Irodalom

[1] M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. In *IEEE Transactions on Software Engineering*, 22(1), 1996.

[2] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the First Annual ACM Conference on Computer and Communications Security*, 1993.

[3] M. Bellare and P. Rogaway. Optimal asymmetric encryption – How to encrypt with RSA. In *Advances in Cryptology – EUROCRYPT'94*, Lecture Notes in Computer Science 950, Springer-Verlag, 1995.

[4] M. Bellare and P. Rogaway. The exact security of digital signatures: How to sign with RSA and Rabin. In *Advances in Cryptology - EUROCRYPT'96*, Lecture Notes in Computer Science 1070, Springer-Verlag, 1996.

[5] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, 1993.

[6] D. Bleichenbacher. A chosen ciphertext attack against protocols based on the RSA encryption standard RSA PKCS #1. In *Advances in Cryptology – CRYPTO'98*, Lecture Notes in Computer Science 1462:1–12, Springer-Verlag, 1998.

[7] M. Blum and S. Micali. How to generate cryptographically strong pseudo-random bits. *SIAM Journal of Computing*, 13(4):850–863, November 1984.

[8] D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203-213, 1999.

[9] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. In *Proceedings of the Royal Society*, December 1989.

[10] R. Cramer and V. Shoup. A practical public key cryptosystem probably secure against adaptive chosen ciphertext attack. In *Advances of Cryptology – Crypto'98*, Lecture Notes in Computer Science 1462, Springer-Verlag, 1998.

[11] J. Daemen and V. Rijmen. *The Design of Rijndael*. Springer-Verlag, 2001.

[12] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM*, 33(4):210–217, 1986.

[13] O. Goldreich and L. Levin. A hard predicate for all one-way functions. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing*, 1989.

[14] O. Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Springer-Verlag, Algorithms and Combinatorics, Vol. 17, 1998.

[15] A. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28:270–299, April 1984.

[16] N. Koblitz. *A Course in Number Theory and Cryptography*. Graduate Texts in Mathematics, No. 114, Springer-Verlag, New York, 2nd edition, 1994.

[17] N. Koblitz. *Algebraic Aspects of Cryptography*. Algorithms and Computation in Mathematics, Vol. 3, Springer-Verlag, New York, 1998.

[18] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal of Computation*, 17(2), April 1988.

[19] A. Mehrotra and L. Golding. Mobility and security management in the GSM system and some proposed future improvements, In *Proceedings of the IEEE*, 86(7):1480–1496, July 1998.

[20] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*, CRC Press, 1996.

[21] Nemetz T. és Vajda I., Algoritmusos adatvédelem. Akadémiai Kiadó, 1991.

[22] D. O'Mahony, M. Peirce, and H. Tewari. *Electronic payment systems*. Artech House Inc, Boston, 1997.

[23] B. Preneel. Analysis and Design of Cryptographic Hash Functions. Doctoral Dissertation, Katholieke Universiteit Leuven, 1993.

[24] B. Schneier. *Applied Cryptography*. Wiley, 1996.

[25] D. Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.

[26] S. Vaudenay. Security flaws induced by CBC padding – Applications to SSL, IPSEC, WTLS, . . . In *Advances in Cryptology – EUROCRYPT'02*, Lecture Notes in Computer Science 2332, Springer-Verlag, 2002.

[27] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol. In *Proceedings of the 2nd Usenix Workshop on Electronic Commerce*, 1996.

[28] P. Zimmermann. *The Offi cial PGP User's Guide*. MIT Press, 1995.