Published Sources on CRYPTOLOGY (2004)

compiled by B. Lippmann, FOGE Berlin

Abadi, M. und Feigenbaum, J.
Secure Circuit Evaluation. J. Cryptology 2 (1990), 1-12.

Abadi, M. und Feigenbaum, J. und Kilian, J.
On Hiding Information from an Oracle
JCSS 39 (1989), 21-50

Abromeit
Codes.
Informationstheorie
BSV

Aho und Hopcroft und Ullman
The Design and Analysis of Computer Algorithms
Addison Wesley 1974

Amt für Fernmeldewesen der Bundeswehr
AFmBw, Abt. I/3, Mathematische Grundlagen für die Entzifferung

Anderson, R.
A serious weakness of DES (2.11.96),

Anderson, R., Kuhn, M.
Tamper Resistance- A Cautionary Note.

Anderson, R.
ATM Security- Why Cryptosystems fail

Arazi
A Commonsense Approach to the Theory of Error Correcting Codes
MIT Press 1988

Babai, L.
Trading Group Theory for Randomness.
Proc. 17 STOC 1985, 421-429

Babai, L., L. Fortnow und C. Lund
Nondeterministic Exponential Time ... Proc. 31 FOCS 1990, 16-25

Bacard, Andre
Non- Technical PGP FAQ

Computer Privacy, Handbook

Balcazar, J.L., J. Diaz und J. Gabarro
Structual Complexity I. Springer Verlag 1988

Bamford, James
NSA Amerikas geheimster Nachrichtendienst.
Abner, S. 132 ff.) Zahl der Hemden, S. 469 f)
deutsche Ausgabe:Zürich und Wiesbaden 1986

Bamford, James, W. Madsen
The Puzzle Palace. Penguin Books 1995
(Geschichte der NSA)

Bamford, James
The Puzzle Palace. Houghton Mifflin 1982

Barlow, Mike
CRYPTO (Code- Knack- Paket) in: SdW, Dez.88, S.11

Bartholome, A. Rung, J., Kern, H.
Zahlentheorie für Einsteiger. Verlag Vieweg 1995

Bauer, Friedrich L., Goos
Inforamtik Bd. II, Kryptologie, S. 295ff.)

Bauer, Friedrich L.
Klassische Kryptologie- Verfahren und Maximen- in: Informatik Spektrum
Heidelberg, S. 5-82, S. 74-81

Bauer, Friedrich L.
Decrypted secrets. Methods and Maximes of Cryptology.
Berlin 1997

Bauer, Friedrich L.
Kryptologie. Springer Verlag Heidelberg 1993, 1997

Bauer, Friedrich L.
Entzifferte Geheimnisse- Methoden und Maximen der Kryptologie.
Berlin 1995 (leicht überarbeitete Fassung von "Kryptologie"
Decrypted Secrets (Springer 1997)

Baumann, Rüdeger
Datenkompression nach Huffman.
in: LOGIN 14(1994) H. 5/6, S. 58-62

Baumann, Rüdeger
Didaktik der Informatik. Klett Stuttgart 1996

Baumann, Rüdeger
Digitales Geld- Bestellen und Bezahlen im Internet.
In: LOG In 17 (1997) H2, S. 30-38

Becker, K.-Cl. , Albrecht Beutelspacher
Hinter Schloß und Riegel? Kryptologie oder: Wie schütze ich meine Daten. mc, Mai 1994 p.88-95

Beesley, Patrick
Very Special Intelligence. Geheimdienstkrieg der britischen Admiralität 1939-1945
Ullstein Berlin 1979

Beiler, Albert H.
Recreations in the Theory of Numbers.
Dover Publications New York 1988

Beker, H. und F. Piper
Cipher Systems. The Protection of Communication. Northwood, London 1982

Beker, H., F. Piper
Cryptography and Coding. Clarendon Press. Oxford 1989

Beker, H., F. Piper
Secure Speech Communications
Academic Press 1985

Ben-or, M., O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali und P. Rogaway
Everything Probable is Provable in Zero-Knowledge. CRYPTO 88, Springer LNCS 403, 37-56

Benaloh, J. C., M. de Mare
One- Way Accumulators: A Decentralized Alternative to Digital Signatures, in: EUROCRYPT 93
Proceedings, S. 274-285
Springer- Verlag 1994

Bennet, C.H., Brassard, G. und Ekert, A.K. (BBE)
Quanten-Kryptographie. SdW Dezember 1992, S. 96-104
Quantum Cryptography. Scientific American Bd. 267(1992), H. 4

Bennet, C.H. und G. Brassard
An Update on Quantum Cryptography. CRYPTO 84, Springer LNCS 196 (1985)

Bennett, William Jr.
Scientific and Engineering Problem- Solving with the Computer
Prentice Hall 1976

Berendt, G.
Elemente der Kryptologie. In: R.-H. Schulz (Hg.): Mathematische Aspekte der Angewandten Informatik,
BI Verlag Mannheim 1994,
S. 128-146

Bertrand, G.
ENIGMA ou la plus grande Enigme de la Guerre 1939-1945
Librairie, Paris 1973

Beth, Thomas
Kryptographie als Instrument des Datenschutzes; in: Informatik Spektrum, Heidelberg, S. 5-82, S. 81-96

Beth, Thomas, Peter Heß, Klaus Wirl
Kryptographie; in: Leitfaden der angewandten Informatik; Teubner-Vlg., Stuttgart 1983
Materialien zur Kryptographie. Universität Erlangen 1982

Beutelspacher, Albrecht und Jörg Schwenk.
Was ist Zero-Knowledge? Mathematische Semesterberichte 40(1993)

Beutelspacher, Albrecht
Kryptologie. Vieweg Verlag 1994. 4. Auflage

Beutelspacher, Albrecht und Jörg Schwenk
Was ist ein Beweis? Überblicke Mathematik 1996 Vieweg Verlag Wiesbaden 1996

Beutelspacher, Albrecht, Jörg Schwenk, Klaus-Dieter Wolfenstetter
Moderne Verfahren der Kryptographie. Vieweg 1995

Beutelspacher, Albrecht
Kryptographie- Eine Einführung in die Wissenschaft von der Geheimhaltung der Daten. In Der
Mathematikunterricht (MU) 33(1987) H.3., S. 4-14

Beutelspacher, Albrecht
Hilfreiche Dämonen- oder: Wie schütze ich meine Daten vor Veränderung? In: Der
Mathematikunterricht (MU) 33(1987), H. 3, S. 16-21

Beutelspacher, Albrecht
Geheimsprache und Geheimzeichen. Mathe Welt in: Mathematik lehren
E. Friedrich- Vlg. 1995

Beutelspacher, Albrecht

Chiffrieren und Codieren. In: Der Mathematikunterricht (MU) 3/1987, S. 4-14

Bickenbach, J. (Hsg.)
Schriftenreihe Wissenschaft und Frieden. Militarisierte Informatik. Das Projekt in Bletchley Park. S. 12
ff.) Juni 1985

Biernoth, H.
Der RSA- Algorithmus. Eine Einführung in die moderne Kryyptographie.
Staatsexamensarbeit
Universität Giessen 1992 (unveröffentlicht)

Biham, E., A. Biryukov
How to Stregthen DES Using Existing Hardware, in: Advances in Cryptology-ASIACRYPT 94 Proceedings
Springer Verlag 1995

Biham, E, A. Shamir
Differential Cryptoanalysis of DES-like Cryptosystems, in: Advances in Cryptology-CRYPTO 90
Proceedings, Springer Verlag 1991, p. 2-21

Biham, E., P.C. Kocher
A Known Plaintext Attack on the OKZIP Stream Cipher, K.U. Leuven Workshop on Cryptographic
Algorithms, Springer Verlag 1995

Blahut
Theory and Practice of Error Control Codes
Addison Wesley 1983

Blakley, G.R., G.A. Kabatianski
On General Perfect Secret Sharing Schemes, in: Advanced in Cryptology-CRYPTO 95, Springer Verlag
1995

Blaze, M.
Protocol Failure in the Escrowed Encryption Standard.

Blaze, M.
A Cryptographic File System for UNIX.

Blum, M., S. Goldwasser
An Efficient Probabilistic Public- Key Encryption Scheme Which Hides All Partial Information. Advances
in Cryptology: Proceedings of CRYPTO 84, Springer Verlag 1985,S. 289-299

Bonatz, Heinz

Die deutsche Marine- Funkaufklärung 1914-1945.
Wehr und Wissen Verlagsgesellschaft, Darmstadt 1970

Boyd, Carl
Old Dominion University Norfolk, Virginia
The Role of cryptologic intelligence in the poacific war 1941-1943 in: The Enigma Bulletin, May 1998,
p. 5ff.)

Brandstädt, Andreas
Geheime Nachrichten und Verschlüsselung.
in: Wurzel 1(1992), S. 23ff.)

Brassard, G.
Modern Cryptology. Springer LNCS 325
Lecture Notes in Computer Science, 1988

Brennecke, Ralph
Mit Passwort und Codeschlüssel.
Das Parlament 26.4. 1986

Bressoud, D.M.
Factorization and Primality Testing
Springer New York 1989

Brickell, E., D. Denning u.a.
SKPIJACK Review: Interim Report.

Brown, Anthony Cave
Bodygard of Lies. New York 1975
deutsch: Die unsichtbare Front. München 1976

Buchheit, Gert
Die anonyme Macht. Die Kryptologie, S. 219ff.)
Frankfurt/M. 1969

Burke, Colin
Information and Secrecy. Vannevar Bush, Ultra and the other Memex. London 1994

Burrows, M. und M. Abadi und R.M. Needham
A Logik of Authentification. Rep. 39, Digital Eqquipment Corporation Systems Research Center, Palo
Alto, Calif., Febr. 1998

Burrows, M. und M. Abadi und R.M. Neddham
A Logic of Authentification. ACM Transactions on Computer Systems Vol. 8 Nr. 1

(1990) 18-36

Calvocoressi, Peter
Top Secret Ultra.
Sphere Books Ltd., London 1980

Cameron, Alistair GW
Interstellar Communication, W.A. Benjamin 1963

Carroll, John M.
Secrets of Electronic Espionage. New York 1966
deutsch: Der elektronische Krieg. Berlin, Wien 1967

Chaum, D.
The Dining Cryptographers Problem: Unconditional Sender and Receiver Untraceability
J. Cryptology Vol 1 Nr. 1 (1988)

Chaum, D., A. Fiat, M. Naor
Untraceable Electronic Cash. in: Advanced in Cryptology- CRYPTO 88 Proceedings, Springer Verlag
1990

Chaum, David
Advances in Cryptology: Proceedings of Crypto 83.
Plenum Press New York 1984

Chor, B. und R. Rivest
A Knapsack-Type Public Key Cryptosystem Based on Arithmetic in Finite Fields.
IDEEE Transactions on Information Theory, 45
(1988), p. 901-909

Ciarcia, S.
Build a Hardware Data Encryptor
Byte. Sept. 97-111

Clark und Cain
Error-Correction Coding for Digital Communications
Plenum Press 1981

Crutchfield, J.P., J.D. Farmer, N.H. Packard, R.S. Shaw
Chaos. Scientific American Bd. 255 (1986) H.6., S. 38-49

D`Agapeyeff, Alexander
Codes and Ciphers. Oxford University Press 1932, London 1939

Daeman, J.
Cipher and Hash Function Design

Ph.D. Dissertation, Katholieke Universiteit Leuven, März 95

Davies, D.W., W.L. Price
Security for Computer Networks, John Wiley & Sons, 1984

Dawies, D.W.
The Lorenz Cipher Machine SZ 42. Cryptologia, Jan 95, XIX,
p. 39-61

Dea, Edward J.
Mac Arthur`s ULTRA Codebreaking and the War against Japan 1942-1945.
University Press of Kansas
1992

Deavours, Ciph A., Kahn, Kruh, Mellen, Winkel
Cryptology Yesterday, Today, and Tomorrow
Artech House 1987

Denning, Dorothy Elizabeth Robling
Kryptography and Data Security. Addison- Wesley, Reading 1983
(Vorläufer von Schneier)

Dewdney, A.K.
Die Geschichte der legendären ENIGMA (I)
Spektrum der Wissenschaft Dez. 1988, S. 8ff.
vorhanden, Artikel in 1) SdW und 2) Krypto II
Auf den Spuren der ENIGMA

Dewey, G.
Relative frequency of english speech sounds. Harvard Univ. Press, Cambridge
1923

Diffie, W.
The first ten years of Public Key Cryptography.
In: Contemporary Cryptology: The Science of Information Integrity,
G.J. Simmons, ed., IEEE Press 1992, p. 65-134

Diffie, W. und M.E. Hellman
New Directions in Cryptography. IEEE Transactions on Information Thery, 6
November 1976, 644-654

Diffie, W. und M.E. Hellman
Privacy and Authentification. Proc. of the IEEE 67/3 Mrz 79

Dittes, Axel
Testballon geplatzt- Chaos Computer- Club knackt Verschlüsselung von Software-
CD

c't- Magazin Mai 1994, S. 18

Dobbertin, H.
Welche Hash- Funktionen sind für digitale Signaturen geeignet?
In: Digitale Signaturen, P. Horster (Hrsg.) Vieweg Verlag, 1996.

Dobbertin, H.
Cryptoanalysis of MD4
Proceedings of the 3rd Workshop on Fast Software Encryption Cambridge,
Springer- Verlag 1996
(Lect.Not.Comp.SCi. Bd. 1039) p. 53-70

Donnerhacke, L., S. Peter
Vorsicht, Falle! ActiveX als Füllhorn für Langfinger,
iX 3/1997, S. 90-93

Duelli, H., P. Pernsteiner
Alles über Mobilfunk: Dienste- Anwendungen- Kosten- Nutzen, Franzis-Verlag
München 1992

Ebon, Martin
KGB- Death and Rebirth
ch.11: Whose Codes? Whose Ciphers?
USA 1994

Elcrotel
Schlüsselgerät "Elcrotel"

ElGamal, T.
A Public Key Cryptosystem and a Signature Scheme based on Diskrete
Logarithms. IEEE Trans. on
Information Theory, Vol. IT-31 (1985), 469-472

Enever, Ted
Britains`Best Kept Secret
Alan Sutton Publishing Ltd. 1994

Engel, Arthur
Datenschutz durch Chiffrieren: Mathematische und algorithmische Aspekte; in:
MU 6/79, S. 30-51

ENIGMA
Zur alliierten Funkaufklärung im Zweiten Weltkrieg.
Alte Kameraden 4(1979), Artikel von "w.h.

ENIGMA
Manchmal stotterte das Orakel. Wie der britische Geheimdienst die Funkschlüssel
der Wehrmacht

knackte.
Der Spiegel Nr. 47/1978, S. 121ff.)

Erskine, Ralph
When a purple machine went missing. How Japan nearly Discovered America`s Greatest Secret
Intelligence and National Security 12.3 (1997), p. 185-189

Erskine, Ralph
Typex and the Admirality. Intelligence in the 20th. Century.
Tagungspapier AGN Hamburg 1996

Erskine, Ralph
Cryptologic History Symposium. NSA 29-31 Oct. 1997
Newsletter Winter 1997, p. 1ff)

Erskine, Ralph
Naval Enigma. An Astonishing Blunder.
Intelligence and National Security, July 1996

Farago, Ladislas
The Broken Seal. Operation Magic and the Secret Road to Pearl Harbor.
Random House New York 1967
deutsche Ausgabe:
Codebrecher am Werk.
Berlin 1967

Farago, Ladislas
Das Spiel der Füchse.
Ullstein Berlin 1972

Feigenbaum, J.
Overview of Interactive Proof Systems and Zero Knowledge. In: Contemporary Cryptology: The Science
of Information Integrity, G. J. Simmons, ed. IEEE Press 1992, 423-439

Feistel, H.
Cryptography and Computer Privacy, Scientific American Bd. 228 (1973) H.5, S. 15-23

Figl, Andreas
Systeme des Chiffrierens. Graz 1926

Fischer, Peter
Die Rätsel- Maschine. Wie die Alliierten im Zweiten Weltkrieg die deutschen Geheimcodes knackten.
Frankfurter Rundschau, 3.5. 1975

Flicke, Wilhelm F.
Agenten funken nach Moskau, München 1954.

Flicke, Wilhelm F.
Spionagegruppe Rote Kapelle, Kreuzlingen 1954

Foote, Alexander
Handbuch für Spione. Anhang: Mein im Verkehr mit Moskau gebrauchter Funkschlüssel. S. 224ff.)
Darmstadt 1954

Foote, Alexander
Lucy contra OKH. Aus dem Kriegstagebuch eines Sowjet-Spions.
in: Der Spiegel (Serie) 24.2. 1954 (9/54), S. 25ff.

Fowler, M., Radhi Parekh
Codes and Diphers. Educ. Development Corp. 10302 E, 55th Place. OK 74146-6515 USA 1995

Fox, Dirk
Schlüsseldienst- Private Kommunikation mit PEM und PGP
Computer und Technik, Heise Verlag 9/95

Franke, Herbert W.
Die geheime Nachricht.
Umschau- Verlag Frankfurt/Main 1982

Frankel, Y., M. Yung
Escrow Encryption System Visited: Attacks, Analysis and Designs, in: Advances in Cryptology- CRYPTO
95, Springer Verlag 1995, S. 222-235

Franksen, O.I.
Mr. Babbage`s Secret. The Tale of a Cipher and APL. Prentice Hall, Englwood Cliffs 1985

Fricker, Francois
Neue Rekord- Faktorisierung. Spektrum der Wissenschaft,
Nov 90, 38-41

Friedman, William F.
Cryptology, Artikel in "Encyclopaedia Britannica. 1970

Friedman, William F.
Elements of Cryptoanalysis. Washington 1924
Aegean Park Press, Laguna Hills, 1976

Fumy, Walter, Hans Peter Rieß

Kryptographie. Oldenburg Verlag 2. Aufl. München 1994

Furrer, F.J.
Fehlerkorrigierende Block- Codierung für die Datenübertragung. Birkhäuser Verlag, Basel etc. 1981

Gaines, Helen Fouche`
Elementary Cryptoanalysis. Boston 1939, Boston 1944, Dover 1956
auch: Cryptoanalysis

Galland, Joseph S.
An Historical and Analytical Bibliography of the Literature of Cryptology. Evanston 1945

Gallwitz (Fall)
Entführungsfall Nina von Gallwitz
Code- Satz- Beispiel
in: Spiegel 21(1982), S. 112)

Gardner, Martin
Extraterrestrial Communication. Scientific American. 1971

Gardner, Martin
A New Kind of Cipher That Would Take Millions of Years to Break. Scientific American Bd. 237 (1977)
H. 8, S. 120-124

Gardner, Martin
Das verhexte Alphabet- Tips und Tricks für Geheimschriften.
Ullstein 1981

Garfinkel, Simson
PGP. Pretty Good Privacy
Verschlüsselung von Email.

Geffe, P.
How to protect data with ciphers that are really hard to break
Electronics, 99-101

Giessmann, E.G.
Sichere Verschlüsselungen- geht das überhaupt. Alpha 6/1995
(Teil I), Alpha 7/1995 (Teil II)

Gilbert, James L., John P. Finnegan
U.S. Army Signals Intelligence in World War II
Center of Military History, Washington 1993

Goldwasser, Shafi, Mihir Bellare

Lecture notes on Cryptography

Gollmann, D.
Algorithmenentwurf in der Kryptographie. BI Mannheim 1994

Golomb
Shift Register Sequences
Aegean Park Press 1982

Grabau, Rudolf
Die Fernmeldetruppe EloKa des Heeres 1956 bis 1990.
Fernmeldering e.V. Bonn 1995

Grabau, Rudolf
Funküberwachung und Elektronische Kampfführung.
Stuttgart 1986

Greefkes, J.A. und K. Riemens
Codemodulation mit digital gesteuerte Kompandierung für Sprachübertragung. In: Philips Technische
Rundschau 11/12 1970/1971

Groehler, Olaf
Das Super- Geheimnis. Entschlüssleter Funkcode der Faschisten.
Sport und Technik 12(1979), S. 12f.

Gröndahl, B.
Die Entdeckung der Public-Key-Kryptographie- Ehre wem Ehre gebührt. In: Internet

GUEVARA
Der Geheimcode des Che Guevara.
Spektrum der Wissenschaft, Dez. 1992, S. 98

Hamming, R.
Coding and Information Theory
Prentice-Hall 1980

Hamming, R.
Information und Codierung
VCH Weinheim 1987

Harris, R.
Enigma. Heyne Verlag München (7. Aufl.) 1995

Hastad, J.
On Using RSA with Low Exponent in a Public Key Network, in: Advances in Cryptology- CRYPTO 85

Proceedings, Springer- Verlag 1986, S. 403-408

Hauthal, Horst
Beitrag zur Geschichte des Chiffrierwesens im Auswärtigen Amt 1939-1945, Bonn 1985
Newsletter, Winter 1997, S. 5

Heibey, H.W.,Pfitzmann, A und Sandl, U
Kryptographie- Herausforderung für Staat und Gesellschaft.
In : LOG IN 16(1996) H. 5/6 S. 37-43

Heider, F.P.,D. Kraus, M. Welschenbach
Mathematische Methoden der Kryptoanalyse, in DuD- Fachbeiträge, Bd. 8, Vieweg-Vlg. Braunschweig
1985

Heinrich, Alf
ENIGMA- das gelöste Rätsel
kurzwelle hören, Nov. 1989, S. 46-51

Hellmann, Martin E.
A Cryptoanalytic Time- Memory Trade Off,
IEEE Transactions on Information Theory, Bd. 26 H4 (1980),
p. 401-406

Hellmann, Martin E.
Die Mathematik neuer Verschlüsselungssysteme.
Spektrum der Wissenschaft Heft 10 (1979), S. 92-101
The mathematicsof public key cryptography.
Scientific american (August 1979)

Henze,E., H.H. Homuth
Einführung in die Codierungstheorie. Vieweg Braunschweig 1974, Kap. 3

Hermann, Th., W. Poguntke
Fehlerkorriegierende Codes in der Cryptologie. Math. Semesterb. 42(1995), S. 139-151

Hermans, Arnold
Verschlüsselung und Entschlüsselung von Nachrichten. PM 31(1989), Nr. 5, S. 262-270

Herzog, Heinrich
Verschlüsselung von Texten und Disketten. in: LOGIN H.3(1988)

Hess, Sigurd
Venona und die Folgen - der angelsächsische Einbruch in einen sowjetischen Schlüssel während des Kalten Krieges, in: Hartmut Klüver/Thomas Weis (ed.),

Marinegeschichte - Seekrieg - Funkaufklärung, Beiträge zur Schiffahrtsgeschichte vol. 10, Deutsche Gesellschaft für Schiffahrts- und Marinegeschichte e.V., Düsseldorf 2004.

Hinsley, F. H., Alan Stripp
Code Breakers- the inside Story of Bletchley Park
Oxford University Press 1993

Hochhuth, Rolf
Alan Turing. Rowohlt 1987

Hodges, A.
Alan Turing: Enigma. Springer Verlag 1994

Höhne, Heinz
Kennwort: Direktor. Frankfurt 1970

Hölterling, Victor
Leserbrief zu "Schlüssel M"
Die Welt, 16.6. 1986

Hoffmann, L.J.
Building in Big Brother- The Cryptographic Policy Debate,
Springer Verlag 1995

Horak, H.
Der bunte Zoo der Kryptologie. Mathe-plus (Feb. 1987) 3/3

Horchem, HJ
Die lautlose Macht. Bd. 1, 1985
BfV vs. MfS (Guillaume) S. 138
Geheime Daten, Chiffren und Computer, S. 279
Geheimschriften, S. 281
Funk- und Codiergeräte. S. 307

Horster, P., Michels, V., Petersen, H.
Das Meta-ElGamal- Signaturverfahren und seine Anwendungen. Vieweg Verlag Wiesbaden 1995

Horster, Patrick
Kryptologie: in Reihe Informatik, Bd. 47, Bibliographisches Institut, Mannheim 1985
BI- Verlag

Jackson, Keith M.
Secure Information Transfer- PC Encryption
Blackwell, Oxford 1990

Jäger, Ulrich
Geheimschrift.
PM, 1(1981), S. 32ff.)

JEGLORZ
Fall Horst Jeglorz
"Der DDR- Code ist nicht zu knacken"
Der Spiegel 41(1973)

Johnson, Brian
Streng Geheim.
Motorbuch Verlag Stuttgart.
The Secret War. BBC London 1978

Jones, R.V.
Most Secret War
Coronet Books, 1978

Jungnickel, D.
Graphen, Netzwerke und Algorithmen. BI Wissenschaftsverlag. 2. Auflage 1990

Kaderali, Firoz
Kryptologie: Technischer Datenschutz in Kommunikationsnetzen.
Addison- Wesley Bonn 1997 (mit CD)

Kaeding, Friedrich Wilhelm
Häufigkeitsöwrterbuch der deutschen Sprache. 1898

Kahn, David
The Codebreakers- The Story of Secret Writing. 1. Auflage McMillan, New York 1967, 2. Auflage
Scribner New York 1996

Kahn, David
Cryptology. Artikel in The Cencyclopedia Britannica.

Kahn, David
Seizing the Enigma. The Race to Break the German U Boat Codes 1939-1945.
Boston 1991

Kahn, David
Modern cryptology. Scientific American. Vol. 215 July 1966
in: Amt für Fernmeldewesen der Bundeswehr
Technisches Informationsblatt. 4/1967

Kahn, David
Interview in: DAMALS 9(1995), S. 20, 21

Kahn, David
Kryptologie
Playboy Dez. 1975

Kaliski, B.S.Y., L. Yin
On Differential and Linear Cryptoanalysis of the RC5 Encryption Algorithm.
Springer Verlag 1995, S.
171-184

Kameda, T., K. Weihrauch
Einführung in die Codierungstheorie I, BI Zürich 1973

Kardel, F.
Die Falltürfunktion als mathematische Grundlage für eine Codierung und Decodierung auf dem
Kleincomputer. In: LOG IN 4/1984 Teil 1: H.1, S. 56-62, Teil 2: H2 S. 61-62, Teil 3: H3, S. 62-64

Kasiski, Friedrich W.
Die Geheimschriften und die Dechiffrierkunst.

Kaufman, Perlman, Speciner
Network Security
Prentice Hall 1995

Kemmerer, R., C. Meadows und J. Millen
Three Systems for Cryptographic Protocol Analysis. J. Cryptology Vol. 7 Nr. 2 (1994), 79-130

Kennedy, William V.
The intelligence war, London 1983

Kilian, J.
Uses of Randomness in Algorithms and Protocols. MIT Press. Cambridge (Mass.) 1990

Kilian, J., P. Rogaway
How to protect DES against exhaustive key search, in Advances in Cryptology-Crypto 96, Springer
Verlag 1996

Kippenhahn, Rudolf
Verschlüsselte Botschaften. Rowohlt Hamburg 1997

Kirchhofer, Kirk H.
Kryptologie Teil 1 In: Internationale Wehr- Revue Genf Nr. 2, 1976, S. 281ff., Teil 2 Nr. 3/76, S. 389ff.,

Teil 3 Nr. 4/1976, S. 585ff.

Kleiner, Hans-J.
Das RSA- Verfahren, in: PM 26, 5/84, S. 133-140
Praxis der Mathematik

Knightley, Phillip
Profis und Code-Knacker in Friedenszeiten, S. 77ff.)
Achtung: Feind hört mit (Ultra/Blechtley), S. 151ff.)
Die Spionage im 2o. Jahrhundert. Ullstein 1992

Knudsen, L.R., W. Meier
Improved Differential Attacks von RC5, in: Advances in Cryptology-CRYPTO 96, Springer Verlag 1996

Knuth, D.
The Art of Computer Programming. Addison Wesley 1981

Koblitz, Neal
A course in Number Theory and Cryptography. Springer Verlag New York, Berlin 1987

Kochanski, Martin
A survey of data insecurity packages. Cryptologia. Volume XI Number 1, January 1987

Kocher, P.
Fault-induced crypto attacks and the RISKS of press releases,

Kocher, P.C.
Cryptoanalysis of Diffie - Hellmann, RSA, DSS, and other Systems Using Timing Attacks, siehe
/1164,349/

Koerber, B. und I. Peters
Von der ITG zum Informatikunterricht- Beispiel einer spiralcurricularen Planung und Durchführung
größerer Unterrichtsvorhaben. In: LOGIN 14 (1994), H. 1, S. 11-15

Koestler, Arthur
Die Geheimschrift.

Konnheim, Alan G.
Cryptography. A Primer. John Wiley New York 1981

Korner, T.W.
The Pleasures of Counting
Cambridge 1996

Kozaczuk, Wladyslaw
Im Banne der Enigma.
Militärverlag der DDR, Berlin (Ost) 1987

Kozaczuk, Wladyslaw
Geheimoperation Wicher.
Bernhard & Graefe Verlag, Koblenz 1989

Kramish, Arnold
Der Greif. Der Code der Codes, S. 289ff.
Kindler München 1987

Kranakis, Evangelos
Primality and Cryptography. Teubner Stuttgart 1986.

Krauch, Helmut
Erfassungsschutz. Der Bürger in der Datenbank: zwischen Planung und Manipulation. Stuttgart 1975

Krebs, Gerhard
Die Funkentschlüsselung im Pazifik im Zweiten Weltkrieg
Vortrag AGN Hamburg Mai 1996

Künzell, S.
Binnendifferenzierung im Informatikunterricht.
In: LOG IN 18(1998) H 1 u.a.

Kuhn, M.
Der Cäsar- und der Vigenere- Code. Ein Einstieg in einer Unterrichtsreihe "Kryptographie" unter
Verwendung von PASCAL. Computer und Unterricht 18/1995, S. 55-57 Friedrich-Vlg. Seelze 1995

Kuhn, M.
Moderne Kryptographie. Hintergründe und Auswirkungen aktueller Chiffrierverfahren- nicht nur für
den Informatikunterricht. Computer und Unterricht 18/1995, S. 41-43

Kullback, Solomon
Statistical Methods in Cryptoanalysis (1938)
Laguna Hills Aegean Park Press 1976

Kunze, M.
Netz- Razzia
c`t 7/95, S. 22

Kuppinger, M., J. Resch
Ist sicher auch sicher genug?

UNIX Open 11/96, S. 68-72

Laffin, John
Codes and Ciphers. Abelard- Schumann 1964

Lai, X, J.L. Massey, S. Murphy
Markov ciphers and differential cryptoanalysis.
in Advances in Cryptology- Eurocrypt 91, Springer Verlag 1991, S. 17-38

Lamport, L.
Password Authentification with Insecure Communication,
Comm. ACM 24(1981) H.11, S. 770-772

Landmann, Salcia
Mattenenglisch, Leserbrief zu "Schwyzerdütsch nicht abhörbar?"
Die Welt 11. 5. 1982

Langie, Andre`
Cryptography. Constable London 1922

Leiberich, Otto
Kryptologie als geschichts- und geisteswissenschaftliches Phänomen.
Tagungsbeitrag AGN Hamburg
Mai 1996

Lenstra, A.K. , HJJ.W. Lenstra
The Development of the Number Field Sieve,
Lecture Notes in Mathematics 1554, Springer Verlag 1993

Levy, Steven
Bericht vom Kryptokrieg.
in Die Zeit, 30. 12. 1994

Lewin, Ronald
Entschied ULTRA den Krieg? Verlag Wehr und Wissen
Koblenz und Bonn 1981

Lindner, R., B. Wohak, H. Zeltwanger
Planen, Entscheiden, Herrschen
Vom Rechnen zur Elektronischen Datenverarbeitung. Rowohlt Reinbek
Taschenbuch Vlg. 1984, Bd.
7715

Lidl, R., Pilz, P.
Angewandte abstrakte Algebra II, S. 96-111, Bibliographisches Institut Mannheim
1982.

Lin und Costello

Error Control Coding
Prentice Hall 1983

van Lint, J.H.
Public Key Cryptography; in: Nieuw Archief voor Wiskunde (4), Vol. 1 (1983), S. 259-269

van Lint, J.
Introdukiton to Coding Theory
Springer 1982

Lorz, Stephan
Kryptographie macht die Computernetze sicherer.
Rheinischer Merkur, 22. 12. 1995

Luckhardt, N., H. Bögeholz
Schlüsselerlebnisse, PGP- Frontends, c`t 1/96, S. 132-138

Lysing, Henry
Secret Writing. David Kemp New York 1936

Mansfield, Louis C.S.
The Solution of Codes and Ciphers. London 1936

Massey, J. L.
Was ist ein Bit Information?
Freqquenz 37 (1987), 5, S.110-115

McEliece, A.
Public-Key Cryptosystem based on Algebraic Coding Theory. DSN Progress Report, 42-44 (1978), 114-
116

Meier, Helmut
Deutsche Sprachstatistik. Hildesheim 1967

Menezes, Alfred J., Paul C. van Oorschot, Scott A. Vanstone
The Handbook of Applied Cryptography. CRC Press 1996

Meulen, Michael van der
The Book Cipher System of the Wehrmacht.
Cryptologia XIX Number 3 July 1995 pp. 247-260

Meulen, Michael van der
Le Radiogramme de la Victoire
Intelligence History Study Group, Tutzing April 1998

Meulen, Michael van der
Cryptology in the early Bundesrepublik.

Cryptoloogia XX, Juli 1996

Meyer, Carl H., Stephen M. Matyas
Cryptography: A New Dimension in Computer Data Security
John Wiley & Sons 1982

Meyer, Carl H., Stephen M. Matyas
Cryptography: A Guide for the Design and Implementation of Secure Systems.
John Wiley & Sons New
York 1982

Mild, Oskar
Der programmierbare Taschenrechner als Chiffriergerät
in: CHIP, Januar 1982 S. 39ff.

Miller, A.R.
The cryptographic mathematics of Enigma. Cryptologia Jan 1995 XIX/1, S. 66-80

Millikin, Donald D.
Elementary Cryptography and Cryptoanalysis. New York University Bookstore
1943

Montgomery, Hyde H.
Cynthia. The spy who changed the course of the war. Any Elisabeth Pack,
London 1966
deutsche Ausgabe:
Cynthia. Geliebte und Geheimagentin. Meisterspionin im 2. Weltkrieg, Velbert
1966
auch:
Cynthia. Bond in Blond, in: Der Spiegel 1966, H. 23, S. 102 ff.)

Moore, Dan Tyler, Martha Waller
Cloak and Cipher. Bobbs-Merrill 1962

Morgan, B.Q.
German Frequency Word Cook. 1929 (Bearbeitung des Kaeding- Buches)

Murbach, Georges
Geheimschrift knacken.
backup Mai 1987, S. 44f.)

Murphy, Brian
Das Geschäft der Spione. Moewig- Verlag

Murphy, S.
The Cryptoanalysis of FEAL-4 with 20 Chosen Plaintexts
Journal of Cryptology Bd. 2 (1990) H.3, S. 145-154

Nampil, C.
Vortrag Kryptographie, Stichwortsammlung
Forum Berlin, Juli 1985

Newman, Bernard
Spionage.
Wäsche- Stickereien, S. 105)

Nickels, Hamilton
Codemaster- Secrets of Making and Breaking Codes.
Paladin Press Boulder, Colorado 1990

Nicolas, J. L.
Tests de primalite, in: Expositiones Mathematicae, 2/1984, S. 223-234,
Bibliographisches Institut
Mannheim.

Niederdrenk- Felgner, Cornelia
Algorithmen der elementaren Zahlentheorie, CMI Institut für Fernstudien (DIFF),
Universität Tübingen
1988
Programmdiskette zu CM 1 bis CM 3 Nr. 01262

Niederdrenk, K.
Die endliche Fourier- und Walsh-Transformation mit einer Einführung in die
Bildverarbeitung.
Vieweg, Braunschweig 1984

Nollau, Günther, Ludwig Zindel
Gestapo ruft Moskau
München 1979

Nyberg, Sture
Chiffrierung. In. Neue Zürcher Zeitung , 12.12. 1973

Oberschelp, W.
Algorithmen und Computer im Unterricht. Kurseinheit 1-7, Fernuni Hagen FB
Mathematik und
Informatik 1986 Kurseinheit 3

Page, Bruce, David Leitch, Pjilip Knightley
Philby- The Spy Who Betrayed a Generation.
Verlag Andre Deutsch, London 1968

Parrish, Th.
The ULTRA Americans- the U.S. Role in Breaking the Nazi Codes.
Stein and Day Publ., Briarcliff Manor, 1986

Paschke, Adolf
Das Chiffrier- und Fernmeldewesen im Auswärtigen Amt, seine Entwicklung und Organisation, Bonn
1957 in:
Intelligence Newsletter Winter 1997, p. 6 ff.

PEARL HARBOR
New Pearl Harbor Facts- Special Supplement- Section 2A in: Chicago Tribune 7. 12. 1966

Pearson, P.
Cryptoanalysis of a MacLaren- Marsaglia System
Cryptologia. 8: 97-108

PELTON
Fall Ronald Pelton. Sowjetische Code, NSA
Der Spiegel 9.6. 1986

Peng, T.A.
One million primes through the sieve
Byte, fall 1985

Perec, G.
Anton Voyls Fortgang. Frankfurt/M 1998

Perrault, Gilles
Die Professoren haben das Wort (S. 28ff.)
Auf den Spuren der Roten Kapelle.
Rowohlt 1969

Peters, T.
Das Tom Peters Seminar. Management in chaotischen Zeiten.
Campus Verlag Frankfurt/New York 1995

Peterson und Weldon
Error-Correcting Codes
MIT Press 1972

Pfitzmann, B., M. Schunter und M. Waidner
How To Break Another "Provably Secure" Payment System. EUROCRYPT, 95, Springer LNCS 921, S. 121-
132

Pfitzmann, B.
Digital Signature Schemes, General Framework and Fail- Stop- Signatures
Springer Verlag LNCs Bd.
1100, 1996

Pfleeger
Security in Computing
Prentice Hall 1989

Playboy
Die Code- Knacker, Heft Dez. 1975

Pfleeger
Security in Computing
Prentice-Hall 1989

Pleil, Th.
Geheimdienste hören gezielt deutsche Unternehmen ab.
Im Visier der Spione.
VDI- Nachrichten vom 14.3. 1997

Pötzl, Norbert F.
Chipkarten revolutionieren das menschliche Zusammenleben. IN: Der Spiegel, 48, 1994 H. 47, S. 62-79

Pötzl, Norbert F.
Über die Risiken perfektionierter Informationsverarbeitung.
Das Parlament, 26.4. 1986

POLY
Firma, Schweiz: Der Kode- Knacker AFR- 2000
Elektor, April 1985, S. 4-58

Pomerance, Carl
Recent Developments in Primality Testing: in: Mathematical Intelligencer, Vol. 3 (1983), S. 97-105,
Springer-Verlag

Pomerance, Carl
Search for prime numbers.
Scientific American, Dec. 1982

Pommerening, Klaus
Datenschutz und Datensicherheit.
BI- Wissenschaftsverlag Mannheim 1991

Prahl, Herbert
Nur Wasser hat keine Balken. in: PM 16.6. 1986

Pratt, Fletcher
Secret and Urgent. Bobbs- Merrill 1939

Praun, ALbert

Über Klartext und Geheimschriften. Wehrwissenschaftliche Rundschau, Mittler und Sohn 7/68

Preneel, B., R. Govaerts und J. Vandewalle
Information Authentification: Hash Functions and Digital Signatures. In: Computer Security and
Industrial Cryptography, Hrsg. B. Preneel u.a. Springer LNCS 741 (1993). S. 87-131

Pretty Good Privacy Inc.,
http://www.pgp.com

Putney, Diane T.
Ultra and the Army Air Forces in World War II.
Office of Air Force History USAF, Washington D.C. 1987

Quantenkryptographie
Süddeutsche Zeitung 15.4. 1993

Rabin, M.O.
Probalistic Algorithmic for Testing Primality; in: Journal of Number Theory 12 (1980), S. 128-138

Randell, B.
The Colossus. University of Newcastle upon Tyne Computing Laboratory 1976

von Randow, Thomas
Kryptologie. Die Codeknacker. Zeit- Magazin 16.3.1990, S. 66-71

Retter, C.
Cryptoanalysis of a MacLaren- Marsaglia System (1984)
Cryptologia 8: 97-108

Ribenboim, Paulo
Gibt es primzahlerzeugende Funktionen?
DdM 2 (1994), S. 81ff

Ribenboim, Paulo
The Book of Prime Number Records. Springer Verlag, New York 1988,1996

Rice, Peter
Arithmetic on your PC
BYTE, March 1985

Richter & Co. (Hannover)
CD-660, der Code- Knacker
ELO 6(1986)

Riesel, Hans

Prime Numbers & Computer Methods for Factorization.
Birkhäuser, Boston 1985

Rivest, R.
The RC5 encryption algorithm. in: Fast Software Encryption- Second International Workshop, Leuven
Belgien, Springer Verlag 1995. LNCS Bd. 1008, S. 86-96

Rivest, R.L., A. Shamir, L. Adleman
A Method for obtaining digital signatures and public key cryptosystems, Comm. of the ACM 21 (1978),
S. 120-126

Rogaway, P., D. Coppersmith
A Software- Oriented Encryption Algorithm. in: Fast Software Encryption, Cambridge Security Workshop
Proceedings, Springer Verlag 1994, S. 56-63

Rogier, N., P. Chauvaud
The compression function of MD2 is not collision free, siehe
Rohrbach, Hans
Chiffrierverfahren der neuesten Zeit. Archiv der elektr. Übertragung Heft 9(1948)
S. 362-369

Rohrbach, Hans
Mathematische und maschinelle Methoden beim Chiffrieren und Dechiffrieren.
FIAT Review of German Science, Wiesbaden 1948.

Rohwer, Jürgen
Die Nachrichtentechnik und der Angriff auf Pearl Harbor, in:
Militärgeschichtliche Mitteilungen, 1968, Heft 2, Freiburg 156ff.

Rohwer, Jürgen
Die Funkaufklärung und ihre Rolle im 2. Weltkrieg. Krieg im Äther.
In: Sammlung der Kolloquiumsvorträge, XIX. Folge
Motorbuch Verlag Stuttgart 1979

Rohwer, Jürgen
"Ultra-Dienst und "Magic". In: Marine- Rundschau H.10 1979, S. 637

Rollema, D.W.
Enigma. Wireless World, June 1983, p. 49-54

Roman, S.
Introduction to Coding and Information Theory
Springer 1997

RSA

Sicherheit bei der Datenübermittlung durch Public- Key- Verschlüsselung.
Sicherheitsberater 2.9. 1985

Rueppel, R.
Analysis and Design of Stream Ciphers. Springer Verlag Berlin 1986.

Ruhmann, I., Schulzki-Haddouti, C.
Abhör- Dschungel- Geheimdienste lesen ungeniert mit.
In: c`t 16(1998), H. 5, S. 82-93

Ryska, Norbert, Siegfried Herda
Kryptographische Verfahren in der Datenverarbeitung.
Springer-Verlag Berlin, Heidelberg, New York 1980

Salomaa, A.
Computation and automata.

Cambridge University Press, 1985

Salomaa, A.
Public- Key Cryptography. Springer Verlag Berlin 1990
2. Auflage 1996

Santoni, Alberto
Ultra siegt im Mittelmeer.
Hg. von Jürgen Rohwer
Verlag Bernhard und Graefe Koblenz 1985

Schauffler, Rudolf
Erinnerungen eines Kryptologen.
Urach/Württemberg 1962
Newesletter WInter 1997. p. 4

Schaumüller-Bichl, Ingrid
Sicherheitsmanagement
BI- Wissenschaftsverlag, Mannheim 1992

Schmidt- Eenboom, Erich
Sicherheit in der Informationstechnik: Abwehr auf Abwegen.

Schneickert, Hans
Die Geheimschriften im Dienste des Geschäfts- und Verkehrslebens. Leipzig 1900

Schneier, Bruce
Angewandte Kryptographie. Addison Wesley, Bonn 1996.
Applied Cryptography. John Wiley & Sons 1996

Schneier, Bruce
E- mail Security: how to keep your electronic messages private.

John Wiley & Sons, 1995

Schneier, Bruce
Description of a New Variable- Length Key, 64-Bit Block Cipher, in : Fast Software Encryption,
Cambridge Security Workshop Proceedings, Springer- Verlag 1994, S. 191-204

Schneier, Bruce
The Blowfish Encryption Algorithm,
Dr. Dobbs Journal Bd. 19 (1994) H.4, S. 38-40

Schnitzspan, W.
Schwierigkeiten mit dem Thema Militär und weitere Geheimnisse- Integration gesellschaftlicher
Aspekte in den Informatikunterricht. In: Computer und Unterricht 1992, H. 8, S. 52-56

Schulz, Ralph- Hardo
Codierungstheorie- eine Einführung. Braunschweig/Wiesbaden, Vieweg 1991

Schulz, Ralph-Hardo, Chr. Tismer
Implementierung eines kleinen Hamming- Codes
PM 28(1986)

Schulz, Ralph- Hardo
Primzahlen in öffentlichen Chiffrierverfahren. Mathematik lehren 61 (1993), S. 56-64

Schulz, Ralph-Hardo
Über das Zählen mit Hilfe von Bäumen.
math. did. 3 (1980), S. 35-55

Schulz, Ralph- Hardo
Übersetzen von Nachrichten für die digitale Übertragung. Ausgewählte Aspekte der Quellencodierung.
MU 3(1987), S. 23-44

Schulz, Ralph- Hardo
Wörterinterpretationen an Beispielen einfacher Codes.
DdM 2(1984), S. 113-131

Schwill, Andreas
Kryptographie. (RSA) in: LOG IN 7(1987), Heft 3, S. 56f.), auch: BI Mannheim, Schülerduden "Informatik"

Seiffert, M.
Verschlüsselungsmethoden- Eine anwendungsorientierte Einführung mit SCHEME in LOGIN 14(1994),

H. 3, S. 33-40

Sennholz, K.
Verschlüsselte Botschaften. Informatik betrifft uns. 2/1995, S. 1-23

Sgarro, Andrea, Marcus Würmeli
Geheimschriften. Weltbild- Verlag Augsburg 1991

Shamir, Adi
How to Share a Secret.
Communications of the ACM, Bd. 22 (1979) H.1, S. 612-613

Shamir, Adi
über A. Shamir: Schachteln im Rucksack. Ein israelischer Mathematiker knackte einen Computer-
Code...
in: Der Spiegel 48(1982), S. 219ff.)

Shannon, Claude Elwood
Communication Theory of secrecy systems. Bell. Sys. Tech. J. 28 u.30 (1949), 657-715

Siegenthaler, T.
Decrypting a class of stream ciphers using ciphertext only (1985)
IEEEE Transactions on Computer

Simmons, Gustavus J. (Hg.)
Contemporary Cryptology. IEEE Press 1992.

Simmons, Gustavus
Cryptology. The Mathematics of secure Communication; in: Mathematical Intelligencer, Vol. 4(1979),
S. 233-246

Simmons, G.J.
Cryptoanalysis and Protocol Failures. Comm. ACM Vol. 37
Nr. 11 (1994), S. 56-65

Simmons, G.
The Subliminal Channel and Digital Signatures.
in: EUROCRYPT 84, Springer Verlag 1985, S. 364-378

Sinkov, Abraham
Elementary Cryptography. Random Hause and The L. W. Singer Company Pb.
New York 1968

Skillen, Hugh
The Enigma Symposium 1992

Hugh Skillen 1992

Smith, Bradely F.
The Ultra Magic Deals and the most secret Relationship 1940-46
Presidio Press Novato 1993

Smith, John
Public key cryptography.
BYTE, Nanuary 1983

Smith, Laurence Dwight
Cryptography. The Science of Secret Writing. New York Norton 1943 (Dover Paperback 1955)

Stadlin, Hans
100 Jahre Boris Hagelin 1892-1992
Firmenveröffentlichung der Crypto Ag Zug

Stallings, William
Sicherheit im Datennetz. Datensicherheit mit PGP, Prentice Hall London 1995

Stallings, William
Cryptography and Network Security: Principles and Practice, Prentice Hall 1998

Stallings, William
Datensicherheit mit PGP
Prentice Hall

Steinacker, A.
Anonyme Kommunikation in Netzen. BI Wissenschaftsverlag, Mannheim 1993

Stephan, Franz
Dringend: Wer hat eine Geheimschrift, die wirklich niemand entziffern kann?
PM, 19.7. 1985

Stephan, Franz
Den Schlüssel kennt jeder- entschlüsseln kann keiner.
PM, 23. 8. 1985

Stiller, Werner
Verschlüsselungen im Fotomaterial
Im Zentrum der Spionage. Mainz 1986

Stinson, Douglas R.
Cryptography. Theory and Practice.
CRC Press Boca Raton London 1995

Stolberg, Catrin
Bericht über TV- Sendung "...gegen Engeland. Dokumentation über den U-Boot-

Krieg im Nordatlantik":
In Bletchley Park entschlüsselten die Briten deutsche Funksprüche. in:
Berliner Morgenpost 22.4. 1987

Stripp, Alan
A British cryptoanalyst salutes the polish cryptoanalysts.
The Enigma Bulletin May 1998, p. 1ff)

Stürzinger, Oskar
Maschinelle Chiffrierverfahren. 1960
Crypto AG Zug

The Cryptogram
Info- Blatt (Canada), siehe SdW Dez. 1988, S. 11

Thong, T.K., R. Schulz
Implementation of the RSA Public Key Cryptosystem. Math. Medley 19/2 1991
(SIngapore) S. 53-64

Topsoe, F.
Informationstheorie
Teubner, Stuttgart 1974

Townsend, P.D., J.G. Rarity. P.R. Trapster
Enhanced Single Photon Fringe Visibility in a 10km-long Prototype Quantum
Cryptography Channel.
Electronic Letters Bd. 28 (1993) H. 14 S. 1291-1293

Trenkle, Fritz
Die deutschen Funknachrichtenanlagen bis 1945. Elektromechanische
Schlüsselmaschinen (Rudolf
Staritz)
Telefunken Systemtechnik ULm 1990

Tuchman, Barbara W.
The Zimmermann Telegramm.
New York 1958

Türkel, Siegfried
Chiffrieren mit Geräten und Maschinen. Graz 1927

Tully, Andrew
Die Unsichtbare Front., Krypto Beispiele S. 94

Tum, R.
Privacy transformations for databank systems, in: Proc. Nat. Comp. Conf. and
Exp. (NCC) 1973

Uher, B.
Geheimcodes und Vershclüsselungen und die Mathematik des Zufalls. Mathe-Welt. Mathematik lehren
71/1995 S. 8(30)-23(45)

Uhl, W.
Kodierungen im Unterricht.
In: MU- Der Mathematikunterricht 33(1987), H. 3, S. 46-72

Ungerer, Bert
Knackfreundlich- schnelle online- Plattenverschlüsselung birgt Risiken
c't - magazin für computertechnik, Juni 1994

Vierengel, Heinz
ZVDIALSFBNOUPYM
Technologie und Schule 4/74

Wängler, Hans Heinrich
Rangwörterbuch neuhochdeutscher Umgangssprache. 1963

WALKER
Fall John Walker/Jerry Whitworth
Die Zeit, 8. 11. 1985

Wayner, Peter
Disappearing Cryptography
Academic Press 1996

Wefelscheid, H.
Einführung in die Informationstheorie
MU 3(1974), S. 5-35

Weighton, Ch.
Meisterspione der Welt, S. 49ff.)
Düsseldorf 1963

Weikert, Alexandra und Hubert
Kryptographie mit dem Computer
Verschlüsselungs- Praxis mit PGP

Weis, R.
Zwei Schlüssel einer Nachricht- Kryptographie mit öffentlichen Schlüsseln.
In: PC Magazin Spezial (Kryptographie)

Welch, A.T.
A Technique for High- Performance Data Compression,
IEEE Computer 17(6) (1984, S. 8-14

Welsh, Dominic
Codes and Cryptography. Clarendon Press. Oxford New York 1988

West, Nigel
G.C.H.Q- The Secret Wireless War 1900-1986 Coronet Books 1987

Wetjen, B.
Know-how zum Nulltarif
Wirtschaftsdienst, Monatsschrift der IHK Dresden
Nr. 2/96, S. 15-17

Whitaker, P., L. Kruh
From Bletchley Park to Berchtesgaden.
Cryptologia July 1987, p. 129-155

White, Maurice
Secret Writing. Washington The Washington Service Bureau, 1938, S. 24 ff.
(Service Booklet Nr. 181)

Wieckmann, Jürgen
Chaos Computer Club. Das chaos-computer- buch- Hacking made in Germany,
Hamburg Rowohlt 1988

Wilkinson, Leland
Systat: The System for Statistics. Systat Inc., Evanston, IL, 1987

Winterbotham, Frederick, W.
The Ultra Secret.
Harper&Row New York-
Weidenfeld und Nicholson, London 1975
dazu: Seelöwe hat ausgespielt
Der Spiegel 36(1975), S. 52ff.)
Aktion ULTRA. Ullstein 1976

Wise, David, Thomas B. Ross
Das Spionage Establishment, S.49ff.)
Berlin 1968

Witten, Helmut
Codierungstheorie. Ein Überblick, LOGIN 5/6 (1994) S. 26-34

Wobst, R.
Schnell & geheimnisvoll, Ein neues Verschlüsselungsverfahren.
UNIX- Magazin 7/92, S. 86-95

Wobst, R.
Dringendes Bedürfnis,

UNIX Open 4/93, S, 32-34

Wobst, R.
Diskette voller Geheimnisse.
UNIX Open 9/95, S. 54-61

Wobst, R.
Wissen ist Macht. UNIX Open 4/96, S. 94-100
Starke Abwehr. UNIX Open 5/95, S. 118-124

Wolfe, Jack M.
A first course in Cryptoanalysis. Brooklyn College Press 1943

Wolfe, James Raymond
Secret Writing. Mc Grqaw Hill 1970

Wright, Peter
Spy Catcher. Viking Penguin 1987

Wrixon, Fred B.
Codes and Ciphers
Prentice Hall General Reference New York 1992

Yardley, Herbert Osborne
The American Black Chamber. Bobbs-Merrill 1931

Zimmermann, Phil(ip)
PGP, deutsche Übersetzung: SBN 3-9802182-5-2

Zimmermann, Phil(ip)
Pretty Good Privacy: Public Key Encryption for the Masses.

Zwikirsch, Joachim
So erbeuteten die Briten den deutschen Code.
Berliner Morgenpost, 15.3. 1987