Que otros se jacten de los libros que les ha sido dado escribir; yo me jacto de aquellos que me fue dado leer. Jorge Luis Borges.

***96 The next stage of Differential Fault Cryptanalysis: How to break completely unknow cryptosystems. Octubre 1996. Disponible en //www.jya.com/dfa.htm.

***98 Skipjack and KEA algorithm specifications version 2.0. 29de Mayo de 1998. Disponible en http://csrc.nist.gov/encryption/skipjack-kea.htm

ABR77 Teoría de la información y codificación. Norman Abramson. Paraninfo 1977.

AEN28 AENEAS TACTICUS. Textos completos. LOEB CLASSICAL LIBRARY 1928.

AMO97 Seguridad para INTRANET e INTERNET. Edward Amoroso, Ronald Sharp. Prentice Hall 1997.

AND** Improved Differential Fault Analysis. Ross J. Anderson, Markus G. Kuhn. Disponible en //www.jya.com/akdfa.txt.

AND93 Why cryptosystems fail. Ross Anderson. Disponible en http://www.counterpane.com.

AND93b Introducción a la combinatoria. Ian Anderson. Vicens Vives 1993.

AND94 Number theory. George A. Andrews. Dover 1994.

AND98 On the limits of steganography. Ross J. Anderson, Fabien A.P.Petitcolas. IEEE Journal of selected areas in communications. Mayo 1998.

AND99 Information hiding-A survey. Ross J. Anderson, Fabien A.P.Petitcolas, Markus G. Kuhn. Proceedings of the IEEE . Julio 1999.

APA93 Teoría de los números. E. Aparicio. Universidad del Pais Vasco 1993.

ART98 Galois Theory. Emil Artin. Dover 1998.

ALV96 Akelarre: Nuevo algoritmo de cifrado en bloque. Gonzalo Alvarez, Dolores de la Guía, Fausto Montoya, Alberto Peinado. Actas de la IV reunión española sobre criptología.

BAG96 The applications of genetic algorithms in cryptanalysis. A.J.Bagnall. Master of science thesis. University of East Anglia, 1996.

BAN96 Discrete-event system simulation. J. Banks, J. S. Carson, B. Nelson. Prentice Hall 1996.

BAR84 Cryptanalysis of shift-register generated stream cipher systems. Wayne G. Barker. Aegean Park Press 1984.

BAU82 Cryptology – Methods and Maxims. Proceedings Eurocrypt 82. Springer Verlag.

BAU97 Decrypted secrets. F.L. Bauer. Springer Verlag 1997

BEC90 Introduction aux méthodes de la cryptologie. Brian Becket. Masson 1990.

BEI77 Recreations in theory of numbers. Albert H. Beiler. Dover 1977.

BEK82 Cipher systems. The protection of communications. Northwood books 1982.

BEL97 Probable plaintext cryptanalysis of the IP security protocols. Steven M. Bellovin. Proceedings of the 1997 Symposium on Network and Distributed Systems Security. IEEE Press.

BEU94 Cryptology. Albrecht Beutelspacher. Mathematical Association of America 1994.

BRE89 Factorization and primality testing. David M. Bressoud. Springer –Verlag 1989

BIH91 Differential cryptanalysis of the full 16-round DES. Eli Biham. 1991. Disponible en http://www.counterpane.com.

BIH92 New types of cryptanalytic attacks using related keys. Eli Biham 1992. Disponible en http://www.counterpane.com.

BIH93 Differential cryptanalysis of the Data Encryption Standard. Eli Biham, Adi Shamir. Springer Verlag 1993.

BIH94 A know plaintext attack on the pkzip stream cipher. Eli Biham, Paul C. Kocher. 1994. Disponible en http://www.counterpane.com.

BIH94b On Matsui´s linear cryptanalysis. Eli Biham 1994. Disponible en http://www.counterpane.com.

BIH96 A new cryptanalytic attack on DES. Eli Biham y Adi Shamir. Octubre 1996. Disponible en http://www.jya.com/dfa.htm.

BIH96b Cryptanalysis of triple-modes of operation. Eli Biham 1996. Disponible en http://www.counterpane.com.

BIH97 Differential fault analysis of secret key cryptosystems. Eli Biham y Adi Shamir 1997. Disponible en http://www.counterpane.com.

BIH98 Initial observations on Skipjack: cryptanalysis of Skipjack-3XOR. Eli Biham y Adi Shamir 1998. Disponible en http://www.counterpane.com.

BIH98b Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. Eli Biham y Adi Shamir 1998. Disponible en http://www.counterpane.com.

BLA96 Minimal key lengths for symmetric ciphers to provide adequate comercial security. Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, Michael Wiener. Enero 1996. Disponible en http://www.counterpane.com.

BON** On the importance of checking computations. Dan Boneh, Richard A. DeMillo, Richard J. Lipton. Disponible en http://www.jya.com/smart.pdf.

BON98 Exposing an RSA private key given a small fraction of its bits. Dan Boneh, Glenn Durfee, Yair Frankel. http://theory.stanford.edu/~dabo/abstracts/bits_of_d.html.

BON99 Twenty years of attacks on the RSA cryptosystem. 1999. Dan Boneh. Disponible en http://crypto.stanford.edu/~dabo/pubs.html.

BOR93 A la búsqueda de la seguridad. Paulina Borsook. BYNARY 53. Julio/Agosto 1993.

BOS82 Codes, ciphers, and computers: An introduction to information security. Bruce Bosworth. Hayden 1982.

BUC99 Factorización de números grandes. Johannes Buchmann. Investigación y Ciencia. Abril de 1999.

CAI97 How to break Gifford's cipher. Thomas R. Cain, Alan T. Sherman. Cryptologia vol. XXI, nº 3 Julio 1997.

CAR86 The automated cryptanalysis of substitution ciphers. John M. Carroll, Steve Martin. Cryptologia vol. X nº 4, Octubre 1996.

CAR87 The automated cryptanalysis of polyalphabetic ciphers. John M. Carroll, Lynda Robbins. Cryptologia Vol. XI nº 4. Octubre de 1987.

CAS99 Seguridad en redes y cortafuegos. M. Castro Gil. Actas de los X Cursos de verano de la UNED. 1999.

CAS00 Sobre el uso de redes neuronales en el estudio de MD5.J. C. Hernández Castro, I. M. Galván León, J. M. Sierra Cámara, B. Ramos Alvarez, A. Muñoz Cuenca. En Criptología y Seguridad de la Información. Actas de le VI Reunión Española sobre criptología y seguridad de la información. RAMA 2000.

CHO84 A knapsack-type public key cryptosystem based on arithmetic in finite fields. Proceedings of CRYPTO 84. Springer-Verlag 1985.

CHO86 Two issues in public key cryptography. Ben-Zion Chor. MIT Press 1986.

CIL92 La teoría de los números. Javier Cilleruelo, Antonio Cordoba. Biblioteca Mondadori 1992.

CLA96 Combinatorial optimization and the knapsack cipher. Andrew Clark, Ed Dawson, Helen Bergen. Cryptologia vol. XX nº 1 Enero 1996.

CLA97 A parallel genetic algorithm for cryptanalysis of the polyalphabetic substitution cipher. Andrew Clark, Ed Dawson. Cryptologia Vol. XXI nº 2 Abril 1997

CLA98 Optimisation heuristics for cryptology. Andrew John Clark. Thesis por degree of Doctor of Philosphy. Febrero 1998.

COC73 A note on non-secret encryption. C. Cocks 1973. http://www.cesg.gov.uk/about/nsecret/home.htm.

COH95 Los números primos. Henri Cohen. Mundo Científico nº 161. Octubre 1995.

COH96 A course in computational algebraic number theory. Henri Cohen. Springer Verlag 1996.

COO84 A generalization of the knapsack algorithm using Galois fields. Rodney Cooper y Wayne Patterson. Cryptologia Vol. 8, nº 4. Octubre 1984.

COR90 Introduction to algorithms. Thomas H. Cormen, Charles E. Leiserson, Ronald R. Rivest. The MIT Press 1990.

COR00 Computing with quantum physics. David Cory, Raymond Laflamme. Dr. Dobb's Journal special report. Diciembre 2000.

COU99 The mathematics of ciphers. Number theory and RSA cryptography. S. C. Coutinho. A. K. Peters 1999.

CRA97 El desafío de los grandes números. Richard E. Crandall. Investigación y Ciencia Abril 1997.

CSC85 Departament of Defense. Password management guideline.CSC-STD-002.85.

DAT83 An introduction to Data Base Systems, vol. 2. Addison-Wesley 1983.

DEA85 Machine cryptography and modern cryptanalysis. Cipher A. Deavours, Louis Kruh. Artech House 1985.

DEM89 Applied cryptology, cryptographic protocols, and computer security models. Richard de Millo. American Mathematical society 1983.

DEN83 Cryptography and data security. Dorothy Elizabeth Robling Denning. Addison Wesley 1983.

DEN93 The clipper chip: A technical summary. Dorothy Denning. Abril 1993. http://www.COSC.georgetown.edu/~denning.

DEN94 Key escrowing today. Dorothy Denning. Abril 1993. http://www.COSC.georgetown.edu/~denning.

DEN99 Information warfare and security. Dorothy Denning. Addison Wesley 1999.

DEV93 Network security. Mario Devargas. NCC Blackwell Ltd. 1993.

DoD28 Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200.28-STD.

DRO** Códigos secretos. Asael Dror. BINARY 11.

DUR98 Criptosistemas de mochila. R. Durán, F. Montoya, J. Muñoz. NOVATICA nº 134. Julio-Agosto 1998.

DWI71 Cryptography the science of secret writing. Laurence Dwight Smith. Dover 1971.

EFF98 Cracking DES. Electronic Frontier Foundation. O´Reilly & Associates 1998.

ELL70 The possibility of non-secret encryption. J.H.Ellis 1970. http://www.cesg.gov.uk/about/nsecret/home.htm.

ELL87 The story of non-secret encryption. J.H.Ellis 1987. http://www.cesg.gov.uk/about/nsecret/home.htm.

FER81 Database security and integrity. E.B. Fernandez, R.C. Summers, C.Wood. Addison Wesley 1981.

FER96 Una nueva vía de ataque al DES. José Luis Ferrer Gomila, Llorenç Huguet. Actas de la IV Reunión Española de Criptología.

FER97 Cryptanalysis of Akelarre. N. Ferguson, B. Schneier. http://www.counterpane.com/akelarre.html.

FIP81 Federal Information Processing Standards Publication 81. DES modes of operation. 2 de Diciembre de 1980. disponible vía ftp en http://www.itl.nist.gov/fipspubs/fip81.htm.

FIP180 Federal Information Processing Standards Publication 180-1. Secure hash standard. 17 de Abril de 1995. disponible vía ftp en http://www.itl.nist.gov/fipspubs/fip180-1.htm.

FIP186 Federal Information Processing Standards Publication 186-1. Digital signature standard. 15 de Diciembre de 1998. disponible vía ftp en http://www.itl.nist.gov/fipspubs/.

FOR93 Automated cryptanalysis of substitution ciphers. W. S. Forsyth, R. Safavi-Naini. Cryptologia Octubre de 1993.

FOR95 Criptografía y seguridad en comunicaciones. Jordi Forné, José L. Melús y Miguel Soriano. Novatica No 116. Julio-agosto 1995.

FOS** Genetic Algorithm Hardness and Aproximation Complexity: A research agenda. James A. Foster. Disponible via ftp.

FOS97 Drawbacks of the One-Time Pad. Caxton C. Foster. Cryptologia Octubre de 1997.

FRI94 An adventurer´s guide to number theory. Richard Friedberg. Dover 1994.

FUS97 Técnicas criptográficas de protección de datos. Amparo Fúster, Dolores de la Guía, Luis Hernández Encinas, Fausto Montoya Vitini, Jaime Muñoz Masqué. Ra-Ma 1997.

GAR99 Seguridad y comercio en el Web. Simson Garfinkel , Gene Spafford. McGraw-Hill 1999.

GIB93 Primes and programming. An introduction to number theory with computing. Peter Giblin. Cambridge University Press 1993.

GOL82 Shift register sequences. Solomon W. Golomb. Aegean Park Press 1982.

GRE96 Ask and Ye shall receive: A study in social engineering. Toni Greening. ACM SIGSAC Vol. 14 Nº 2. Abril 1996

GUI90 Identification by biometrics. Daniel Guinier. ACM SICSAC Vol. 8 Nº 2-1990.

GUI98 Cifrado en flujo. Dolores de la Guía. IX Cursos de verano de la UNED. Ávila 1998.

HER99 Soluciones Criptográficas en aplicaciones no dedicadas. Julio César Hernández. Byte 133/134. Abril y Mayo de 1999.

HUG** Criptografía: Algoritmos DES y RSA. Lorenzo Huguet. Datamation.

HUG88 A first course in number theory. Edgar , Hugh M. Wadsworth 1988.

ITSEC Information Technology Security Evaluation Criteria (ITSEC). 1991.

JAK95 A fast method for cryptanalysis of substitution ciphers. Thomas Jakobsen. Cryptologia Vol. XIX nº 3. Julio de 1995.

KAS40 Matemáticas e imaginación. E. Kasner y James Newman. ORBIS 1987 traducción de la obra original impresa en 1940.

KIN92 An implementation of probabilistic realaxation in the cryptanalysis of simple substitutions ciphers. John C. King, C. Bahler. Cryptologia Vol. XVI nº 3. Julio de 1992.

KIN94 An algorithm for the complete automated cryptanalysis of periodic polyalphabetic substitution ciphers. John C. King. Cryptologia Vol. XVIII nº 4. Octubre de 1994.

KIR74 Elementary number theory. Allan M. Kirch. Intext educational publishers 1974.

KNU69 The art of computer programming: Seminumerical algorithms, Vol. II. Addison-Wesley 1969.

KNU80 El arte de programar ordenadores. Algoritmos fundamentales, Vol. I. Ed. Reverté 1980.

KOB94 A course in number theory and cryptography. Neal Koblitz. Springer Verlag 1994.

KOB97 Cryptography as teaching tool. Neal Koblitz. Cryptologia Octubre de 1997.

KOB98 Algebraic aspects of cryptography. Neal Koblitz. Springer Verlag 1998.

KOC95 Timming attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. P.C.Kocher. //www.cryptography.com/timingattack.

KON81 Cryptography, a primer. A. Konheim. Wiley 1981.

KUL79 Statistical methods in cryptanalysis. Solomon Kullback. Aegean Park Press 1979.

LEN93 The factorization of the ninth Fermat number. A. K. Lenstra, H. W. Lenstra, jr., M. S. Manasse, and J. m. Pollard. Mathematics of computation, volume 61, number 203, july 1993, pages 319-349.

LON90 Geometries, codes and cryptography. G. Longo. Springer-Verlag 1990.

LOP96 Generación de números primos mediante tests de primalidad probabilistas. Javier López, Francisco Oña, Lucía Pino, Carlos Maraval. Actas de IV reunión española de criptología.

LOX90 Number theory and cryptography. J. H. Loxton, Cambridge University Press 1990.

LUB96 Pseudorandomness and cryptographic aplications. Michael Luby. Princeton University Press 1996.

LUC99 Criptografía y seguridad en computadores. Manuel José Lucena López 1999. Disponible en http://www.kriptopolis.com/criptografia.zip.

MAT82 Cryptography. A new dimension in computer security. Matyas y Meyer. John Wiley & sons 1982.

MAT93 The use of genetic algorithms in cryptanalysis. Robert A. J. Matthews. Cryptologia Vol. 17. nº 2. Abril 1993

MEL01 Cryptography decrypted. H.X. Mel y Doris Baker. Addison Wesley 2001.

MEN97 Handbook of applied cryptography. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. CRC Press 1997.

MIN99 Teoría y práctica de la seguridad informática. Jesús Mª. Minguet Melián. Actas de los X Cursos de verano de la UNED. 1999.

MOL94 Seguridad, información y poder. José María Molina Mateos. Incipit Editores 1994.

MON98 Algunos criptoanálisis particulares. Fausto Montoya Vitini. Actas del IX curso de verano de la UNED sobre Criptología. Julio de 1998.

MOR79 Password security: A case history. Robert Morris y Ken Thompson. Communications of the ACM, 22. Noviembre 1979.

MOR94 Seguridad y protección de la información. J. L. Morant- A. Ribagorda- J. Sancho. Editorial Centro de Estudios Ramón Areces 1994.

MUN97 Codificación de la Información. C. Munuera y J. Tena. Ed. Universidad de Valladolid 1997.

NIC99 ICSA guide to cryptography. R. Nichols. McGraw-Hill 1999.

NEU** Encryption, a few cryptic remarks. Bill Neugent. ACM SIGSAC Vol. 10 No.1.

OYS88 Number theory and its history. Ore Oystein. Dover 1988.

PAS98 Criptografía digital. Fundamentos y aplicaciones. José Pastor Franco y Miguel Angel Sarasa Lopez. Prensas Universitarias de Zaragoza 1998.

PAS99 Protección criptográfica. J. Pastor Franco. Actas de los X Cursos de verano de la UNED. 1999.

PAT87 Mathematical cryptology for computer scientists and mathematicians. Wayne Patterson. Rowman & Littlefield 1987.

PFL89 Security in computing. Charles P. Pfleeger. Ed. Prentice-Hall. 1989.

PIP82 Stream ciphers. Fred Piper. Proceedings de Eurocrypt 82.

PIN96 Introducción a la criptografía. Pino Caballero. Ra-Ma 1996.

POM90 Cryptology and computational number theory. Carl Pomerance, Editor. American Mathematical Society 1990.

RAM93 An automatic approach to solve simple substitution ciphers. R.S. Ramesh, G. Athithan, K. Thiruvengadam. Cryptologia Vol. XVII nº 2. Abril 1993.

RAM99 Aplicaciones criptográficas. Segunda Edición. Jorge Ramió Aguirre. Dpto. de Publicaciones de la Escuela Universitaria de Informática. Universidad Politécnica de Madrid. Junio 1999.

RIB90 The new book of prime number records. P. Ribenboim. Springer-Verlag 1996.

RIB99 Tendencias de las metodologías de seguridad. A. Ribagorda Garnacho. Actas de los X Cursos de verano de la UNED. 1999.

RIE94 Prime numbers and computer methods for factorization. Hans Riesel. Birkhäuser 1994.

RIF91 Comunicación digital. J. Rifà, Ll. Huguet. Masson 1991.

ROD86 Protección de la información. Diseño de criptosistemas informáticos. A.Rodriguez Prieto. Ed. Paraninfo 1986.

ROS96 Elementary number theory and its applications. Kenneth H. Rosen. Addison Wesley 1996.

ROS98 Implementing elliptic curve cryptography. Michael Rosing. Manning publications 1998.

RSA78 A method for obtaining digital signatures and public key cryptosystems. R. Rivest, L. Shamir, A. Adleman. Communications ACM 21-2. 1978.

RSA99 RSA crypto challenge sets new security benchmark. 1999. Disponible en http://www.rsa.com/pressbox/html/990826.html

RUB94 Comments on "Cryptanalysis of knapsack ciphers using genetic algorithms". Frank Rubin. Cryptologia Vol. XVIII nº 2 Abril 1994.

SAL96 Public-key cryptography. Arto Salomaa. Springer-verlag 1996.

SEB89 Cryptography. An introduction to computer security. J. Seberry y J. Pieprzyk. Prentice Hall 1989.

SCH93 Digital signatures. Bruce Schneier. BYTE Noviembre 1993.

SCH94 Applied cryptography. Bruce Schneier. John Wiley & Sons 1994.

SCH96 Differential and linear cryptanalysis. Bruce Schneier. Dr. Dobb's Journal. Enero 1996.

SCH98 Criptografía entre la espada y la pared. Bruce Schneier. Byte Junio 1998.

SCH99 Attack trees. Bruce Schneier. Dr. Dobb's Journal. Diciembre 1999.

SCH00 Security Research and the future. Bruce Schneier. Dr. Dobb's Journal special report. Diciembre 2000.

SHA48 A mathematical theory of communication. Bell Systems J. 1948.

SHE93 Statistical Techniques for language recognition: An introduction and guide for cryptanalysts. Ravi Ganesan, Alan T. Sherman. Cryptologia Vol. XVIII, nº 4. Octubre 1994.

SHR94 Number theory in science and communication. 2ª edición. Manfred R. Schroeder. Springer-Verlag 1994.

SIM83 The prisoner's problem and the subliminal channel. Proceedings of Crypto83. Plenum Press 1984.

SIM94 Contemporary cryptology. G. J. Simmons. IEEE Press 1994.

SIN66 Elementary cryptanalysis. Abraham Sinkov. Mathematical Association of America 1966.

SIN00 Los códigos secretos. Simon Singh. Editorial Debate 2000.

SMI97 Internet cryptography. Richard E. Smith. Addison-Wesley 1997-

SOL16 Mensajes secretos. La historia de la criptografía española desde sus inicios hasta los años 50. José Ramón Soler Fuensanta y Francisco Javier López-Brea Espiau. Ed. Tirant lo Blabnch 2016.

SOR99 Generación y análisis de secuencias pseudoaleatorias. Miguel Soriano, Raúl Gonzalo. Edicions UPC 1999.

SPI93 Use of a genetic algorithm in the cryptanalaysis of simple substitution ciphers. Spillman, Janssen, Nelson, Kepner. Cryptologia vol. XVII, nº 1. Enero 1993.

SPI93b Cryptanalysis of knapsack ciphers using genetic algorithms. Richard Spillman. Cryptologia Vol. XVII nº 4 Octubre 1993.

STA95 El modelo de confianza PGP: una tela de araña. William Stallings.BYTE No. 5 . Marzo 1995.

STA98 Cryptography and network security. Principles and practice. William Stallings. Prentice Hall 1998.

STA99 The HMAC algorithm. William Stallings. Dr. Dobb´s nº 298. Abril de 1999.

STI95 Cryptography. Douglas R. Stinson. CRC Press 1995.

TEN98 Criptosistemas simétricos. Juan Tena Ayuso. Actas de los IX Cursos de verano de la UNED. 1998.

TEN99 Fundamentos teóricos. Juan Tena Ayuso. Actas de los X Cursos de verano de la UNED. 1999.

VIN77 Fundamentos de la teoría de los números. I. Viongradov. Ed. Mir 1977.

WAY93 ¿Deben reglamentarse los métodos de cifrado?. Peter Wayner. BYNARY 53. Julio/Agosto 1993.

WAY96 Los vándalos de la información. Peter Wayner. BYTE No. 14. Enero 1996.

WAY96b Disappearing cryptography. Peter Wayner. Academic Press 1996.

WIE93 Efficient DES key search. Michael J. Wiener. Advances in cryptology:Proceedings of CRYPTO ‘92.Springer-Verlag 1993.

WIL74 Non-secret encryption using a finite field. M. Williamson 1974. http://www.cesg.gov.uk/about/nsecret/home.htm.