REFERENCES

[1] Caloyannides, M.A. (2000) Encryption Wars: Early Battles. IEEE Spectrum, 37(4), April 2000. pp.37-43.

[2] Denning, D.E. (1983) Cryptography and Data Security. Addison-Wesley Publishing Company, Inc.

[3] Schneier, B. (1999) Applied Cryptography. John Wiley & Sons, Inc.

[4] Stallings, W. (1999) Cryptography and Network Security, 2nd Edition. Prentice Hall Inc.

[5] Simmons, G.J. (1979) Symmetric and Asymmetric Encryption. Computing Surveys, 11 (4). pp.305-330.

[6] Shannon, C. (1949) Communication Theory of Secrecy Systems. Bell System Technical Journal, 28(4).

[7] Sorkin, A. (1984) LUCIFER: A Cryptography Algorithm, Cryptologia, 8 (1).

[8] Data Encryption Standard (1977) FIPS PUB 46, Washington, DC. National Bureau of Standards.

[9] Adams, C. (1997) The CAST-128 Encryption Algorithm. RFC 2144.

[10] Brown, L., Pieprzyk, J. and Seberry, J. (1990) LOKI - a cryptographic primitive for authentication and secrecy applications. In: Proceedings of AUSTCRYPT 90. Springer-Verlag. pp.229-236.

[11] Shimizu, A. and Miyaguchi, S. (1988) Fast data encipherment algorithm FEAL. In: EUROCRYPT '87 Proceedings. Springer-Verlag. pp.267-278.

[12] Lai, X. and Massey, J. (1991) Markov Ciphers and Differential Cryptanalysis. In: Advances in Cryptology-EUROCRYPT '91 Proceedings. Springler-Verlag.

[13] Merkle, R. (1991) Fast software encryption functions. In: Menezes and Vanstone ed. Proceedings of CRYPTO '90. Springer-Verlag. pp.476-501.

[14] Diffie, W. and Hellman, M. (1976) New Directions in Cryptography. IEEE Transactions on Information Theory, IT-22 (6). pp.644-654.

[15] Diffie, W. and Hellman, M. (1997) Exhaustive Cryptanalysis of the NBS Data Encryption Standard. Computer, 10. pp.74-84.

[16] Fairfield, R.C., Matusevich, A. and Plany, J. (1985) An LSI Digital Encryption Processor (DEP). IEEE Communications, 23 (7). pp.30-41.

[17] Verbauwhede, I., Hoornaert, F., Vanderwalle, J., De Man, H. and Govaerts, R. (1988) Security Considerations in the Design and implementation of a New DES Chip. In: Advances in Cryptology: EUROCRYPT '87 Proceedings. Springer-Verlag. pp.287-300.

[18] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 4 (1). pp.3-72.

[19] Matsui, M. (1993) Linear Cryptanalysis Method for DES Cipher. In: Advances in Cryptology - EUROCRYPT '93 Proceedings. Springer-Verlag. pp.386-397.

[20] Knudsen, L. and Meier, W. (1996) Improved differential attacks on RC5. In: Advances in Cryptology-CRYPTO'96. Springer-Verlag. pp.216-228.

[21] ISO DIS 8732 (1987) Banking-Key Management (Wholesale). London. Association for Payment Clearing Services.

[22] Merkle, R.C. and Hellman, M. (1981). On the Security of Multiple Encryption. Computer Communications of the ACM, 24 (7). pp.465-467.

[23] Van Oorschot, P.C. and Wiener, M.J. (1991) A Known-Plaintext Attack on Two-Key Triple Encryption. In: Advances in Cryptology – EUROCRYPT '90 Proceedings. Springer-Verlag. pp.318-325.

[24] Kam, J.B. and Davida, G.I. (1979) A Structured Design of Substitution-Permutation Encryption Networks. IEEE Transactions on Computers, C-28 (10). pp.747-753.

[25] Feistel, H. (1973) Cryptography and Computer Privacy. Scientific American. 228 (5). pp.15-23.

[26] Webster, A. and Tavares, S.E. (1985) On the Design of S-Boxes. In: Advances in Cryptology - CRYPTO '85. Springer-Verlag. pp.523-534.

[27] Heys, H.M. and Tavares, S.E. (1994) Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis. In: Proceedings of the 2nd Annual ACM Conference on Computer and Communications Security. ACM Press. pp.148-155.

[28] Meier, W. and Staffelbach, O. (1989) Nonlinearity Criteria for Cryptographic Functions. In: Advances in Cryptology - EUROCRYPT '89 Proceedings. Springer-Verlag. pp.549-562.

[29] Biham, E. and Shamir, A. (1991) Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 4 (1). pp.3-72.

[30] Youssef, A.M., Tavares, S.E. and Heys, H.M. (1996) A New Class of Substitution-Permutation Networks, SAC '96. In: Third Annual Workshop on Selected Areas in Cryptography. Kingston, Ontario. Queen's University. pp.132-147.

[31] Webster, A.F. and Tavares, S.E. (1996) On the design of S-Boxes. In: Advances in Cryptology: Proceedings of CRYPTO'85. Springer-Verlag. pp.523-534.

[32] Sivabalan, M., Tavares, S.E. and Peppard, L.E. (1993) On the Design of SP Networks from an Information Theoretic Point of View. In: Advances in Cryptology: Proceedings of CRYPTO '92. Springer-Verlag. pp.260-279.

[33] Biham, E. (1994) New Types of Cryptanalytic Attacks Using Related Keys. In: Advances in Cryptology - EUROCRYPT '93 Proceedings. Springer-Verlag. pp.398-409.

[34] Merkle, R.C. and Hellman, M. (1981) On the Security of Multiple Encryption. Communications of the ACM, 24 (7). pp.465-467.

[35] Nyberg, K. (1994) Differentially Uniform Mappings for Cryptography. In: T. Helleseth, Ed. Advances in Cryptology, Eurocrypt '93 Proceedings. Springer-Verlag.

[36] Biham, E. and Biryukov, A. (1995) How to Strengthen DES Using Existing Hardware. In: Advances in Cryptology – ASIACRYPT '94 Proceedings. Springer-Verlag.

[37] Matsui, M. (1996) New Structure of Block Ciphers with Provable Security Against Differential and Linear Cryptanalysis. In: Fast Software Encryption, 3rd International Workshop Proceedings. Springer-Verlag. pp.205-218.

[38] Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A. (1999) Handbook of Applied Cryptography, 4th Edition. CRC Press.

[39] Denning, D.E. (1984) Digital Signatures with RSA and Other Public-Key Cryptosystems. Communications of the ACM, 27 (4). pp.388-392.

[40] Meyer, C.H. and Matyas, S.M. (1982) Cryptography: A New Dimension in Computer Data Security. John Wiley & Sons.

[41] Davies, D.W. (1983) Some Regular Properties of the DES. In: Advances in Cryptology, Proceedings of Crypto 82. Plenum Press.

[42] J.H. Moore, J.H. and Simmons, G.J. (1987) Cycle Structure of the DES with Weak and Semi-Weak Keys. In: Advances in Cryptology-CRYPTO '86. Springer-Verlag. pp. 3-32.