Použitá literatura

Knihy

Bamford James, *The Puzzle Palace: A Report on America´s Most Secret Agency*. Boston: Houghton Mifflin, 1982. Úplný příběh National Security Agency.

Denning, Dorothy E.R. *Cryptography and Data Security*. Reading: Addison Wesley, 1983.

Hinsley, F.H., and Alan Stripp. *Code Breakers: The Inside Story of Bletchley Park*. Oxford: Oxford University Press, 1993.

Hodges, Andrew. *Alan Turing: The Enigma*. New York: Simon&Schuster, Inc., 1983.

Úplný životopis brilantního vědce, který rozluštil kód „Enigma", největší německé tajemství za druhé světové války. Turing byl průkopníkem moderního počítačového věku a nakonec krutou obětí studené války na poli vojenských tajemství a sexuálních skandálů.

Kahn, David. *The Codebreakers*. New York: Macmillan Company, 1972.

Kahn, David. *Seizing the Enigma: The Race to Break the German U-boat Codes*, 1939-1943. Bostoon: Hougton Mifflin, 1991.

Merkle, Ralph. *Secrecy, Authentication and Public Key Systems*. Ann Arbor: UMI Research Press, 1982.

Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, 1994. Nejsouhrnnější dosud vydaná kniha o počítačovém šifrování a technikách uchování dat v soukromí.

RSA Data Security, Inc. *MailSafe: Public Key Encryption Software* (user´s manual) Version 5.0. Redwood City, Calif.: 1994.

Smith, Lawrence Dwight. *Cryptography: The Science of Secret Writing*. New York: Dover Publications, 1941.

Weber, Ralph Edward. *United States Diplomatic Codes and Ciphers*, 1775-1938. Chicago: Precedent Publishing Inc., 1970.

Přednášky a ostatní publikace

Association for Computing Machinery, „Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy.“ *Report of a Special Panel of the ACM U.S. Public Policy Commitee* (USACM) (June 1994). (URL: *http://info.acm.org/reports/acm_crypto_study.html*)

Coppersmith, Don. *IBM Journal of Research and Development 38* (1994).

Diffie, Whitfield. „The First Ten Years of Public-Key Cryptography,“ *Proceeding og the IEEE 76* (1988): 560-76. Procházka historií šifrování veřejným klíčem od Whitfielda Diffieho s objevnými komentáři.

Diffie, Whitfield, and M.E. Hellman. „New Directions in Cryptography.“ *IEEE Transactions on Information Theory IT-22* (1976).

Hoffman, Lance J., Ali, Faraz A., Heckler, Steven L., and Ann Huybrechts. „Cryptogrphy Policy.“ *Communications of the ACM 37* (1994): 109-17.

Lai, Xuejia. „On the Design and Security of Block Ciphers.“ *ETH Series in Information Processing 1* (1992). Článek, popisující šifru IDEA.

Lai, Xuejia, and James L. Massey. „A Proposal for New Block Encryption Standard.“ *Advances in Cryptology-EUROCRYPT ´90 Proceedings* (1992): 55-70. Další článek o IDEA.

Lenstra, A.K., Lenstra, Jr., H.W., Manasse, M.S., and J.M. Pollard. „The Number Field Sieve.“ *Proceedings of the 22nd ACM Symposium on the Theory of Computing*. Baltimiore: ACM Press, 1990, pp. 564-72.

Lenstra, A.K., Lenstra, Jr., H.W., Manasse, M.S., and J.M. Pollard. „The Factorization of the Ninth Fermat Number.“ *Mathematics of Computation* 61 (1993): 319-50.

Merkle, Ralph. „Secure Communication Over Insecure Channels.“ *Communications of the ACM* 21 (1978): 294-99 (předloženo v roce 1975).

Merkle, Ralph, and Martin E. Hellman. „On the Security of Multiple Encryption.“ *Communications of the ACM* 24 (1981): 465-67.

Merkle, Ralph, and Martin E. Hellman. „Hidding Information and Signatures in Trap Door Knapsacks.“ *IEEE Transactions on Information Theory* 24 (1978): 525-30.

National Bureau of Standards. *Data Encryption Standard FIPS PUB 46-1* (1978).

Rivest, Roon. *Ciphertext: The RSA Newsletter* 1 (1993).

Rivest, Ron, Shamir, A., and L. Adleman. „A Method for Obtaining Digital Signatures and Public Key Cryptosystems.“ *Communications of the ACM* 21 (1978).

Simmons, G.J. „How to Insure that Data Acquired to Verify Treaty Compliance are Trustwothy," in „Authentication without secrecy: A secure communications problem uniquely solvable by asymmetric encryption techniques." *IEEE EASCON ´79*, Washington, D.C. 1979, pp. 661-62.

Thompson, Ken. „Reflections on Trusting Trust." *Communications of the ACM* 27 (1984). Tohle si musí přečíst každý, kdo se snaží pochopit omezení počítačové bezpečnosti a důvěry.

Elektronické zdroje

Cypherpunk Internet mailing list. Pro informace odešlete e-mail na adresu *cypherpunk-request@toad.com*.

Edstrom, Gary B. „Frequently Asked Questions" (PGP FAQ). Elektronicky přístupné ve skupině Usenet *alt.security.pgp* s příležitostnou aktualizací.

Electronic Privacy Information Center (EPIC). E-mail: *info@epic.org*.

Electronic Frontier Foundation (EFF). E-mail: *info@eff.org*.

Hastur, Henry. „Stealth," program rozdělí zprávy PGP tak, že nemohou být snadno identifikovány. Dostupný pod anonymním FTP na *wuarchive.wustl.edu:/pub/aminet/util/crypt/StealthPGP1_O.lba*

Meeks, Brock N. *Cyberwire Dispatch*. Je to poštovní seznam, který sleduje problematiku elektronického soukromí. Můžete si jej objednat odesláním zprávy „subscribe cwd-1" na adresu *majordomo@cyberweeks.com*.

Xenon (neznámý pseudonym). „Here´s How to MacPGP!" Dostupné po odeslání e-mailu na adresu *qwerty@netcom.com* s heslem „Bomb me!". Dostupné také na *ftp://ftp.netcom.com /pub/qwerty*.

Zimmermann, Phil. *PGP User´s Guide*. Bouldeer, Colo., 1994. Zahrnuto do softwaru PGP.

Můžete najít tyto zájmové skupiny Usenet: *alt.security.pgp, alt.privacy, comp.security.misc, sci.crypt.*

Ačkoliv existuje mnoho zdrojů PGP a s nimi souvisejících souborů (viz příloha A), na adrese *ftp.ox.ac.uk* najdete zvláště úplnou sadu zdrojů PGP, včetně nejaktuálnějších jazykových souborů.