- <i>Bibliografía recomendada en castellano</i>	1.029
- <i>Bibliografía recomendada en inglés</i>	1.037
- <i>Enlaces a páginas Web de capítulos</i>	1.046
- <i>Enlaces de interés en Internet</i>	1.063
- <i>Tablas de frecuencia de monogramas</i>	1.066
- <i>Tablas mod 27 y mod 37 con inversos</i>	1.068
- <i>Tabla de Vigenère</i>	1.070
- <i>Tabla código Baudot</i>	1.071
- <i>Tablas ASCII y ANSI</i>	1.072
- <i>Tabla y ejemplo código base 64</i>	1.076
- <i>Tablas de primos del 2 al 1.999</i>	1.078
- <i>Tabla de polinomios primitivos</i>	1.080

Resumen del Contenido

- <i>El proyecto docente Criptolab</i>	1.081
- <i>Cuaderno de prácticas en html</i>	1.082
- <i>Software para prácticas</i>	1.085
- <i>Formación universitaria de seguridad informática en España</i>	1.097
- <i>Propuesta de formación para un Máster en Seguridad Informática</i>	1.100
- <i>Palabras finales de autor</i>	1.106

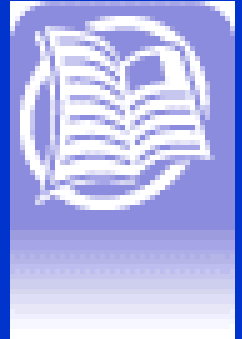
Documento Anexo

- “*Criptosistemas Clásicos*” correspondiente al tercer capítulo del libro “*Aplicaciones Criptográficas*” (1999) que puede descargar desde este enlace:

<http://www.criptored.upm.es/descarga/CriptoClasica.zip> 

Uno de los primeros libro de la asignatura

“Aplicaciones Criptográficas”, 2ª edición, Junio de 1999
Departamento de Publicaciones - Escuela Universitaria de
Informática - Universidad Politécnica de Madrid
Carretera de Valencia km. 7 - 28031 Madrid (España)
I.S.B.N.: 84-87238-57-2. Depósito Legal: M-24709-1999



“Si dotamos a Internet de las medidas de protección y seguridad que nos ofrecen las técnicas criptográficas, dejará de ser ese peligroso y caótico tablón de anuncios para convertirse en el supermercado electrónico del futuro y la herramienta de trabajo de la generación del próximo siglo.”

A Anita y Jordi

Adquisición de edición impresa del libro

- Este libro electrónico, en su condición de curso en diapositivas de libre distribución en Internet, es parte del material docente que se usa en la asignatura de **Seguridad Informática** y que el autor imparte desde el año 1994 en la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España.
- La versión 4.1 del libro ha sido editada por el Departamento de Publicaciones de la Escuela Universitaria de Informática con ISBN: 84-86451-69-8 (2006).
- Para cualquier consulta en este sentido sobre condiciones de compra y envío del mismo, dentro o fuera de España, por favor póngase en contacto con el Departamento de Publicaciones de la EUI-UPM, Carretera de Valencia Km 7, código postal 28031, Madrid, España. Por email a publicaciones@eui.upm.es o bien telefónicamente al número +34 91 3367905.

Instalación y actualización

Al descomprimir **SegInfoCrip_v41.zip**, acepte el nombre completo de los archivos del libro y éstos se guardarán en la carpeta:

C:\Seguridad Informatica\v4.1 Libro Electronico

Para una más fácil localización, cada archivo tiene su nombre por tema, precedido por un número que indica el capítulo del libro.

Recuerde que por su naturaleza este libro electrónico puede actualizarse. Luego, cuando observe en la página Web de CriptoRed la existencia de un archivo **SegInfoCrip_vX.zip** más actual que el que tiene instalado en su computador, por favor descargue e instale el libro actualizado.


Si estas actualizaciones son de poca consideración (erratas, etc.), ello no conllevará el cambio de número de versión. Por tanto, le recomiendo que consulte en CriptoRed si hay una nueva actualización cada 9 meses.

Actualización de versiones

- El libro en su versión 4.1 consta de 21 capítulos, contando de esta forma con 1.106 diapositivas. Se han actualizado especialmente los capítulos de cifrado simétrico profundizando el estudio del algoritmo AES, y el de vulnerabilidades de la cifra con RSA.
- Se han corregido erratas, vuelto a revisar cada uno de los capítulos, se ha puesto la numeración en la parte superior de la pantalla y además se han incrementado los enlaces a sitios Web en cada capítulo.
- En esta versión no se incluye el documento en Word con más de 100 páginas y 70 ejemplos resueltos sobre criptografía clásica, y que corresponde al capítulo tercero del libro Aplicaciones Criptográficas previamente citado. Su lectura sólo tiene interés bajo un punto de vista histórico y de cultura general. Como ya se ha indicado en una diapositiva anterior, puede descargarlo como un archivo anexo.

Novedades en las versiones 4.0 y 4.1

Prácticas y enlaces a sitios de Internet:

- Al final de algunos capítulos y en cuyos temas además existe un software de laboratorio, se han incluido algunas prácticas. Le recomiendo que se tome un tiempo y, una vez leído el capítulo y reforzado los conceptos del mismo, intente realizar dichas prácticas. Como bien sabrá, ésta es la forma en que mejor se aprende.
- Además, se han incluido enlaces a Internet en temas específicos en las mismas diapositivas de clase, con objeto de reforzar conceptos. Puede acceder a esa página Web desde la misma presentación en Power Point pinchando en el icono  que aparecerá junto a la dirección Web.
- Si debido a la conexión a Internet que tenga en su computador no puede acceder a la web desde dicho icono, use la dirección indicada copiándola al portapapeles y pegándola luego en el navegador.

Prácticas incluidas en la versión 4.1

- Capítulo 06: Teoría de la Información 5 prácticas
- Capítulo 07: Teoría de los Números 15 prácticas
- Capítulo 08: Teoría de la Complejidad Algorítmica 9 prácticas
- Capítulo 09: Sistemas de Cifra Clásica 17 prácticas
- Capítulo 12: Cifrado Simétrico en Bloque 29 prácticas
- Capítulo 13: Cifrado Asimétrico con Mochilas 10 prácticas
- Capítulo 14: Cifrado Asimétrico Exponencial 50 prácticas
- Capítulo 15: Funciones Hash en Criptografía 13 prácticas
- Capítulo 16: Autenticación y Firma Digital 22 prácticas
- Capítulo 17: Certificados Digitales y Estándar PKCS 4 prácticas
- Capítulo 18: Aplicaciones de Correo Seguro 33 prácticas
- Capítulo 19: Protocolos y Esquemas Criptográficos 4 prácticas
- **Número de prácticas propuestas en el libro 211 prácticas**

¿Por qué sigo usando la versión 2.000?

- En este último año ha aparecido una nueva versión de Office pero nuevamente me he visto en la obligación -y necesidad- de seguir usando la versión 2.000 SR-1.
- **Primero:** estas últimas versiones aportan muy poco a la animación del libro, tal vez más orientadas a conferencias.
- **Segundo,** y lo más grave: actualizar los archivos con las versiones actuales de Power Point, significa encontrarse con la muy desagradable sorpresa de que aumenta de forma espectacular el tamaño del archivo guardado.
- En algunos casos, sólo guardar un capítulo en una nueva versión significaba pasar de 300 KB a más de 900 KB... ☹.

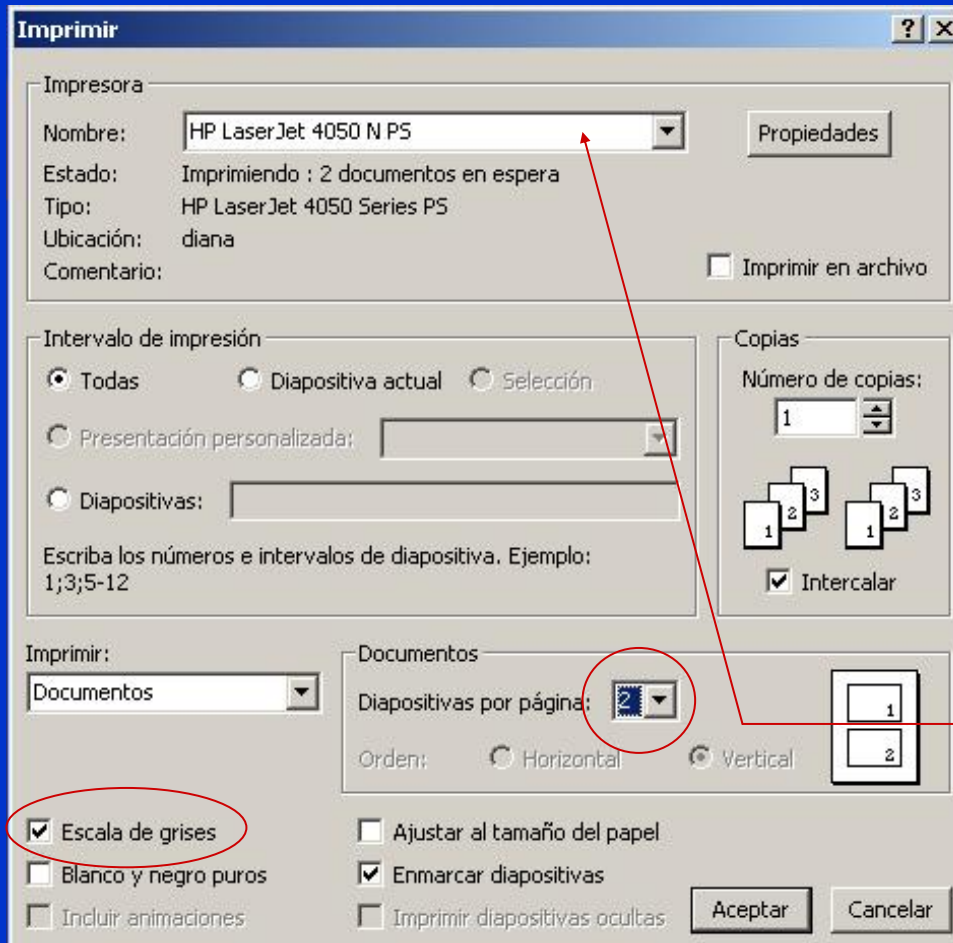
Si no lo cree, haga la prueba...

- Estos mismos apuntes podrían pasar de los 7 MBytes del archivo zip actual a cerca de 20 Mbytes ☹.
- Y subir un documento de ese tamaño en Internet todavía podría considerarse una pequeña insensatez.
- Si tiene alguna de estas nuevas versiones, abra por ejemplo el archivo del capítulo 07 del libro, cambie la numeración de las páginas y guarde el archivo con un nuevo nombre. Compare luego el tamaño los dos archivos.
- Sin entrar en discusiones, tal vez éste es un ejemplo de los despropósitos de la programación de aplicaciones y la escalabilidad y compatibilidad entre versiones, cuando esa nueva versión ofrece prácticamente lo mismo.

Formato imprimible del libro electrónico

- La edición de este libro electrónico ha sido adaptada para que, además de su animación como material de apoyo docente y de autoaprendizaje, pueda también imprimirse en papel en formato ppt o pdf como un documento de estudio y consulta.
- No obstante, es posible que si hace cuentas le sea más económico y conveniente adquirir la edición impresa por el Departamento de Publicaciones de la EUI ya comentado.
- **IMPORTANTE**: Para una lectura más cómoda, se recomienda imprimir **dos** diapositivas por página en formato documentos, en impresión con escalas de **grises** para que el fondo sea blanco. Si decide imprimir más de dos diapositivas por página posiblemente algunas letras se verán con un tamaño demasiado pequeño.

Impresión del libro en PPT o PDF



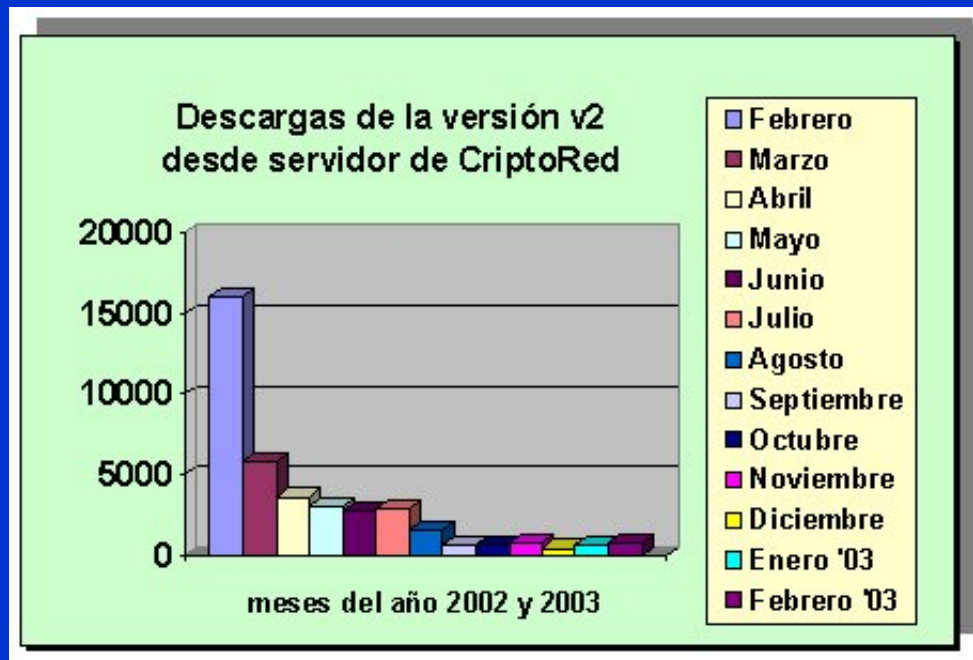
Si su impresora, como la seleccionada en la imagen, tiene entre sus propiedades imprimir por ambas caras, le recomiendo que lo active.

Así, el libro completo en diapositivas ocupará unas 270 hojas, lo que permitirá guardarlo en una carpeta con anillas o bien como un libro en gusanillos.

También puede pedir que se imprima el documento en formato PDF y editarlo con ese programa.

Descargas de la versiones 1 y 2

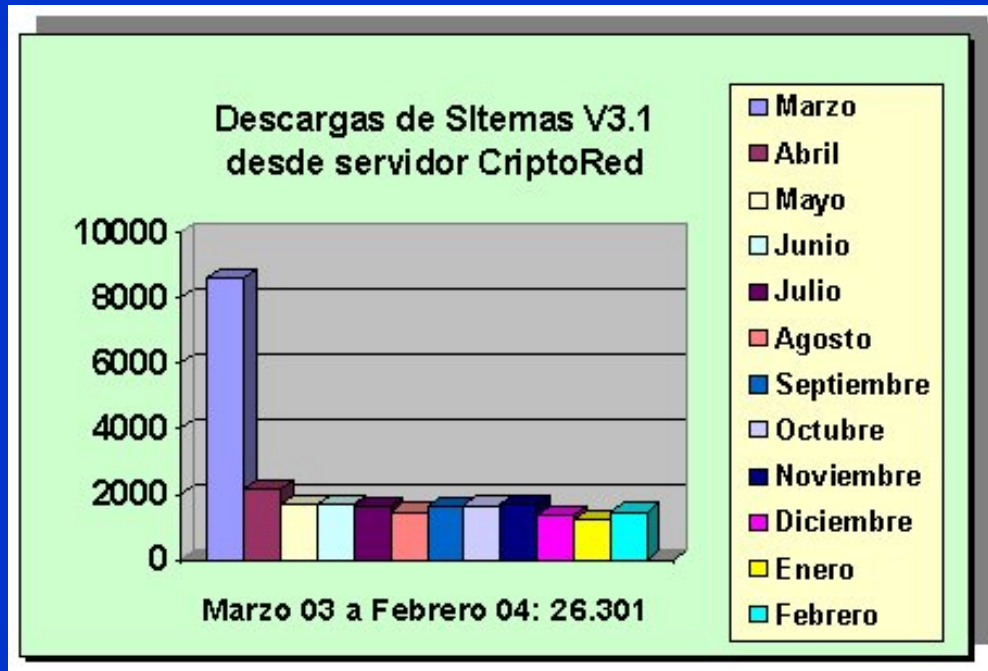
La primera versión 1 del libro electrónico (básica) alcanzó algo más de 2.000 descargas durante el año 2001 desde el mismo servidor.



Febrero 2002	16.020
Marzo 2002	5.892
Abril 2002	3.655
Mayo 2002	3.077
Junio 2002	2.717
Julio 2002	2.940
Agosto 2002	1.602
Septiembre 2002	719
Octubre 2002	674
Noviembre 2002	765
Diciembre 2002	462
Enero 2003	690
Febrero 2003	852

Número total de descargas de la versión 2 desde febrero de 2002 a febrero de 2003: 40.065. Sólo se consideran descargas desde el servidor CriptoRed.

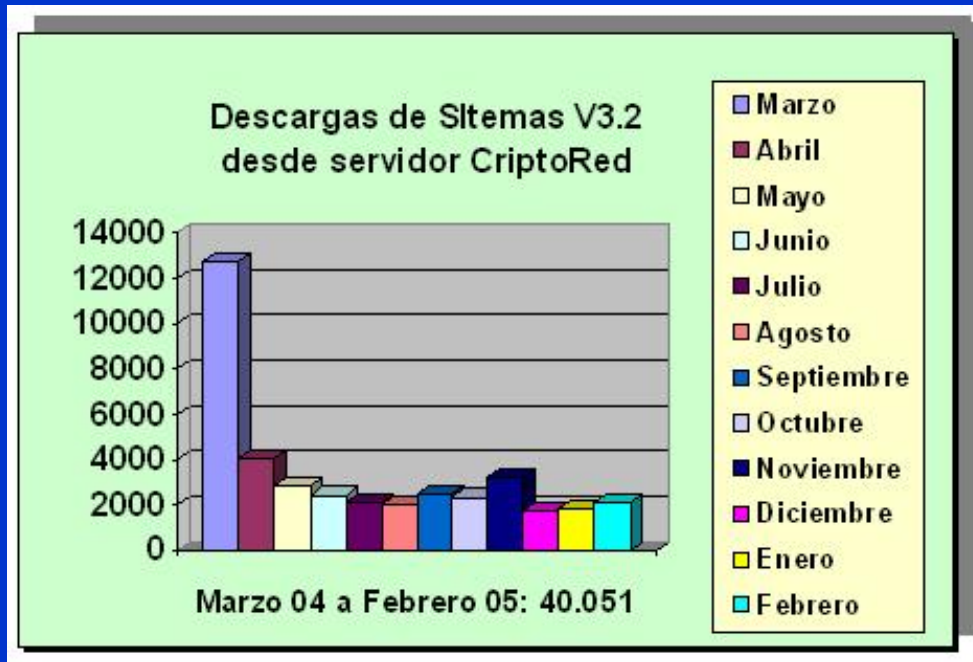
Descargas de la versión 3.1 del libro



Marzo 2003	8.614
Abril 2003	2.164
Mayo 2003	1.709
Junio 2003	1.687
Julio 2003	1.609
Agosto 2003	1.459
Septiembre 2003	1.609
Octubre 2003	1.665
Noviembre 2003	1.711
Diciembre 2003	1.385
Enero 2004	1.232
Febrero 2004	1.457

Total descargas de la versión 3.1 desde marzo de 2003 a febrero de 2004: 26.301. Sólo se consideran descargas desde el servidor CriptoRed.

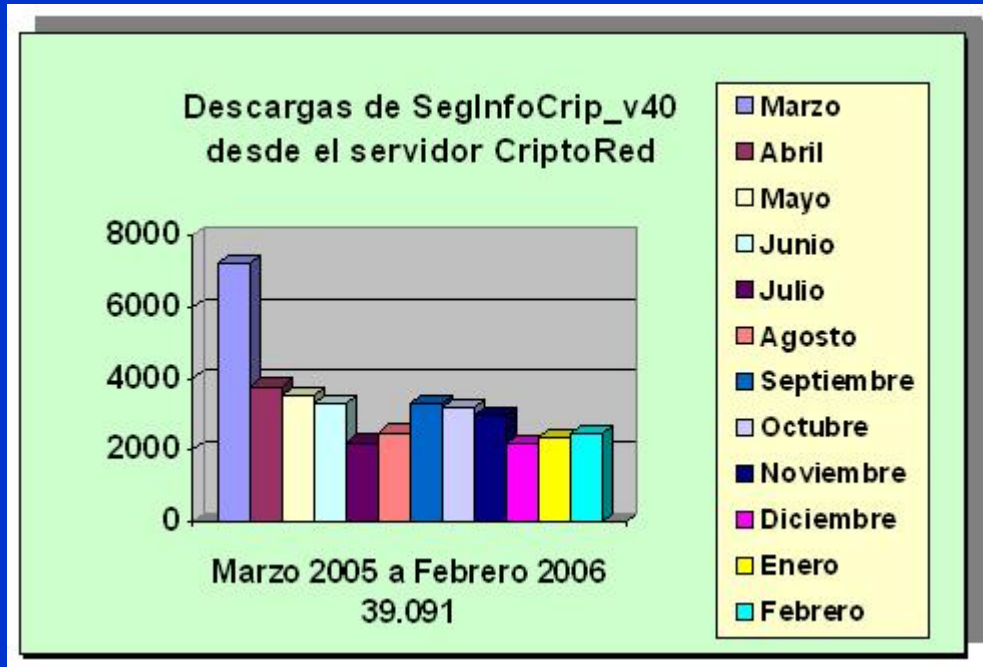
Descargas de la versión 3.2 del libro



Marzo 2004	12.720
Abril 2004	4.067
Mayo 2004	2.877
Junio 2004	2.451
Julio 2004	2.105
Agosto 2004	2.005
Septiembre 2004	2.505
Octubre 2004	2.359
Noviembre 2004	3.219
Diciembre 2004	1.777
Enero 2005	1.842
Febrero 2005	2.124

Total descargas de la versión 3.2 desde marzo de 2004 a febrero de 2005: 40.051. Sólo se consideran descargas desde el servidor CriptoRed.





Descargas de la versión 4.0 del libro



Marzo 2005	7.231
Abril 2005	3.782
Mayo 2005	3.524
Junio 2005	3.306
Julio 2005	2.212
Agosto 2005	2.499
Septiembre 2005	3.310
Octubre 2005	3.207
Noviembre 2005	2.954
Diciembre 2005	2.207
Enero 2006	2.345
Febrero 2006	2.514

Total descargas de la versión 4.0 desde marzo de 2005 a febrero de 2006: 39.091. Sólo se consideran descargas desde el servidor CriptoRed.

Sobre el autor de este libro

- Desde el curso 1994/1995 imparte la asignatura de Seguridad Informática en la titulación de Ingeniero Técnico en Informática de Gestión en la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España. Y desde el curso 2004/2005 es coordinador de la asignatura Gestión, Auditoría, Normativas y Legislación en Seguridad Informática.
 - <http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm> 
 - <http://www.lpsi.eui.upm.es/GANLESI/GANLESI.htm> 
- Es el creador y coordinador de la Red Temática Iberoamericana de Criptografía y Seguridad de la Información CriptoRed, desde diciembre de 1999, y que a 1 de marzo de 2006 cuenta con casi 600 miembros expertos en seguridad y que representan a 155 universidades y más de 190 empresas de Iberoamérica.
 - <http://www.criptored.upm.es> 
- Ha impartido conferencias y cursos sobre criptografía y seguridad informática en Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, España, México, Panamá, Perú, República Dominicana, Uruguay y Venezuela.
 - <http://www.lpsi.eui.upm.es/~jramio> 

Fin del capítulo