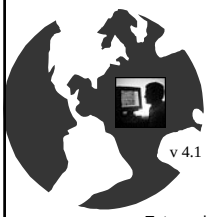
Capítulo 21: Bibliografía, Enlaces, Tablas, Software y Documentos

Seguridad Informática y Criptografía



Material Docente de Libre Distribución

Ultima actualización del archivo: 01/03/06
Este archivo tiene: 78 diapositivas

Dr. Jorge Ramió Aguirre
Universidad Politécnica de Madrid

Bibliografía recomendada en castellano (1)

Pastor, José; Sarasa, Miguel Angel

CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES

Prensas Universitarias de Zaragoza

Año 1998 (597 páginas)

Extenso y completo texto sobre técnicas criptográficas modernas, con una buena cantidad de ejemplos y profusión de tablas con datos de interés. Destacan los capítulos de cifra con clave secreta, en donde se estudian más de una docena de criptosistemas, los de clave pública y su aplicación en firmas digitales y un capítulo dedicado a protocolos criptográficos. En particular, están muy bien tratados los apéndices con temas matemáticos así como los algoritmos de factorización y del logaritmo discreto, algo no muy común y que se agradece. Para el buen seguimiento es necesario contar con una buena base matemática.

Bibliografía recomendada en castellano (2)

Fúster, Amparo; De la Guía, Dolores; Hernández, Luis; Montoya, Fausto; Muñoz, Jaime

TÉCNICAS CRIPTOGRÁFICAS DE PROTECCIÓN DE DATOS. TERCERA EDICIÓN

Editorial Ra-Ma

Año 2004 (416 páginas)

Detallado y actualizado resumen de las técnicas de cifra modernas, profundizando en los sistemas de clave secreta con cifra en flujo y en bloque, de clave pública y sus aplicaciones en redes. De especial interés resulta el capítulo dedicado a protocolos criptográficos y sus apéndices en donde explica los métodos matemáticos usados en criptografía y nociones sobre complejidad computacional. La edición incluye además una interesante colección de problemas y sus soluciones en un CD ROM.

Bibliografía recomendada en castellano (3)

Caballero, Pino

INTRODUCCIÓN A LA CRIPTOGRAFÍA. SEGUNDA EDICIÓN

Editorial Ra-Ma, Textos Universitarios, Madrid

Año 2002 (160 páginas)

Es éste un libro de introducción a las técnicas criptográficas que presenta estos temas bajo una orientación matemática clara y precisa. Corresponde a una actualización de la primera edición de 1996 en la que trata los temas de criptografía teórica, criptografía de clave secreta y pública, problemas de autenticación y accesos y algunas aplicaciones criptográficas. Para un buen seguimiento de la lectura y aprovechamiento de los temas tratados en él, en algunos apartados es recomendable contar con una cierta base de conocimientos en matemáticas a nivel universitario.

Bibliografía recomendada en castellano (4)

Carracedo Gallardo, Justo

SEGURIDAD EN REDES TELEMÁTICAS

Editorial McGraw - Hill

Año 2004 (540 páginas)

Con 11 capítulos que van desde aspectos básicos de la seguridad y los fundamentos teóricos de criptografía hasta las aplicaciones seguras en redes, sus herramientas de protección y autenticación, terminando con conceptos avanzados y muy actuales sobre servicios de anonimato para la sociedad de la información, este libro hace un amplio y claro barrido de la seguridad en las redes telemáticas. Dedicado al estudio de los problemas y las soluciones presentes en la securización de las comunicaciones, está dirigido tanto a estudiantes universitarios como a profesionales egresados de facultades y escuelas de ingeniería que requieren estar al día.

Bibliografía recomendada en castellano (5)

Alvarez Marañón, Gonzalo; Pérez García, Pedro Pablo

SEGURIDAD INFORMÁTICA PARA EMPRESAS Y PARTICULARES

Editorial McGraw - Hill

Año 2004 (440 páginas)

Entre otros temas, el libro trata de la protección del anonimato y de la privacidad en Internet, protección de la confidencialidad de la información mediante el cifrado con EFS y SSL, protección de la disponibilidad de la información mediante sistemas tolerantes a fallos, estrategias de recuperación de sistemas y copias de seguridad, planes de contingencia, utilización de las firmas electrónicas y los certificados digitales, elección adecuada de cortafuegos, creación de una red privada virtual, protecciones ante el malware, sistemas de detección y prevención de intrusiones, etc.

Bibliografía recomendada en castellano (6)

Stallings, William

FUNDAMENTOS DE SEGURIDAD EN REDES. APLICACIONES Y ESTÁNDARES

Prentice-Hall Inc.

Año 2003 (456 páginas)

Corresponde a la traducción del inglés al español del libro que se comenta más adelante. Manteniendo la misma filosofía que su edición en inglés, en este caso contiene 225 páginas menos. Presenta temas de cifra simétrica y asimétrica, algoritmos, firmas, hash, autenticación y seguridad en redes. Está más centrada en la seguridad en Internet, profundizando en temas como correo seguro, protocolos de redes, IP seguro, seguridad en Web, intrusiones, cortafuegos, etc. Un excelente libro para el estudiante, si bien para el profesor es recomendable el original en inglés.

Bibliografía recomendada en castellano (7)

Singh, Simon (traducción de José Ignacio Moraza)

LOS CÓDIGOS SECRETOS

Editorial Debate S.A.

Año 2000 (382 páginas)

Interesante libro de Simon Singh editado en 1999, en el que se hace un repaso extenso de la criptografía denominada clásica, máquinas y artilugios de cifra, máquina Enigma, etc., desde una perspectiva un tanto novelesca que, sin desmerecer en absoluto la calidad técnica del mismo, lo convierte en un excelente libro de amena lectura. Encontrará en él una presentación de los sistemas de cifra asimétrica, la historia inmersa en la búsqueda de la criptografía de clave pública y el intercambio de clave, para terminar con PGP y un capítulo dedicado a la criptografía cuántica.

Bibliografía recomendada en castellano (8)

Morant Ramón, J.L.; Ribagorda Garnacho, A.; Sancho Rodríguez J.

SEGURIDAD Y PROTECCIÓN DE LA INFORMACIÓN

Colección de Informática, Editorial Centro de Estudios Ramón Areces, S.A., Madrid

Año 1994 (388 páginas)

Libro que trata, además de los temas genéricos de la criptografía clásica y moderna, aspectos de seguridad en sistemas operativos, en bases de datos y en redes de computadores. Buen texto descriptivo que profundiza en ciertos aspectos matemáticos y hace un buen estudio de la gestión de claves. Tiene además como característica ser el primer libro con formato universitario sobre criptografía y seguridad informática en España, y seguramente de lengua española. No existen nuevas versiones que serían no obstante muy bien recibidas.

Bibliografía recomendada en inglés (1)

Menezes, Alfred; Oorsschof, Paul; Vanstone, Scott

HANDBOOK OF APPLIED CRYPTOGRAPHY

CRC Press Inc. http://www.cacr.math.uwaterloo.ca/hac/ 

Año 1997 (780 páginas)

Interesante y completo libro dedicado al estudio de los algoritmos con una visión matemática de alto nivel. Sus capítulos están orientados a bases matemáticas para la criptografía, sistemas de claves secretas y públicas, cifradores de flujo y de bloque, hash, autenticación, firma digital y gestión de claves. Obra imprescindible para el estudiante universitario que desea profundizar en el análisis de los algoritmos, si bien el seguimiento del mismo puede resultar algo complejo por el nivel matemático comentado. Junto al de William Stallings, es probablemente el mejor libro de criptografía en la actualidad. Le recomiendo que descargue el libro gratis desde la página web de su autor que verá más arriba.

Bibliografía recomendada en inglés (2)

Stallings, William

CRYPTOGRAPHY AND NETWORK SECURITY. PRINCIPLES AND PRACTICE. THIRD EDITION

Prentice-Hall Inc.

Año 2003 (681 páginas)

Con una centena más de páginas que la segunda edición de (1999), el texto está estructurado de una forma óptima que permite una agradable lectura. Además de cifra simétrica y asimétrica, algoritmos, firmas, hash, autenticación y seguridad en redes, esta edición se centra en la seguridad en Internet, profundizando en temas como correo seguro, protocolos de redes, IP seguro, seguridad en Web, intrusiones, cortafuegos, etc. Incluye algunos ejemplos y ejercicios. Junto al de Alfred Menezes, probablemente es el mejor libro de criptografía y seguridad informática en la actualidad.

Bibliografía recomendada en inglés (3)

Schneier, Bruce

APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C. SECOND EDITION

John Wiley & Sons, Inc., New York

Año 1996 (758 páginas)

Segunda edición del libro con mismo título, con mayor énfasis en los algoritmos de cifra, protocolos, firmas, etc., especialmente en los sistemas con clave privada y pública. El texto de Schneier resulta fundamental para los estudiantes universitarios de asignaturas de criptografía. Incluye una bibliografía es muy completa, hay profusión de tablas y estudia una infinidad de criptosistemas, adjuntando el código fuente en C de muchos de los algoritmos estudiados. Se echa en falta, no obstante, que no tenga algunos ejemplos resueltos en cada capítulo.

Bibliografía recomendada en inglés (4)

Douglas R. Stinson

CRYPTOGRAPHY. THEORY AND PRACTICE. THIRD EDITION

Champan & Hall / CRC

Año 2006 (593 páginas)

Desde su primera edición en el año 1995, el libro de Douglas Stinson se ha actualizado en su totalidad. Manteniendo aquellos capítulos dedicados a la criptografía clásica, el cifrado con clave secreta -en este caso profundizando en el algoritmo AES-, funciones hash, cifras RSA y ElGamal, autenticación y firma digital, en esta edición se agradece la inclusión y actualización en apartados como la generación de bits pseudoaleatorios, primitivas de autenticación con transferencia de conocimiento nulo, distribución de claves, infraestructuras de clave pública y esquemas de compartición de secretos.

Bibliografía recomendada en inglés (5)

Salomaa, Arto

PUBLIC-KEY CRYPTOGRAPHY. SECOND EDITION

EATCS Monographics on Theoretical Computer Science

W. Brauer, G. Rozenberg, A. Salomaa (Eds.), Springer-Verlag, New York

Año 1996 (268 páginas)

Interesante y ameno, profundiza en los criptosistemas de clave pública y protocolos criptográficos en esta segunda edición. En algunos capítulos es necesario contar con una base matemática de nivel universitario para una mejor comprensión. No obstante, su lectura es muy agradable y presenta algunos ejemplos resueltos. Incluye un amplio estudio de los sistemas de mochilas, su implementación, debilidades, tipos de ataques, etc.

Bibliografía recomendada en inglés (6)

Seberry, Jennifer; Pieprzyk, Josef

CRYPTOGRAPHY. AN INTRODUCTION TO COMPUTER SECURITY

Prentice-Hall, New York

Año 1989 (375 páginas)

Además de los temas propios de criptografía clásica y moderna, incluye un capítulo de introducción a la aritmética modular bien estructurado. Trata también la seguridad informática en bases de datos, en sistemas operativos y en redes. Como lector se agradece en especial la gran cantidad de ejercicios propuestos y resueltos en cada capítulo, incluyendo el código en PASCAL.

Bibliografía recomendada en inglés (7)

Pflegger P., Charles

SECURITY IN COMPUTING

Prentice-Hall International Editions, London

Año 1989 (538 páginas)

Texto de consulta general sobre seguridad informática que trata los criptosistemas y además estudia la seguridad en los programas, en informática personal, en las comunicaciones, análisis de riesgos, así como los aspectos legales y éticos de esta especialidad. Incluye varios ejercicios propuestos sin incluir sus soluciones. Debido a la fecha de edición, no profundiza en aspectos de cifra asimétrica y algoritmos actuales.

Bibliografía recomendada en inglés (8)

Kahn, David

THE CODE-BREAKERS

Scribner New York

Año 1996 (1.181 páginas)

Un libro clásico en criptografía y el más completo sobre el apasionante mundo de la criptología en sus primeros años de existencia y en la primera y segunda guerra mundiales. Con una bibliografía de casi mil documentos, este libro es un referente básico de todo el ambiente de espionaje militar tan propio de aquella época y un verdadero documento histórico. Puesto que su primera edición data de 1967, prácticamente no trata la criptografía asimétrica o de clave pública. No obstante, su valor principal es ser un referente único sobre la historia de la criptografía.

Bibliografía de interés en seguridad

- En la última década la bibliografía sobre criptografía y otros temas relacionados con la seguridad informática, en el sentido amplio que se ha comentado en estos apuntes, ha aumentado de una forma espectacular.
- Cada mes aparecen en el mercado una media de tres a cuatro nuevos libros sobre esta temática.
- Cada vez hay más publicaciones originales en español de gran interés, así como traducciones al español de textos en inglés.
- Como es muy difícil estar al día en este tema, y más aún desde unos apuntes en formato electrónico, si desea puede acceder a la página de mi asignatura en donde espero tener un enlace con esta información, aproximadamente a mediados de este año 2006.

http://www.lpsi.eui.upm.es/SInformatica/SInformatica.htm

Enlaces a páginas Web en capítulos (1)

Capítulo 3. Introducción a la Seguridad Informática

- REAL ACADEMIA ESPAÑOLA http://www.rae.es/
- VIRUSPROT http://www.virusprot.com/Opiniones2002.html
- SIR FRANCIS BACON http://www.sirbacon.org/links.html
- KERCKHOFFS http://en.wikipedia.org/wiki/Kerckhoffs%27_law

Capítulo 4. Calidad de Información y Programas Malignos

- CLAUDE SHANNON http://es.wikipedia.org/wiki/Claude_Shannon
- RED IRIS http://www.rediris.es/cert/doc/docu_rediris/poliseg.es.html
- BACKUP http://www.criptored.upm.es/guiateoria/gt_m001l.htm
- HACKERS http://www.umanizales.edu.co/encuentrohackers/tiposh.htm

Enlaces a páginas Web en capítulos (2)

Capítulo 4. Calidad de Información y Programas Malignos (continuación)

- DELITOS INFORMÁTICOS http://www.delitosinformaticos.com/delitos/
- PHISING http://en.wikipedia.org/wiki/Phising
- ANIMACION FLASH DE PHISING http://www.hispasec.com/unaaldia/2406
- ALERTA ANTIVIRUS http://alerta-antivirus.red.es/virus/ver_pag.html?tema=V
- MALWARE WFM http://www.hispasec.com/unaaldia/2639
- VIRUS TOTAL http://www.virustotal.com/

Capítulo 5. Introducción a la Gestión de la Seguridad

- MAGERIT http://www.csi.map.es/csi/pg5m20.htm
- ANALISIS RIESGO CHINCHON http://www.criptored.upm.es/software/sw_m214_01.htm

Enlaces a páginas Web en capítulos (3)

Capítulo 5. Introducción a la Gestión de la Seguridad (continuación)

BELL LAPADULA http://en.wikipedia.org/wiki/Bell-LaPadula_model

CLARK WILSON http://www.criptored.upm.es/guiateoria/gt_m248c.htm

TAKE GRANT http://www.criptored.upm.es/guiateoria/gt_m248b.htm

BIBA http://www.criptored.upm.es/guiateoria/gt_m248a.htm

HARRISON, RUZZO, ULLMAN http://www.criptored.upm.es/guiateoria/gt_m248e.htm

CHINESE WALL http://www.criptored.upm.es/guiateoria/gt_m248d.htm

SEA VIEW http://www.criptored.upm.es/guiateoria/gt_m248f.htm

CRITERIOS SEGURIDAD MAP http://www.csi.map.es/csi/criterios/seguridad/index.html

LEYES PROTECCIÓN DATOS EN ESPAÑA http://www.agpd.es/index.php?idSeccion=77

Enlaces a páginas Web en capítulos (4)

Capítulo 5. Introducción a la Gestión de la Seguridad (continuación)

REAL DECRETO 994/1999 REGLAMENTO MEDIDAS DE SEGURIDAD FICHEROS AUTOMATIZADOS https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/A.8%29%20Real%20Decreto%20994-1999.pdf

LOPD https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf

17799 http://www.aenor.es/desarrollo/normalizacion/normas/resultadobuscnormas.asp?campobuscador=17799

ANÁLISIS ISO 17799 http://www.criptored.upm.es/guiateoria/gt_m209b.htm

DISASTER RECOVERY http://recovery-disaster.info/index.htm

Capítulo 6. Teoría de la Información

CLAUDE SHANNON http://es.wikipedia.org/wiki/Claude_E._Shannon

ARTÍCULO SHANNON http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html

Enlaces a páginas Web en capítulos (5)

Capítulo 6. Teoría de la Información (continuación)

ENTROPÍA DE LA INFORMACIÓN http://en.wikipedia.org/wiki/Information_entropy

COMPRESIÓN DATOS HUFFMAN http://articulos.conclase.net/compresion/huffman.html

COMPRESIÓN DE DATOS http://es.wikipedia.org/wiki/Compresi%C3%B3n_de_datos

DIST. UNIDAD http://www.cs.ucla.edu/~jkong/research/security/shannon1949/node14.html

Capítulo 7. Teoría de los Números

ALGORITMO DE EUCLIDES http://es.geocities.com/eucliteam/

INVERSOS MULTIPLICATIVOS http://www.cut-the-knot.org/blue/Modulo.shtml

EULER http://es.wikipedia.org/wiki/Euler

INDICADOR DE EULER http://mathworld.wolfram.com/TotientFunction.html

Enlaces a páginas Web en capítulos (6)

Capítulo 7. Teoría de los Números (continuación)

TEOREMA FERMAT http://es.wikipedia.org/wiki/Peque%C3%B1o_teorema_de_Fermat

ALGORITMO EXTENDIDO DE EUCLIDES http://en.wikipedia.org/wiki/Euclid

TEOREMA DEL RESTO CHINO http://www.math.hawaii.edu/~lee/courses/Chinese.pdf

PÁGINA DE NÚMEROS PRIMOS http://www.utm.edu/research/primes/

RAÍCES PRIMITIVAS http://mathworld.wolfram.com/PrimitiveRoot.html

GALOIS http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Galois.html

CAMPOS FINITOS http://mathworld.wolfram.com/FiniteField.html

Capítulo 8. Teoría de la Complejidad Algorítmica

O(n) http://www.mm.informatik.tu-darmstadt.de/courses/2002ws/ics/lectures/v14.pdf

Enlaces a páginas Web en capítulos (7)

Capítulo 8. Teoría de la Complejidad Algorítmica (continuación)

- PROBLEMA DE LA MOCHILA http://en.wikipedia.org/wiki/Knapsack_problem
- PROBLEMA DE LA FACTORIZACIÓN http://home.netcom.com/~jrhowell/math/factor.htm
- PROBLEMA LOGARITMO DISCRETO http://en.wikipedia.org/wiki/Discrete_logarithm
- PROBLEMAS NP http://www.csc.liv.ac.uk/~ped/teachadmin/COMP202/annotated_np.html

Capítulo 9. Sistemas de Cifra Clásicos

- PÁGINA DE LA NSA http://www.nsa.gov/public/publi00007.cfm
- ALGORITMOS DE CIFRA http://library.thinkquest.org/27158/concept1_1.html
- ART. DIFFIE-HELLMAN http://www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf
- VERNAM http://www.pro-technix.com/information/crypto/pages/vernam_base.html

Enlaces a páginas Web en capítulos (8)

Capítulo 10. Introducción a la Cifra Moderna

- SISTEMAS DE CIFRA http://en.wikipedia.org/wiki/Category:Cryptography

Capítulo 11. Sistemas de Cifra en Flujo

- PÁGINA DE SOLOMON GOLOMB http://ee.usc.edu/faculty_staff/bios/golomb.html
- AUTÓMATAS CELULARES http://www.criptored.upm.es/investigacion/tfc_m317a.htm
- SECUENCIA DE BRUIJN http://mathworld.wolfram.com/deBruijnSequence.html
- POLINOMIOS http://mathworld.wolfram.com/PrimitivePolynomial.html
- GENERACIÓN DE POLINOMIOS http://www.theory.csc.uvic.ca/~cos/gen/poly.html
- ATAQUE B-M http://planetmath.org/encyclopedia/BerlekampMasseyAlgorithm.html
- ALGORITMO B-M http://ihome.ust.hk/~trippen/Cryptography/BM/frameset.html

Enlaces a páginas Web en capítulos (9)

Capítulo 11. Sistemas de Cifra en Flujo (continuación)

- ATAQUES A CIFRADORES EN FLUJO http://www.cryptosystem.net/stream
- ANÁLISIS A5/1 http://www.argo.es/~jcea/artic/hispasec33.htm
- RC4 http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html
- SEAL http://www.gemplus.com/smart/rd/publications/pdf/HG97chis.pdf
- ARTÍCULO ORIGINAL DEL ATAQUE A5/1 http://cryptome.org/a51-bsw.htm
- ANÁLISIS DEL ATAQUE A5/1 http://www.criptored.upm.es/guiateoria/gt_m116a.htm

Capítulo 12. Cifrado Simétrico en Bloque

- FEISTEL http://en.wikipedia.org/wiki/Feistel_network
- COMPENDIO DE CIFRADORES http://www.quadibloc.com/crypto/intro.htm

Enlaces a páginas Web en capítulos (10)

Capítulo 12. Cifrado Simétrico en Bloque (continuación)

- ATAQUES A CIFRADORES EN FLUJO http://www.cryptosystem.net/stream
- MODOS DE CIFRA EN DES http://www.itl.nist.gov/fipspubs/fip81.htm
- ESPECIFICACIONES DEL DES http://www.itl.nist.gov/fipspubs/fip46-2.htm
- TRIPLE DES http://www.rsasecurity.com/rsalabs/node.asp?id=2231
- IDEA http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm
- CLAVES DÉBILES IDEA http://www.cosic.esat.kuleuven.ac.be/publications/article-140.pdf
- PÁGINA DEL NIST http://www.nist.gov/
- DES CHALLENGE III http://www.rsasecurity.com/rsalabs/node.asp?id=2108
- ANUNCIO DEL AES http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Enlaces a páginas Web en capítulos (11)

Capítulo 12. Cifrado Simétrico en Bloque (continuación)

- PÁGINA OFICIAL DEL AES http://www.iaik.tu-graz.ac.at/research/krypto/AES/
- DOCUMENTO ESTUDIO DEL AES http://www.criptored.upm.es/guiateoria/gt_m480a.htm
- PÁGINA RIJMEN http://www.iaik.tu-graz.ac.at/research/krypto/AES/old/%7Erijmen/rijndael/
- GRÁFICOS DEL AES http://www.quadibloc.com/crypto/co040401.htm
- ANÁLISIS AES Y BABY AES http://www.criptored.upm.es/guiateoria/gt_m117i.htm

Capítulo 13. Cifrado Asimétrico con Mochilas

- M-H http://www-fs.informatik.uni-tuebingen.de/~reinhard/krypto/English/4.5.3.e.html
- MOCHILA M-H http://www.behdad.org/download/Presentations/knapsack/knapsack.ppt
- ATAQUE A M-H http://www.behdad.org/download/Presentations/knapsack/knapsack.ppt

Enlaces a páginas Web en capítulos (12)

Capítulo 14. Cifrado Asimétrico Exponencial

- D-H http://www.cs.purdue.edu/homes/ninghui/courses/Fall04/lectures/diffie-hellman.pdf
- LOGARITMO DISCRETO http://en.wikipedia.org/wiki/Discrete_logarithm
- RSA http://www.di-mgt.com.au/rsa_alg.html
- MÉTODOS DE FACTORIZACIÓN http://home.netcom.com/~jrhowell/math/factor.htm
- DESAFÍO RSA 640 http://www.rsasecurity.com/rsalabs/node.asp?id=2964
- EL SISTEMA RSA http://www.criptored.upm.es/guiateoria/gt_m117f.htm
- OPEN SSL http://www.openssl.org
- ATAQUES A RSA http://crypto.stanford.edu/~dabo/papers/RSA-survey.pdf
- HISTORIA DE RSA http://livinginternet.com/i/is_crypt_pkc_inv.htm

Enlaces a páginas Web en capítulos (13)

Capítulo 14. Cifrado Asimétrico Exponencial (continuación)

- POHLIG-HELLMAN http://ieeexplore.ieee.org/xpl/abs_free.jsp?arNumber=1055817
- ELGAMAL http://web.usna.navy.mil/~wdj/book/node48.html
- LOGARITMO DISCRETO http://en.wikipedia.org/wiki/Discrete_logarithm

Capítulo 15. Funciones Hash en Criptografía

- MD5 http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html
- RFC MD5 http://www.faqs.org/rfcs/rfc1321.html
- RFC SHA-1 http://www.faqs.org/rfcs/rfc3174.html
- LITTLE ENDIAN – BIG ENDIAN http://www.algoritmia.net/articles.php?id=57
- SURVEY ATAQUES A HASH http://www.criptored.upm.es/guiateoria/gt_m238a.htm

Enlaces a páginas Web en capítulos (14)

Capítulo 15. Funciones Hash en Criptografía (continuación)

- ATAQUES HASH http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html

Capítulo 16. Autenticación y Firma Digital

- RFC MESSAGE AUTHENTICACION CODE http://www.faqs.org/rfcs/rfc3537.html
- FIPS HMAC http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf
- MODELO NEEDHAM-SCHROEDER http://www.lsv.ens-cachan.fr/spore/nssk.html
- SISTEMA KERBEROS http://www.isi.edu/gost/publications/kerberos-neuman-tso.html
- PÁGINA OFICIAL DE KERBEROS http://web.mit.edu/kerberos/www/
- AUTENTICACIÓN http://www.mug.org.ar/Infraestructura/ArticInfraestructura/300.aspx
- PÁGINA L. LAMPORT http://research.microsoft.com/users/lamport/

Enlaces a páginas Web en capítulos (15)

Capítulo 16. Autenticación y Firma Digital (continuación)

- PÁGINA M. RABIN http://www.deas.harvard.edu/ourfaculty/profile/Michael_Rabin
- PÁGINA Y. DESMEDT http://www.cs.fsu.edu/~desmedt/
- RSA http://www.enstimac.fr/Perl/perl5.6.1/site_perl/5.6.1/Crypt/RSA.html
- FIRMA ELGAMAL http://www.math.clemson.edu/faculty/Gao/crypto_mod/node5.html
- ESTÁNDARES DE FIRMA DEL NIST http://www.itl.nist.gov/fipspubs/fip186.htm
- SEGURIDAD DSS http://lists.gnupg.org/pipermail/gnupg-users/2000-August/006286.html

Capítulo 17. Certificados Digitales y Estándar PKCS

- PKI X.509 DE LA IEFT http://www.ietf.org/html.charters/pkix-charter.html
- CERTIFICADO VERISIGN https://digitalid.verisign.com/client/enroll.htm

Enlaces a páginas Web en capítulos (16)

Capítulo 17. Certificados Digitales y Estándar PKCS (continuación)

- PKCS LABORATORIOS RSA http://www.rsasecurity.com/rsalabs/pkcs/

Capítulo 18. Aplicaciones de Correo Seguro

- RFC PRIVATE ENHANCED MAIL PEM http://www.ietf.org/rfc/rfc1421.txt
- PHILIP ZIMMERMANN http://www.philzimmermann.com/ES/background/index.html
- GNUPG GNU PRIVACY GUARD http://www.gnupg.org/
- PGP S/MIME http://www.imc.org/smime-pgpmime.html

Capítulo 19. Protocolos y Esquemas Criptográficos

- PROTOCOLOS CRIPTOGRÁFICOS http://www.criptored.upm.es/guiateoria/gt_m023c.htm
- FIRMA CIEGA http://www.di.ens.fr/~pointche/Documents/Papers/2003_joc.pdf

Enlaces a páginas Web en capítulos (17)

Capítulo 19. Protocolos y Esquemas Criptográficos (continuación)

ENTEROS DE BLUM http://zoo.cs.yale.edu/classes/cs467/2005f/course/lectures/ln20.pdf

VOTO TELEMÁTICO http://vototelematico.diatel.upm.es/

Capítulo 20. Introducción a la Cifra con Curvas Elípticas

CRIPTOGRAFÍA CON CURVAS ELÍPTICAS (Búsqueda Google - español)
http://www.google.es/search?hl=es&q=criptografia+curvas+el%C3%ADpticas&meta=

CRIPTOGRAFÍA CON CURVAS ELÍPTICAS (Búsqueda Google - inglés)
http://www.google.es/search?hl=es&q=elliptic+curve+cryptography&meta=

ECC CHALLENGE http://www.certicom.com/index.php?action=res,ecc_solution

LIBRERÍA PARA CURVAS ELÍPTICAS http://shoup.net/ntl/

Enlaces de interés en Internet (1)

Los enlaces que puede encontrar en Internet sobre temas de seguridad informática son muchos. Es posible que algunos por el paso del tiempo o por una política de gestión del servidor no apropiada, no estén activos. En estas tres diapositivas pondremos sólo unos cuantos enlaces que se recomiendan al lector, en los que encontrará información interesante, documentación, estándares, software, etc. Use el portapapeles.

- CriptoRed
  http://www.criptored.upm.es/
- Hispasec
  http://www.hispasec.com/
- RedIRIS
  http://www.rediris.es/
- VirusProt
  http://www.virusprot.com/
- Kriptópolis
  http://www.kriptopolis.com/
- Criptonomicón
  http://www.iec.csic.es/criptonomicon/
- Revista Red Seguridad
  http://www.borrmart.es/redseguridad.php
- Revista SIC
  http://www.revistasic.com/
- Organización ISACA
  http://www.isaca.org/
- Computer Security Resource Center del NIST
  http://csrc.nist.gov/
- CERT de Carnegie Mellon
  http://www.cert.org/
- National Security Agency
  http://www.nsa.gov/

Enlaces de interés en Internet (2)

- Página Web de Alfred Menezes
  http://www.cacr.math.uwaterloo.ca/~ajmeneze/
- Página Web de Bruce Schneier
  http://www.counterpane.com/schneier.html
- Página Web del libro de William Stallings
  http://williamstallings.com/Crypto3e.html
- Página Web de Solomon Golomb
  http://csi.usc.edu/faculty/golomb.html
- Página Web de Vincent Rijmen: Rijndael
  http://www.esat.kuleuven.ac.be/~rijmen/rijndael/
- Página Web de Philip Zimmermann
  http://www.philzimmermann.com/
- Crypto++ Library
  http://www.eskimo.com/~weidai/cryptlib.html
- Conceptos sobre voto electrónico
  http://oasis.dit.upm.es/~jantonio/documentos/voto-electronico/article.html
- Esteganografía
  http://www.stegoarchive.com/
- Software libre de esteganografía
  http://members.tripod.com/steganography/stego/software.html
- Página de criptografía visual de Doug Stinson
  http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html
- Quantum Cryptography Tutorial
  http://www.cs.dartmouth.edu/~jford/crypto.html
- PGP internacional
  http://www.pgpi.org/
- Computer Security Information
  http://www.alw.nih.gov/Security/security.html
- Cryptographic Compendium de John Savard
  http://home.ecn.ab.ca/~jsavard/crypto/entry.htm
- PKCS standards: RSA Security Corporation
  http://www.rsasecurity.com/rsalabs/pkcs/
- The Prime Pages
  http://www.utm.edu/research/primes/
- Polinomios primitivos
  http://mathworld.wolfran.com/primitivepolynomial.html
- SW para generación de polinomios primitivos
  http://www.theory.csc.uvic.ca/~cos/gen/poly.html
- Cryptome: documentos sobre criptografía
  http://cryptome.org/

Enlaces de interés en Internet (3)

- Delitos Informáticos y Leyes
  http://www.delitosinformaticos.com/
- Electronic Frontier Foundation EFF
  http://www.eff.org/
- Leyes, LOPD, 17799, etc. CSI – MAP - España
  http://www.map.es/csi/fr600001.htm#5
- SSH – Cryptography A-Z
  http://www.ssh.com/support/cryptography/
- Linux Security
  http://www.linuxsecurity.com/
- Ley Orgánica de Protección de Datos LOPD
  http://www.igsap.map.es/cia/dispo/lo15-99.htm
- The Internet Engineering Task Force
  http://www.ietf.org/
- FIPS Federal Inf. Process. Standards Publications
  http://www.itl.nist.gov/fipspubs/
- RFC Editor Homepage
  http://www.rfc-editor.org/
- Open SSL
  http://www.openssl.org/
- ANSI American National Standards Institute
  http://www.ansi.org/
- ETSI. Política y normas de seguridad Europa
  http://www.etsi.org/technicalfocus/home.htm
- Cryptography and Inform. Security Group MIT
  http://theory.lcs.mit.edu/~cis/
- Computer Forensics Laboratory
  http://www.dcfl.gov/index.shtml
- VeriSign
  http://www.verisign.com/
- The Hacker Quarterly
  http://www.2600.com/
- Web spoofing. Universidad de Princeton
  http://www.cs.princeton.edu/sip/pub/spoofing.html
- Apache Software Foundation
  http://www.apache.org/
- GNU Software de seguridad
  http://www.gnu.org/directory/security/
- Netscape Security
  http://wp.netscape.com/security/
- Windows Security
  http://www.microsoft.com/security/

Tabla de frecuencia de monogramas

A	7,49	A	10,60	A	9,83	Ñ	-,--	Ñ	0,10	Ñ	0,07
B	1,29	B	1,16	B	0,86	O	7,37	O	8,23	O	7,75
C	3,54	C	4,85	C	4,15	P	2,43	P	2,71	P	2,41
D	3,62	D	5,87	D	4,04	Q	0,26	Q	0,74	Q	0,73
E	14,00	E	13,11	E	11,41	R	6,14	R	6,95	R	5,26
F	2,18	F	1,13	F	0,81	S	6,95	S	8,47	S	7,13
G	1,74	G	1,40	G	0,85	T	9,85	T	5,40	T	3,62
H	4,22	H	0,60	H	0,57	U	3,00	U	4,34	U	3,24
I	6,65	I	7,16	I	6,04	V	1,16	V	0,82	V	0,69
J	0,27	J	0,25	J	0,17	W	1,69	W	0,12	W	0,00
K	0,47	K	0,11	K	0,00	X	0,28	X	0,15	X	0,18
L	3,57	L	4,42	L	4,34	Y	1,64	Y	0,79	Y	0,63
M	3,39	M	3,11	M	2,42	Z	0,04	Z	0,26	Z	0,29
N	6,74	N	7,14	N	6,03				Blanco		6,33

Valores de frecuencia en tanto por ciento en archivos de 50.000 caracteres.
Columnas: 1º Inglés (mod 26); 2ª Castellano (mod 27); 3ª Castellano (mod 28)

Monogramas más frecuentes mod 27

E	13,11	C	4,85	Y	0,79
A	10,60	L	4,42	Q	0,74
S	8,47	U	4,34	H	0,60
O	8,23	M	3,11	Z	0,26
I	7,16	P	2,71	J	0,25
N	7,14	G	1,40	X	0,15
R	6,95	B	1,16	W	0,12
D	5.87	F	1,13	K	0,11
T	5,40	V	0,82	Ñ	0,10
Frecuencia alta		Frecuencia media		Frecuencia baja	

Con los 9 caracteres más frecuentes podemos formar la palabra ESTIRANDO

Alfabeto castellano y sus inversos mod 27

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Alfabeto y tabla módulo 27

a	inv (a,27)	a	inv (a,27)	a	inv (a,27)
1	1	2	14	4	7
5	11	7	4	8	17
10	19	11	5	13	25
14	2	16	22	17	8
19	10	20	23	22	16
23	20	25	13	26	26

Alfabeto castellano y sus inversos mod 37

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Alfabeto y tabla módulo 37

0	1	2	3	4	5	6	7	8	9
27	28	29	30	31	32	33	34	35	36

a	inv (a,37)	a	inv (a,37)	a	inv (a,37)	a	inv (a,37)	a	inv (a,37)	a	inv (a,37)
1	1	2	19	3	25	4	28	5	15	6	31
7	16	8	14	9	33	10	26	11	27	12	34
13	20	14	8	15	5	16	7	17	24	18	35
19	2	20	13	21	30	22	32	23	29	24	17
25	3	26	10	27	11	28	4	29	23	30	21
31	6	32	22	33	9	34	12	35	18	36	36

Tabla de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
Ñ	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y

Código Baudot (cifrador de Vernam)

Código Binario	Carácter	Código Binario	Carácter
00000	Blanco	10000	T
00001	E	10001	Z
00010	=	10010	L
00011	A	10011	W
00100	Espacio	10100	H
00101	S	10101	Y
00110	I	10110	P
00111	U	10111	Q
01000	<	11000	O
01001	D	11001	B
01010	R	11010	G
01011	J	11011	↑
01100	N	11100	M
01101	F	11101	X
01110	C	11110	V
01111	K	11111	↓

Código ASCII/ANSI de nivel bajo (1)

Byte	carácter
0010 0000	Espacio
0010 0001	!
0010 0010	“
0010 0011	#
0010 0100	$
0010 0101	%
0010 0110	&
0010 0111	‘
0010 1000	(
0010 1001	)
0010 1010	*
0010 1011	+
0010 1100	,
0010 1101	-
0010 1110	.
0010 1111	/

Byte	carácter
0011 0000	0
0011 0001	1
0011 0010	2
0011 0011	3
0011 0100	4
0011 0101	5
0011 0110	6
0011 0111	7
0011 1000	8
0011 1001	9
0011 1010	:
0011 1011	;
0011 1100	<
0011 1101	=
0011 1110	>
0011 1111	?

Byte	carácter
0100 0000	@
0100 0001	A
0100 0010	B
0100 0011	C
0100 0100	D
0100 0101	E
0100 0110	F
0100 0111	G
0100 1000	H
0100 1001	I
0100 1010	J
0100 1011	K
0100 1100	L
0100 1101	M
0100 1110	N
0100 1111	O

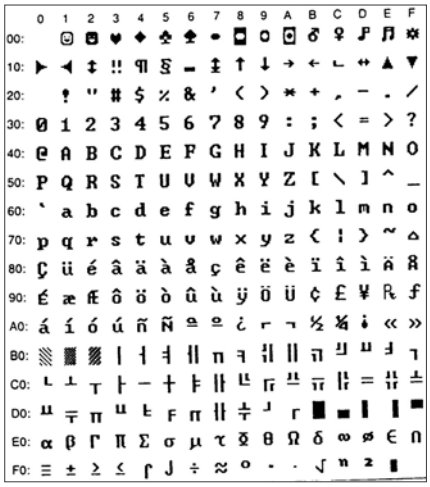
Código ASCII/ANSI de nivel bajo (2)

Byte	carácter
0101 0000	P
0101 0001	Q
0101 0010	R
0101 0011	S
0101 0100	T
0101 0101	U
0101 0110	V
0101 0111	W
0101 1000	X
0101 1001	Y
0101 1010	Z
0101 1011	[
0101 1100	\
0101 1101	]
0101 1110	^
0101 1111	_

Byte	carácter
0110 0000	`
0110 0001	a
0110 0010	b
0110 0011	c
0110 0100	d
0110 0101	e
0110 0110	f
0110 0111	g
0110 1000	h
0110 1001	i
0110 1010	j
0110 1011	k
0110 1100	l
0110 1101	m
0110 1110	n
0110 1111	o

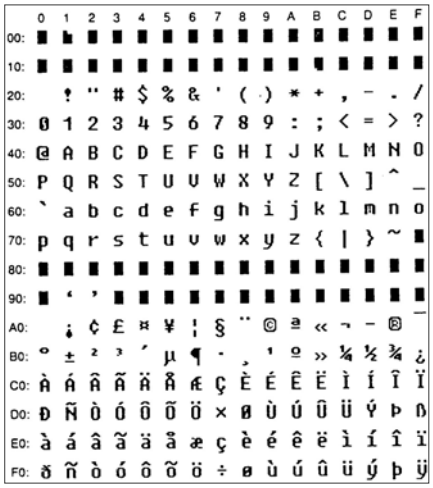
Byte	carácter
0111 0000	p
0111 0001	q
0111 0010	r
0111 0011	s
0111 0100	t
0111 0101	u
0111 0110	v
0111 0111	w
0111 1000	x
0111 1001	y
0111 1010	z
0111 1011	{
0111 1100	|
0111 1101	}
0111 1110	~
0111 1111	

Tabla de código ASCII extendido



00-0F: Valor decimal: 000-015
10-1F: Valor decimal: 016-031
20-2F: Valor decimal: 032-047
30-3F: Valor decimal: 048-063
40-4F: Valor decimal: 064-079
50-5F: Valor decimal: 080-095
60-6F: Valor decimal: 096-111
70-7F: Valor decimal: 112-127
80-8F: Valor decimal: 128-143
90-9F: Valor decimal: 144-159
A0-AF: Valor decimal: 160-175
B0-BF: Valor decimal: 176-191
C0-CF: Valor decimal: 192-207
D0-DF: Valor decimal: 208-223
E0-EF: Valor decimal: 224-239
F0-FF: Valor decimal: 240-255

Tabla de código ANSI extendido



00-0F: Valor decimal: 000-015
10-1F: Valor decimal: 016-031
20-2F: Valor decimal: 032-047
30-3F: Valor decimal: 048-063
40-4F: Valor decimal: 064-079
50-5F: Valor decimal: 080-095
60-6F: Valor decimal: 096-111
70-7F: Valor decimal: 112-127
80-8F: Valor decimal: 128-143
90-9F: Valor decimal: 144-159
A0-AF: Valor decimal: 160-175
B0-BF: Valor decimal: 176-191
C0-CF: Valor decimal: 192-207
D0-DF: Valor decimal: 208-223
E0-EF: Valor decimal: 224-239
F0-FF: Valor decimal: 240-255

La codificación en Base 64

Valor 6 bits		Carácter codificado	Valor 6 bits		Carácter codificado	Valor 6 bits		Carácter codificado	Valor 6 bits		Carácter codificado
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
										(Relleno)	=

Tabla de codificación en Base 64

Cada 3 bytes ANSI (24 bits) se convierten en 4 elementos Base 64 de 6 bits cada uno. El fichero aumenta un 33% pero ello se compensará al usar la compresión zip.

Ejemplo de codificación Base 64

$Hola_{ANSI}$ = 01001000 01101111 01101100 01100001
$Hola_{B64}$ = 010010 000110 111101 101100 011000 01 (00 00) = SG9sYQ= =

Valor 6 bits		Carácter codificado	Valor 6 bits		Carácter codificado	Valor 6 bits		Carácter codificado	Valor 6 bits		Carácter codificado
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/
										(Relleno)	=

Tabla de codificación en Base 64

Tabla de primos del 1 al 1000

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
101	103	107	109	113	127	131	137	139	149	151	157	163	167	173	179	181	191	193	197	199				
211	223	227	229	233	239	241	251	257	263	269	271	277	281	283	293									
307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397									
401	409	419	421	431	433	439	443	449	457	461	463	467	479	487	491	499								
503	509	521	523	541	547	557	563	569	571	577	587	593	599											
601	607	613	617	619	631	641	643	647	653	659	661	673	677	683	691									
701	709	711	727	733	739	743	751	757	761	769	773	787	797											
809	811	821	823	827	829	839	853	857	859	863	877	881	883	887										
907	911	919	929	937	941	947	953	967	971	977	983	991	997											

Tabla de primos del 1001 al 2000

1009	1013	1019	1021	1031	1033	1039	1049	1051	1061	1063	1069	1087	1091	1093	1097	
1103	1109	1117	1123	1129	1151	1153	1163	1171	1181	1187	1193					
1201	1213	1217	1223	1229	1231	1237	1249	1259	1277	1279	1283	1289	1291	1297		
1301	1303	1307	1319	1321	1327	1361	1367	1373	1381	1399						
1409	1423	1427	1429	1433	1439	1447	1451	1453	1459	1471	1481	1483	1487	1489	1493	1499
1511	1523	1531	1543	1549	1553	1559	1567	1571	1579	1583	1597					
1601	1607	1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693	1667	1699		
1709	1721	1723	1733	1741	1747	1753	1759	1777	1783	1787	1789					
1801	1811	1823	1831	1847	1861	1867	1871	1873	1877	1879	1889					
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987	1993	1997	1999				

Polinomios primitivos

Polinomios para n = 3: $x^3 + x + 1$; $x^3 + x^2 + 1$
Polinomios para n = 4: $x^4 + x + 1$; $x^4 + x^3 + 1$
Polinomios para n = 5: $x^5 + x^2 + 1$; $x^5 + x^4 + x^3 + x^2 + 1$; $x^5 + x^4 + x^2 + x + 1$; $x^5 + x^3 + x^2 + x + 1$; $x^5 + x^4 + x^3 + x + 1$; $x^5 + x^3 + 1$
Polinomios para n = 6: $x^6 + x + 1$; $x^6 + x^5 + x^2 + x + 1$; $x^6 + x^5 + x^3 + x^2 + 1$; $x^6 + x^4 + x^3 + x + 1$; $x^6 + x^5 + x^4 + x + 1$; $x^6 + x^5 + 1$

(1, 0)	(11, 2, 0)	(21, 2, 0)	(31, 3, 0)	(41, 3, 0)
(2, 1, 0)	(12, 6, 4, 1, 0)	(22, 1, 0)	(32, 7, 6, 2, 0)	(42, 5, 4, 3, 2, 1, 0)
(3, 1, 0)	(13, 4, 3, 1, 0)	(23, 5, 0)	(33, 13, 0)	(43, 6, 4, 3, 0)
(4, 1, 0)	(14, 5, 3, 1, 0)	(24, 4, 3, 1, 0)	(34, 8, 4, 3, 0)	(44, 6, 5, 2, 0)
(5, 2, 0)	(15, 1, 0)	(25, 3, 0)	(35, 2, 0)	(45, 4, 3, 1, 0)
(6, 1, 0)	(16, 5, 3, 2, 0)	(26, 6, 2, 1, 0)	(36, 11, 0)	(46, 8, 5, 3, 2, 1, 0)
(7, 1, 0)	(17, 3, 0)	(27, 5, 2, 1, 0)	(37, 6, 4, 1, 0)	(47, 5, 0)
(8, 4, 3, 2, 0)	(18, 7, 0)	(28, 3, 0)	(38, 6, 5, 1, 0)	(48, 7, 5, 4, 2, 1, 0)
(9, 4, 0)	(19, 5, 2, 1, 0)	(29, 2, 0)	(39, 4, 0)	(49, 9, 0)
(10, 3, 0)	(20, 3, 0)	(30, 6, 4, 1, 0)	(40, 5, 4, 3, 0)	(50, 4, 3, 2, 0)

Algunos polinomios de x^n para n = 1 hasta n = 50

Explicación de la notación: $(50, 4, 3, 2, 0) \Rightarrow p(x) = x^{50} + x^4 + x^3 + x^2 + 1$

Software: el proyecto docente Criptolab

- En el año 1995, terminando el primer curso en que se imparte la asignatura de Seguridad Informática en la Escuela Universitaria de Informática de la Universidad Politécnica de Madrid, España, el profesor de la misma echa a andar un proyecto docente con el nombre Criptolab. Básicamente, el objetivo es crear un conjunto de aplicaciones y software de prácticas hechas por alumnos memoristas de últimos cursos, con el fin de formar un completo laboratorio de criptografía y demás herramientas de seguridad informática, de libre distribución y orientado hacia un entorno educativo.
- Para ello se van creando y actualizando enunciados de prácticas en distintas versiones del cuaderno de prácticas y se generan aplicaciones para su uso en el laboratorio de criptografía y seguridad informática.
- En esta página encontrará algunos de los programas que han pasado la prueba final y, por lo tanto, están en Internet para su libre descarga.

Cuaderno de prácticas en html

- Basado en un trabajo inicial realizado por Dña. María Eugenia González Lozano de fecha septiembre de 1999, este cuaderno se ha ido actualizando incluyendo nuevas prácticas y nuevo software de laboratorio desarrollado por alumnos memoristas de la Escuela Universitaria de Informática de la UPM.
- Cuenta con un total de 32 enunciados de prácticas agrupados en este momento en seis bloques con diferentes apartados. En cada uno de estos apartados se incluye un test, en total 15.
- Todas las prácticas se realizan con software propio o bien ajeno siempre de libre distribución.
- ☞ Se han desarrollado distintos proyectos cuyo objetivo era adaptar y actualizar el cuaderno, dándole un formato nuevo y nuevas prestaciones tales como desarrollo de cada práctica y almacenamiento de datos de la misma en línea con el navegador, a través de un perfil de usuario, introducción de un nivel de ayuda contextual en cada enunciado con captura de pantallas, etc., ... pero desgraciadamente no han dado los frutos esperados. Es posible que a final de este año 2006 podamos contar con una versión 4.0 de este cuaderno.

http://www.criptored.upm.es/software/sw_m001k.htm 

Enunciados de prácticas en la versión 3.0

- Entropía de la Información
- Características del Lenguaje
- Cálculos en Matemática Discreta
- Cifrado por Desplazamiento Puro
- Cifrado por Decimación Pura
- Cifrado por Decimación y Despl.
- Cifrado de Vigenère
- Cifrado de Beaufort
- Cifrado de Clave Continua
- Cifrado de Vernam
- Cifrado por Filas
- Cifrado por Columnas
- Cifrado de Playfair
- Cifrado de Hill Digrámico
- Cifrado de Hill N-grámico
- DES Modo ECB
- Debilidades y Ataques a DES
- IDEA Modo ECB
- Función hash MD5
- Función hash SHA-1
- Mochila de Merkle-Hellman
- Intercambio de Clave de DH
- Generación de Claves RSA
- Cifrado RSA con ExpoCrip
- Cifrado RSA con gen RSA
- Firma Digital RSA
- Cifrado ElGamal
- Firma Digital ElGamal
- Firma Digital DSS
- PGP Versión 2.6.3i
- Creación de Claves y Cifrado Convencional con PGP 8.0
- Gestión de Claves y Cifrado Híbrido con PGP 8.0

Nuevas prácticas en próxima versión

A lo largo del año 2006, y en una nueva versión de este cuaderno de prácticas, se espera incluir algunos de los títulos que se indican más abajo, junto al correspondiente software para poder realizarlas.

- Cifra por Homófonos
- Cifra y seguimiento del AES
- Secuencias Cifrantes
- Cifra por Flujo
- Ataques por Fuerza Bruta y Paradoja del Cumpleaños en Funciones Hash
- Cifrado con Curvas Elípticas
- Gestión Avanzadas de Claves con PGP 8.0
- Seguimiento Certificados X.509
- Certificado X.509 en Cliente
- Análisis de la densidad y tipos de claves RSA
- Ataques a RSA basado en la paradoja del cumpleaños
- Simulación del Entorno Kerberos
- Protocolo de Transferencia Inconsciente de Rabin
- Póquer Mental con Criptografía Simétrica
- Póquer Mental con Criptografía Asimétrica
- Simulación Secure Socket Layer
- Esteganografía con Stools
- Cifrado con Criptografía Visual
- Intercambio de Clave Cuántico

http://www.criptored.upm.es/paginas/software.htm#propio

genRSA: generación de claves y cifra RSA

- Autor: D. Juan Carlos Pérez García. Fecha: Febrero de 2004.
- Software basado en la librería pública Cryptlib que permite realizar los cálculos correspondientes a la generación del par de claves asimétricas RSA, partiendo de dos primos con igual número de bits o ligeramente distintos. Generación manual o automática. Para valores de p y q desde 16 -valor mínimo- hasta 32 bits, éstos pueden ser decimales o hexadecimales; para valores mayores hasta una clave de 2048 bits, los datos de la clave deberán ser hexadecimales.
- Generación de claves RSA manual y automática hasta 2048 bits.
- Test de primalidad de Miller-Rabin y Fermat.
- Obtención de claves parejas y cálculo de mensajes no cifrables.
- Cifrado y descifrado de texto y números.
- Descifrado de números con el TRC.
- Ataque al módulo por factorización de primos cercanos.
- Ataque al mensaje secreto por cifrado cíclico.
- Ataque a la clave privada por paradoja del cumpleaños.

http://www.criptored.upm.es/software/sw_m001d.htm

ExpoCrip: cifra y firma exponencial

- Autor: Dña. Olga Mariana González Ming. Fecha: Febrero de 2004.
- Software para prácticas de cifrado exponencial de números decimales, valores hexadecimales y texto ASCII, realizado con librerías propias y eficiente para operaciones de hasta centenas de bits. Incluye herramientas propias para el trabajo con números primos y ayuda contextual.
- Generación manual de claves RSA.
- Cifrado y descifrado RSA de texto y números.
- Obtención de claves parejas y cálculo de mensajes no cifrables.
- Ataque al módulo por factorización con método Pollard Rho.
- Ataque al mensaje secreto por cifrado cíclico.
- Ataque a la clave privada por paradoja del cumpleaños.
- Firma digital RSA.
- Generación manual de claves ElGamal.
- Cifrado y descifrado ElGamal de texto y números.
- Firma digital ElGamal y firma digital DSS.

http://www.criptored.upm.es/software/sw_m001l.htm

safeDES: cifra y ataque al DES

- Autor: D. Miguel Ángel Jiménez Muñoz. Fecha: Enero de 2003.
- Software de cifrado, descifrado y ataques por fuerza bruta de forma similar a los desarrollados por RSA Challengue al algoritmo Data Encryption Standard DES. Operaciones con archivos o bien texto claro por teclado. Los textos y las claves pueden introducirse en formato ANSI o hexadecimal. Si bien el algoritmo implementa sólo el modo Libro Electrónico de Códigos ECB, es posible comprobar los ataques de los que fue objeto en modo CBC con el simple uso la calculadora científica de Windows. Los módulos de ataque permiten delimitar un espacio de claves subconjunto del espacio real. La aplicación cuenta una amplia ayuda contextual que permite el mejor seguimiento de las prácticas con este software.
- Cifrado y descifrado modo ECB.
- Ataque tipo monousuario.
- Ataque tipo simulación multiusuario.
- Ataque tipo multiusuario: aplicación cliente.
- Ataque tipo multiusuario: aplicación servidor.

http://www.criptored.upm.es/software/sw_m001j.htm

CriptoRES: funciones hash MD5 y SHA-1

- Autor: D. José Azaña Alonso. Fecha: Enero de 2001.
- Software para el estudio y seguimiento de las funciones hash más conocidas usadas en la compresión del documento para la firma digital y también en otras aplicaciones de autenticación como los certificados digitales.
- Tanto para MD5 como para SHA-1, la aplicación obtiene los resúmenes de documentos de archivos o texto introducido por teclado.
- Permite hacer un seguimiento del algoritmo de resumen, a nivel de bloques mostrando todas las operaciones en hexadecimal o bien siguiendo los pasos de las operaciones en bajo nivel. Como en este último caso la información mostrada está en bits, por su gran extensión muestra sólo el primer bloque de resumen que es precisamente donde se incluyen los rellenos para congruencia con el tamaño del bloque de 512 bits.
- Incluye una representación gráfica de la ecuación matemática del problema del ataque por la paradoja del cumpleaños.
- Ayuda en formato Windows estándar y contextual mediante la tecla F1.

http://www.criptored.upm.es/software/sw_m001h.htm

Hill: cifra y criptoanálisis

- Autor: Dña Mª Carmen Cogolludo Alcarazo. Fecha: Marzo de 2001.
- Aplicación para prácticas de laboratorio con el cifrador poligrámico de Hill.
- Permite cifrar y descifrar archivos txt con una matriz clave de tamaño 2x2 hasta 10x10 dentro de los siguientes cuerpos: alfabeto castellano con letras en mayúsculas (mod 27), alfabeto incluyendo además los dígitos (mod 37) y por último un subconjunto de caracteres ASCII imprimibles (mod 191). En este último caso, la salida puede guardarse como un archivo en formato base 64.
- Las matrices clave pueden guardarse como un archivo.
- Permite además realizar ataques por criptoanálisis según el método de Gauss-Jordan. Una vez criptoanalizada la matriz clave, entrega un seguimiento de las ecuaciones que han permitido romper el sistema.
- El programa incluye una herramienta para el cálculo del determinante de una matriz, la matriz inversa y el número de matrices válidas dentro de un cuerpo.
- Ayuda en formato Windows estándar y contextual mediante la tecla F1.

http://www.criptored.upm.es/software/sw_m001i.htm

CriptoClásicos: cifra y criptoanálisis

- Autor: D. Luis Miguel Motrel Berjano. Fecha: Marzo de 1999.
- Aplicación para prácticas de sistemas de cifra clásicos que incluye algoritmos de cifra monoalfabética por sustitución y por transposición, cifra polialfabética con los cifradores de Vigenère, de Beaufort y de clave continua.
- Permite, además de cifrar y descifrar, realizar ataques por criptoanálisis a los sistemas anteriores mediante el uso de técnicas de estadísticas del lenguaje.
- Incluye además el cifrador de Vernam, el cifrador de Playfair, el cifrador de Hill digrámico y cifrado por transposiciones.
- Todas las operaciones de cifra pueden realizarse con los alfabetos castellano módulo 27 (letras mayúsculas), castellano módulo 37 (letras y dígitos) e inglés módulo 26 y módulo 36.
- Incluye un apartado con herramientas características de trabajo dentro de un cuerpo finito y estadísticas básicas del lenguaje. Las operaciones están limitadas a cuerpos menores que 65.536.
- Ayuda en formato Windows estándar y contextual mediante la tecla F1.

http://www.criptored.upm.es/software/sw_m001c.htm

CryptoIDEA: cifra y seguimiento de IDEA

- Autor: Dña. Esther Sánchez Mellado. Fecha: Septiembre de 1999.
- Software de prácticas realizado en Delphi que permite cifrar y descifrar con el algoritmo IDEA así como realizar un seguimiento del proceso y la generación de claves directas e inversas de cifra.
- Muestra además los ficheros en números enteros y en binario.
- Incluye un sistema de gestión de bases de datos tipo Paradox 5.0 para el mantenimiento (creación, modificación, borrado, etc.) de claves.
- La generación de claves se hace a partir de un texto o clave ASCII.
- Incluye un apartado de herramientas para cálculos típicos dentro de un cuerpo, en especial mod 65.536 y mod 65.537, valores usados en IDEA. Además el cálculo del máximo común divisor, inversos y conversiones de carácter a ASCII, de entero a binario y de binario a entero.
- Ayuda en formato Windows estándar y contextual mediante la tecla F1.

http://www.criptored.upm.es/software/sw_m001f.htm

Fortaleza: operaciones en cuerpo de cifra

- Autor: Dña. Cristina Chércoles Larriba. Fecha: Febrero de 1999.
- Software de prácticas realizado en Visual Basic que permite realizar y simular las operaciones dentro de un cuerpo más características en sistemas de cifra exponencial como son RSA y ElGamal: operaciones básicas de suma, resta, multiplicación y división, con o sin módulo, raíz, máximo común divisor, cálculo de inversos, potencia y primalidad.
- Usa una librería de números grandes: decenas hasta centenas de dígitos.
- Incluye un módulo de factorización de números compuestos por dos primos mediante los métodos de Pollard Rho, Dixon y Fraccciones Continuas. Además se muestra una lista de primos para poder trabajar con ellos, un conjunto de ejemplos y una tabla de primos titánicos.
- Incluye un módulo de cálculo del logaritmo discreto mediante los métodos de Búsqueda Exhaustiva, Paso Gigante - Paso Enano y Pohlig - Hellman. Además presenta un conjunto de ejemplos.
- Ayuda en formato Windows estándar y contextual mediante la tecla F1.

http://www.criptored.upm.es/software/sw_m001e.htm

Tutorial PGP 2.63i: cuaderno en html

- Autor: D. David Liñán Zayas. Fecha: Julio de 1999.
- Curso en html para un correcto aprendizaje del programa PGP en su versión 2.6.3i. El software presenta una explicación de los algoritmos usados por PGP con figuras, la generación y gestión de claves, cifra, firma, etc. Incluye además diversos ejemplos y enlaces a páginas Web de interés.
- Introducción a la criptografía.
- Comenzando con PGP.
- Generación de claves
- Envío y recepción de correo electrónico.
- Otras funciones de PGP.
- Manejo de claves.
- Distribución de claves.
- Revocación de claves.
- Instalar y configurar PGP.
- Enlaces.

http://www.criptored.upm.es/software/sw_m001g.htm

LECC: libro electrónico de cifra clásica

- Autor: Dña. Ana María Camacho Hernández. Fecha: Junio de 1998.
- Libro electrónico realizado con ToolBook que hace un repaso a los temas principales de la criptografía clásica, incluyendo fotografías de máquinas de cifrar así como de los algoritmos más característicos para la realización de prácticas sencillas en un entorno Windows. Cuenta con cinco secciones:
- Sección 0: Historia de la criptografía. Principios de las técnicas criptográficas. Presentación de los algoritmos escítala, de Polybios y del César.
- Sección 1: Máquinas de cifrar. Rueda de Jefferson, discos de Alberti y Wheatstone, cifrador de Vernam, máquinas Enigma, M-325 y Hagelin.
- Sección 2: Cifrados por sustitución. Monoalfabética, polialfabética, cifra de Vigenère, de Beaufort, por homofonías, de Beale, de Playfair y de Hill.
- Sección 3: Cifrados por transposición. Cifra por grupos, series, columnas y filas.
- Sección 4: Algoritmos. Están implementados en la misma aplicación todos los algoritmos de cifrado y descifrado por sustitución y transposición para poder ejercitarse con ejemplos de textos introducidos por teclado.

http://www.criptored.upm.es/software/sw_m001a.htm

MH: cifra y criptoanálisis de mochilas

- Autor: D. Juan Carlos Rodríguez Castellano. Fecha: Julio de 1997.
- Software para prácticas de cifrado y descifrado del sistema de cifra con mochila de Merkle - Hellman realizado en Delphi.
- Se ha incluido una librería para trabajar con números grandes: decenas o centenas de dígitos, y herramientas básicas de trabajo dentro de un cuerpo.
- Permite el diseño de mochilas del tamaño y datos que desee el usuario, con tamaño recomendable M-H o bien mochilas con un tamaño proporcional al modelo recomendado por Merkle y Hellman.
- Una vez creada una mochila, el programa incluye la opción de criptoanálisis de la misma según el método de Shamir y Zippel, indicando luego de romper la mochila clave los valores analizados hasta lograr su objetivo
- Ayuda en formato Windows estándar y contextual mediante la tecla F1.

http://www.criptored.upm.es/software/sw_m001b.htm

Otro software que se usa en la asignatura

Además del software propio desarrollado dentro del proyecto Criptolab antes comentado, en las prácticas de la asignatura se usa el siguiente software de libre distribución y enlaces a Internet para la realización de algunas prácticas:

- Generación de claves RSA con OpenSSL
  - http://www.slproweb.com/products/Win32OpenSSL.html
- Correo electrónico y cifrado: PGP versión 8.0 Windows
  - http://www.criptored.upm.es/paginas/software.htm#freeware
- Esteganografía: Página de herramientas Steganos Security
  - http://www.stegoarchive.com/
- Criptografía visual: página Web del Dr.Stinson
  - http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html
- Criptografía cuántica: página de Dartmouth College
  - http://www.cs.dartmouth.edu/~jford/crypto.html

La formación universitaria en España

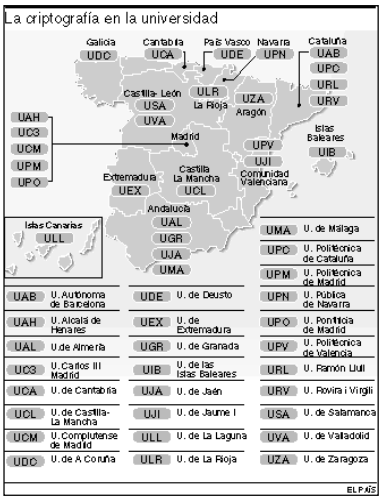
En 1990 la oferta es de 1 asignatura. En 1998, ésta crece hasta 37. En 2005, son más de 60.

El crecimiento tan marcado de esta oferta en España tiene su justificación en diversos hechos de ocurrencia casi simultánea:

- Un entorno universitario propicio.
- Potenciación del mercado laboral.
- Una legislación específica y muy fuerte en seguridad informática.

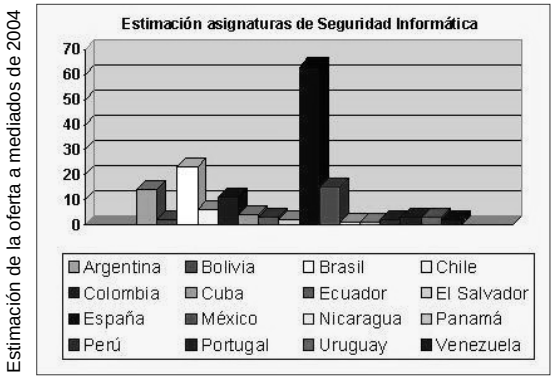
☞ Esta expansión no se ha dado aún en los países de Latinoamérica; sin embargo, hay que estar atentos puesto que el auge de las tecnologías de seguridad de la información es un fenómeno de carácter mundial.

Referencia: "Enseñanza de la Criptografía en España. Primer Informe sobre Perfiles de Asignaturas". Jorge Ramió A., Pino Caballero G.; revista SIC número 34, España, abril de 1999. Gráfica publicada en Ciberpaís, España. (Email Dra. Pino Caballero: pcaballe@ull.es)



La oferta docente en Iberoamérica

Hay un desarrollo muy dispar entre los países de Iberoamérica. Detrás de un crecimiento espectacular en España en los últimos 10 años (1994-2004), sólo muestran una oferta relativamente alta Brasil, Argentina, México y Colombia.



Otros países que no aparecen en este cuadro presentan una oferta docente muy muy baja o casi nula.

Aunque estos datos son una estimación, los valores se basan en un informe del autor y la posterior observación de la oferta universitaria en dichos países.

¿Una Ingeniería en Seguridad Informática?

- Irvine, Chin y Frincke en su artículo Integrating Security into the Curriculum, Revista IEEE, diciembre de 1998, comentaban que: "La Seguridad Informática podría ser el objetivo principal de un curriculum que debería investigar los fundamentos y enfoques técnicos de la seguridad con una profundidad considerable".
- El autor de este libro viene insistiendo desde el año 2000 en la necesidad de una formación amplia en seguridad informática en nuestras universidades. Si bien puede ser utópico un título de Ingeniero en Seguridad Informática, gran parte del temario que propongo a continuación se imparte en varios cursos de Máster en España y en algunos países de Latinoamérica. Y en 2005 algunas universidades españolas ya comienza a pensar en ello ☺.
- En mi ponencia Introducción de las enseñanzas de seguridad informática en los planes de estudio de las ingenierías del siglo XXI, Congreso JENUI, Palma de Mallorca, España, julio de 2001, comentaba: "Se detecta una necesidad en el mercado de nuevos perfiles de ingenieros en seguridad pero no existe respuesta adecuada de la universidad".

Créditos propuestos para un Máster (1/4)

1 crédito docente corresponde a 10 horas de clase de teoría o de prácticas

Fundamentos y Temas Avanzados de la Aritmética Modular (6 cr.)
- Principios y operaciones con cuerpos finitos.
- Algoritmos de cálculos en cuerpos finitos: inversos, raíces, etc.
- Cálculos en Campos de Galois GF.
- Factorización y cálculos con polinomios en GF.
- Uso de curvas elípticas en criptografía.

Fundamentos de la Seguridad Informática (4,5 cr.)
- Conceptos básicos de la seguridad informática.
- Historia de la criptografía, sistemas de cifra clásicos.
- Teoría de la información en seguridad y criptografía.
- Complejidad de los algoritmos en seguridad y criptografía.

Gestión de la Seguridad Informática (6 cr.)
- Políticas de seguridad informática, normativas y estándares.
- Planes de contingencia y de recuperación ante desastres.
- Esquemas de protección física de los datos y copias de seguridad.

Avance por años o cursos

Créditos propuestos para un Máster (2/4)

Legislación en Seguridad Informática (4,5 cr.)
- Leyes de protección de datos.
- Leyes de firma digital, comercio electrónico, etc.
- Legislación de ámbito internacional.
- Delito informático.

Criptografía (6 cr.)
- Cifrado simétrico y asimétrico.
- Algoritmos de autenticación y funciones hash.
- Algoritmos de firma digital.
- Algoritmos y esquemas de certificados digitales.
- Correo electrónico seguro y esquemas híbridos.
- Comparativa y fortaleza de los algoritmos de cifra.

Seguridad en Sistemas Operativos, Lenguajes y Bases de Datos (9 cr.)
- Sistemas operativos seguros, libro naranja.
- Seguridad en entornos Windows, Linux, Unix, Solaris.
- Programación y rutinas de seguridad en C++ y Java.
- Seguridad en SGBD y bases de datos distribuidas.

Créditos propuestos para un Máster (3/4)

Seguridad en Redes (12 cr.)
- Protocolos de seguridad en Internet e Intranet.
- Plataformas y pasarelas seguras: SHTTP, SSL, TLS, IPSec.
- Instalación y gestión de un servidor Web y de correo seguros.
- Autenticación en redes: Kerberos, SSH, X.509.
- Instalación y gestión de Autoridades de Certificación.
- Protección con cortafuegos, detección de intrusos, DoS.
- Redes privadas virtuales VPN, túneles.
- Redes inalámbricas: protocolos, estándares, vulnerabilidades.
- Gestión y fortificación de la máquina.
- Herramientas de control y auditoría de la máquina.
- Hacking ético: test de penetración.

Virus Informáticos (4,5 cr.)
- Clasificación, características y tipos de virus.
- Medidas de alerta, protección y eliminación.
- Análisis de algoritmos malignos, hoax, spam, gusanos y troyanos.
- Seguimiento y caracterización de un virus en lenguaje de bajo nivel.

Créditos propuestos para un Máster (4/4)

Negocio y Comercio Electrónico (4,5 cr.)
- Normas del mercado de e-commerce, e-business.
- Aspectos comerciales del inicio de actividades.
- Seguimiento de las transacciones en la red.
- Norma SET y otros estándares.
- Caracterización de tipos de comercio electrónico.
- Aspectos técnicos del e-government.

Auditoría, Peritaje y Forensia Informática (7,5 cr.)
- Técnicas de auditoría.
- Auditoría de sistemas y seguridad.
- Auditoría jurídica.
- Peritaje y técnicas forenses en seguridad informática.

Temas Avanzados en Criptografía y Seguridad Informática (4,5 cr.)
- Protocolos criptográficos: e-voting, e-gaming, conocimiento cero, ...
- Cifra avanzada: esteganografía, autómatas celulares, criptografía cuántica, ...
- Autenticación avanzada: biometría, smartcards, notarios electrónicos, ...
- Tecnología de tarjetas inteligentes: interconexión, funcionalidades, ...
- Protección del copyright, marcas de agua, sellos de tiempo, ... etc.

Una formación técnica con 11 asignaturas y unas 700 horas

Con cerca de 350 horas de teoría...

y otras 350 horas de prácticas.

Todos estos temas deberían ser del conocimiento de un Responsable o Director de Seguridad Informática ☺

Cuestiones y ejercicios (1 de 2)

1. En un texto cifrado por sustitución afín, se tiene como criptograma C = PCERC QBCSK AQBGR LGFJQ KCXKÑ LCECN RKZHL KKXGF LCAFB. ¿Qué es lo primero que hacemos? Ataque el criptograma con el software de la asignatura. ¿Qué puede concluir?
2. Con el cifrador de Vernam y código Baudot ciframos M = SOL con la clave K = MAR. ¿Qué se obtiene como criptograma?
3. Observando el código ASCII/ANSI de nivel bajo en binario, ¿Por qué es desaconsejable cifrar con mochilas de tamaño 4 u 8?
4. La clave DES escrita en código ASCII es K = HOLAhola. ¿Cuál sería en este caso la clave de 56 bits? ¿Qué puede decir de esto?
5. Observando la tabla de primos del 1 al 1.000 y de 1.001 al 2.000, ¿podríamos concluir que en una ventana igual (2.001 al 3.000; 3.001 al 4.000, etc.) cada vez hay más números primos? ¿Por qué?

Cuestiones y ejercicios (2 de 2)

6. ¿Por qué en módulo 37 existen más inversos que en módulo 27?
7. Codifique en base 64 el texto de 10 caracteres M = ¡Qué tal!
8. ¿Qué mensaje hay en M' = v01lb nNham Ugb2N 1bHRv Pw= = que está codificado en base 64? ¿Por qué el relleno es igual a dos?
9. ¿En cuánto aumenta el tamaño cuando convertimos ASCII/ANSI a código base 64? ¿Es eso significativo en PGP? ¿Por qué sí o no?
10. ¿En qué zona podemos decir que el código ASCII y el ANSI son iguales?
11. ¿Se codificará igual en ASCII que en ANSI el mensaje M_1 = "Voy a entrar"? Y si ahora el mensaje es M_2 = "Pasa, está abierto" ¿Qué consecuencias puede tener esto en un programa?
12. Un mensaje codificado en ANSI hexadecimal es 43 72 69 70 74 6F 67 72 61 66 ED 61, ¿cuál es el texto en castellano?

Palabras finales del autor

- Estimado/a amigo/a: si estas diapositivas le han servido para su formación en seguridad o bien las ha podido usar para dar formación a terceros, puedo decir misión cumplida ☺.
- Como seguro comprenderá, la tarea de actualizar cada año un libro electrónico como éste, precisamente en un área como la seguridad informática, de un desarrollo vertiginoso, resulta muy pesada... y ya van seis ediciones.
- Por este motivo y dado que, además de la coordinación de la la Red Temática Iberoamericana de Criptografía y Seguridad de la Información CriptoRed, posiblemente deberé trabajar en proyectos relacionados con la Seguridad de la Sociedad de la Información, es muy posible que a partir de hoy las versiones de este libro tengan una mayor vigencia y su actualización se plantee cada dos o más años.

Fin del capítulo y del libro