Bibliographie zu Eine kurze Geschichte der verschlüsselten Kommunikation

Stefan Schumacher Stand: 2026-03-24

- https://cryptomancer.de/posts/20260321cltgeschichtekryptographie/
- https://chemnitzer.linux-tage.de/2026/de/programm/beitrag/159

Literatur

- Oberkommando der Wehrmacht (Ed.). (2019). *Allgemeine Schlüsselregeln für die Wehrmacht. H.Dv.g. 7, M.Dv.Nr. 534, L.Dv.g. 7. Vom 1. April 1944*. Books on Demand. https://onlinesammlung.museumsstiftung.de/detail/collection/4963d7d4-3b1b-4ec3-82c3-bcef49442fed
- Oberkommando der Wehrmacht (Ed.). (2019). *Signalschlüssel für den Funksignaldienst (Funksignalschlüssel) – Geheim. M.Dv.Nr. 114. Oktober 1939*. Books on Demand. https://onlinesammlung.museumsstiftung.de/detail/collection/719f4074-48f5-4d76-bb93-478a8fb726e6
- Kippenhahn, R. (1999). *Verschlüsselte Botschaften: Geheimschrift, Enigma und Chipkarte*. Rowohlt.
- Singh, S. (2000). *Geheime Botschaften*. Carl Hanser Verlag.
- Rohwer, J. (1979). Der Einfluss der alliierten Funkaufklärung auf den Verlauf des Zweiten Weltkrieges. *Vierteljahrshefte Für Zeitgeschichte*, *27*(3), 325–369. https://www.ifz-muenchen.de/heftarchiv/1979_3_1_rohwer.pdf
- AdGrafiCS. (2013). *History of Cryptography*. https://adgrafics.net/docs/thawte/history-cryptography.pdf . https://adgrafics.net/docs/thawte/history-cryptography.pdf
- Jozef Gruska. (2012). *History of Cryptography (Zimmermann Telegram section)*. https://www.fi.muni.cz/usr/gruska/crypto14/crypto_14.pdf . https://www.fi.muni.cz/usr/gruska/crypto14/crypto_14.pdf
- Hörenberg, M. (2026). *Enigma ULTRA Decrypts (Original Plaintext Messages)*. Enigma Project and National Archives source copies. https://enigma.hoerenberg.com/index.php?cat=The+U534+messages&page=ULTRA
- Archives", "U. S. N. (Ed.). (2026). _Zimmermann Telegram - Transcription _. National Archives and Records Administration. https://www.archives.gov/education/lessons/zimmermann
- Li, C., Ma, J., Tao, J., Keranen, M., Mayo, J., Shene, C.-K., & Wang, C. (2014). *The Vigenère Cipher*. https://pages.mtu.edu/ shene/NSF-4/Vigenere.pdf
- Wander, M. (2026). *Historic Cipher Examples (incl. Playfair)*. https://wander.science/teaching/network-security/SK_02_Historic_Ciphers.pdf . https://wander.science/teaching/network-

security/SK_02_Historic_Ciphers.pdf

- Bürgler, J. F. (2004). *Kryptologie (historische Beispiele: Caesar, Vigenère, Playfair)*. https://doczz.net/doc/5912796/kryptologie–version-20041015- . https://doczz.net/doc/5912796/kryptologie–version-20041015-
- Azraoui, M., Brunet, S., Canard, S., Diop, A., Eveillard, L., Filipiak, A., Hamdi, A., Misarsky, F., Kuate, D. N., Paindavoine, M., Santos, Q., & Vialla, B. (2021). *CYBERCRYPT: Learn Basic Cryptographic Concepts while Playing*. Cryptology ePrint Archive, Paper 2021/063. https://eprint.iacr.org/2021/063
- Perendi, D. M., & Gope, P. (2021). *The Language's Impact on the Enigma Machine*. Cryptology ePrint Archive, Paper 2021/1434. https://eprint.iacr.org/2021/1434
- Kaminsky, A. (2019). *Enigma 2000: An Authenticated Encryption Algorithm For Human-to-Human Communication*. Cryptology ePrint Archive, Paper 2019/488. https://eprint.iacr.org/2019/488
- Koblitz, N., & Menezes, A. J. (2015). *A Riddle Wrapped in an Enigma*. Cryptology ePrint Archive, Paper 2015/1018. https://eprint.iacr.org/2015/1018
- Molina-Gil, J., Caballero-Gil, C., Gutiérrez-de-Armas, J., & Yung, M. (2024). *Covert 19th century political intrigues of Tenerife nobility revealed by cryptanalyzing an encrypted letter*. Cryptology ePrint Archive, Paper 2024/2031. https://doi.org/10.1080/01611194.2024.2396811
- Blair, E. (2024). *Cryptography at the Crossroads: Ethical Responsibility, the Cypherpunk Movement and Institutions*. Cryptology ePrint Archive, Paper 2024/970. https://eprint.iacr.org/2024/970
- Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (2nd ed.). John Wiley & Sons.
- Ferguson, N., & Schneier, B. (2003). *Practical Cryptography*. John Wiley & Sons.
- Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(4), 656–715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x
- Bellovin, S. M., & Bush, R. (2002). *Security Through Obscurity Considered Dangerous* [Internet-Draft]. Internet Engineering Task Force (IETF). https://datatracker.ietf.org/doc/html/draft-bellovin-obscurity-00
- Morris, R. H., & Thompson, K. (1979). Password Security: A Case History. In *Communications of the ACM* (Vol. 22, Issue 11, pp. 594–597). https://doi.org/10.1145/359168.359172
- Ritchie, D. M. (1975). *On the Security of UNIX*. Bell Laboratories. https://bitsavers.org/pdf/att/unix/UNIX_System_Readings_and_Applications_Volume_2_1987.pdf#page=91
- Morris, R. H. (1978). *Cryptanalysis of Rotor Machine (M-209) and related methods*.
- *Unix crypt(1) source code (Version 6/7)*. The Unix Heritage Society Archive. http://minnie.tuhs.org/cgi-bin/utree.pl?file=V7/usr/src/cmd/crypt/crypt.c
- *A Research Unix Reader: Annotated excerpts from the Programmer's Manual, 1971–1986*. Dartmouth College / TUHS. https://citeseerx.ist.psu.edu/document?doi=42723b1b7024d0fddf7222bd64e961442f08a7af
- Diffie, W., & Landau, S. (2007). The Export of Cryptography in the 20th and the 21st Centuries. In K. de Leeuw & J. Bergstra (Eds.), *The History of Information Security: A Comprehensive Handbook* (pp. 725–769). Elsevier. https://doi.org/10.1016/B978-044451608-4/50027-4
- Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on*

Information Theory, *22*(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638

- Rivest, R. L., Shamir, A., & Adleman, L. M. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342
- Merkle, R. C. (1978). Secure Communications Over Insecure Channels. *Proceedings of the National Computer Conference*.
- Goldwasser, S., & Micali, S. (1982). Probabilistic Encryption & How to Play Mental Poker Keeping Secret All Partial Information. *Proceedings of the 14th Annual ACM Symposium on Theory of Computing (STOC)*, 365–377. https://www.cs.purdue.edu/homes/ninghui/readings/Qual2/Goldwasser-Micali82.pdf
- Shamir, A. (1979). How to Share a Secret. *Communications of the ACM*, *22*(11), 612–613.
- ElGamal, T. A. (1985). A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *IEEE Transactions on Information Theory*, *31*(4), 469–472. https://doi.org/10.1109/TIT.1985.1057074
- National Institute of Standards and Technology (NIST). (1994). *Digital Signature Standard (DSS), FIPS PUB 186*. NIST. https://doi.org/10.6028/NIST.FIPS.186
- Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. *Advances in Cryptology \Normalfont — CRYPTO '85 Proceedings*, 417–426. https://doi.org/10.1007/3-540-39799-X_31
- Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation*, *48*(177), 203–209. https://doi.org/10.1090/S0025-5718-1987-0886104-5
- Cohen, H., & Frey, G. (E. (2005). Handbook of Elliptic and Hyperelliptic Curve Cryptography. In *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press. https://www.maths.gla.ac.uk/ ajb/dvi-texts/ecc.pdf
- Strehle, R. (1994). *Verschlüsselt: Der Fall Hans Bühler*. Werd Verlag.
- Sassòli, M. (2021). Die Schweizerische Neutralität und der Fall Crypto AG. *Swiss Review of International and European Law*, *31*(4), 523–540. https://archive-ouverte.unige.ch/unige:166084
- Dymydiuk, J. (2020). RUBICON and revelation: The curious robustness of the 'secret' CIA–BND operation with Crypto AG. *Intelligence and National Security*, *35*(5), 641–658. https://doi.org/10.1080/02684527.2020.1774853
- Aldrich, R. J., Müller, P. F., Ridd, D., & Schmidt-Eenboom, E. (2020). Operation Rubicon: sixty years of German-American success in signals intelligence. *Intelligence and National Security*, *35*(5), 603–607. https://doi.org/10.1080/02684527.2020.1774849
- Dobson, M. J. (2020). Operation Rubicon: Germany as an intelligence 'great power'? *Intelligence and National Security*, *35*(5), 608–622. https://doi.org/10.1080/02684527.2019.1682621
- Frik, S. (2007). Boris Hagelin and Crypto AG: Pioneers of Encryption. In R. Anderson & C. E. Landwehr (Eds.), *The History of Information Security* (pp. 479–496). Elsevier. https://www.sciencedirect.com/science/article/pii/B9780080454880500273
- Moyes, H. (2020). The Cryptographic Trojan Horse: Operation Condor. *Chief Editor Caverlee Dahill, Assistant Editors Kate Brady*, 19–35.
- Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. Metropolitan Books. https://us.macmillan.com/books/9780805094560/noplace-to-hide

- Brustolin, V., de Oliveira, D., & dos Reis Peron, A. E. (2023). Exploring the relationship between Crypto AG and the CIA in the use of rigged encryption machines for espionage in Brazil. *Cambridge Review of International Affairs*, *36*(1), 54–87. https://doi.org/10.1080/09557571.2022.2123456
- Barker, E., & Kelsey, J. (2006). *Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90* (Special Publication SP 800-90; Issue SP 800-90). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90
- National Institute of Standards and Technology. (2025). *Recommendation for Random Bit Generator (RBG) Constructions, NIST Special Publication 800-90C* (Special Publication SP 800-90C; Issue SP 800-90C). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-90C
- National Institute of Standards and Technology. (2002). *Security Requirements for Cryptographic Modules* (Federal Information Processing Standards Publication FIPS PUB 140-2; Issue FIPS PUB 140-2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.FIPS.140-2
- Young, A., & Yung, M. (1997). Kleptography: Using Cryptography Against Cryptography. In W. Fumy (Ed.), *Advances in Cryptology - EUROCRYPT 1997* (pp. 62–74). Springer Berlin Heidelberg.
- Young, A., & Yung, M. (1997). The prevalence of kleptographic attacks on discrete-log based cryptosystems. In B. S. Kaliski (Ed.), *Advances in Cryptology - CRYPTO 1997* (pp. 264–276). Springer Berlin Heidelberg.
- Brown, D. R. L. (2006). *Conjectured Security of the ANSI-NIST Elliptic Curve RNG*. Cryptology ePrint Archive, Paper 2006/117. https://eprint.iacr.org/2006/117
- Schoenmakers, B., & Sidorenko, A. (2006). *Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator*. Cryptology ePrint Archive, Paper 2006/190. https://eprint.iacr.org/2006/190
- Brown, D. R. L., & Gjøsteen, K. (2007). *A Security Analysis of the NIST SP 800-90 Elliptic Curve Random Number Generator*. Cryptology ePrint Archive, Paper 2007/048. https://eprint.iacr.org/2007/048
- Goh, E.-J., Boneh, D., Pinkas, B., & Golle, P. (2003). The Design and Implementation of Protocol-Based Hidden Key Recovery. In J. C. Kwak & R. H. Deng (Eds.), *Information Security* (Vol. 2851, pp. 165–179). Springer.
- Young, A. L., & Yung, M. (2007). Space-Efficient Kleptography Without Random Oracles. *Information Hiding*, *4567*, 112–129.
- Checkoway, S., Fredrikson, M., Niederhagen, R., Everspaugh, A., Green, M., Lange, T., Ristenpart, T., Bernstein, D. J., Maskiewicz, J., & Shacham, H. (2014). On the Practical Exploitability of Dual EC in TLS Implementations. *Proceedings of the 23rd USENIX Security Symposium*, 319–335.
- Wertheimer, M. (2015). Encryption and the NSA Role in International Standards. *Notices of the American Mathematical Society*, *62*(2), 165–167. https://doi.org/10.1090/noti1213
- Voelsen, D. (2019). 5G, Huawei und die Sicherheit unserer Kommunikationsnetze: Handlungsoptionen für die deutsche Politik. *SWP-Aktuell*, *5/2019*. https://www.ssoar.info/ssoar/bitstream/handle/document/61663/ssoar-2019-voelsen-5G_Huawei_und_die_Sicherheit.pdf
- Kaska, K., Beckvard, H., & Minárik, T. (2019). Huawei, 5G and China as a security threat. *NATO Cooperative Cyber Defence Center for Excellence (CCDCOE)*, *28*, 1–26. https://www.ccdcoe.org/

uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf

- Tekir, G. (2020). Huawei, 5G network and digital geopolitics. *International Journal of Politics and Security*, *2*(4 (Çin Özel Sayısı), 113–135. https://www.researchgate.net/publication/343949557_Huawei_5G_Network_and_Digital_Geopolitics
- Rühlig, T. (2020). Who controls Huawei. *Implications for Europe*. https://www.ui.se/globalassets/butiken/ui-paper/2020/ui-paper-no.-5-2020.pdf
- Friis, K., & Lysne, O. (2021). Huawei, 5G and security: Technological limitations and political responses. *Development and Change*, *52*(5), 1174–1195. https://doi.org/10.1111/dech.12680
- Krolikowski, A., & Hall, T. H. (2023). Non-decision decisions in the Huawei 5G dilemma: Policy in Japan, the UK, and Germany. *Japanese Journal of Political Science*, *24*(2), 171–189. https://doi.org/10.1017/S146810992200038X
- Dunin, E., Ekhall, M., Hamidullin, K., Kopal, N., Lasry, G., & Schmeh, K. (2021). How We Set New World Records in Breaking Playfair Ciphertexts. *Cryptologia*. https://doi.org/10.1080/01611194.2021.1905734