Landmark Journal Articles Related to Cryptology

ADAMS, C. (1997). "Constructing Symmetric Ciphers Using the CAST Design." *Designs, Codes, and Cryptography,* **12** (3): 283-316. **[1]**

AKL, S. (1983). "Digital Signatures: A Tutorial Survey." *Computer,* **16** (2): 15-24 (February 1983). **[2]**

BELLOVIN, S.; & MERRITT, M. (1990). "Limitations of the Kerberos Authentication System." *Computer Communications Review,* **20** (5): 119-132 (October 1990). **[3]**

BELLOVIN, S. (1993). "Packets Found on an Internet." *Computer Communications Review,* **23** (3), 26-31 (J uly 1993). **[3]**

BELLOVIN, S.; & CHESWICK, W. (1994). "Network Firewalls." *IEEE Communications,* September 1994. **[3]**

BLUM, L; BLUM, M.; & SHUB, M. (1986). "A Simple Unpredictable Random Number Generator." *SIAM Journal on Computing,* Number 2, 1986. **[4]**

BOWLES, J.; & PELAEZ, C. (1992). "Bad Code." *IEEE Spectrum,* August 1992.

BRIGHT, HERBERT S.; & ENISON, RICHARD L. (1979). "Quasi-Random Number Sequences from A Long-Period TLP Generator with Remarks on Application to Cryptography." *Computing Surveys,* **11** (4), 357-370 (December 1979). **[5]**

CHAUM, DAVID (1985). "Security Without Identification: Card Computers to Make Big Brother Obsolete." *Communications of the ACM,* **28** (10), 1030-1044 (October 1985). URL: http://www.chaum.com/articles/Security_Wthout_Identification.htm **[6]**

CHAUM, DAVID (1989). "Online Cash Checks." *Advances in Cryptology EUROCRYPT '89* (J.J. Quisquater & J. Vandewalle, eds), Springer-Verlag, pp. 288-293. URL: http://www.chaum.com/articles/Online_Cash_Checks.htm **[6]**

CHAUM, DAVID (1992). "Achieving Electronic Privacy." *Scientific American,* , pp. 96-101 (August 1992). URL: http://www.chaum.com/articles/Achieving_Electronic_Privacy.htm **[6]**

Chaum, David. (1993). “Prepaid Smart Card Techniques. A Brief Introduction and Comparison.” URL: http://www.chaum.com/articles/Prepaid_Smart_Card_Techniques.htm **[6]**

Cocks, Clifford C. (1973). "A Note on Non-Secret Encryption." *CESG Report,* November 1973. URL: http://www.cesg.gov.uk/publications/media/nsecret/notense.pdf **[7]**

Cocks, Clifford C. (19??). "Split Knowledge Generation of RSA Parameters." *CESG Report*. URL: http://www.cesg.gov.uk/publications/media/math/rsa.pdf **[7]**

Cocks, Clifford C. (19??). "Split Generation of RSA Parameters with Multiple Participants." *CESG Report*. URL: http://www.cesg.gov.uk/publications/media/math/rsa2.pdf **[7]**

Coppersmith, D. (1994). "The Data Encryption Standard (DES) and Its Strength Against Attacks." *IBM Journal of Research and Development,* May 1994.

Diffie, W; & Hellman, M (1976). "New Directions in Cryptography." *IEEE Transactions on Information Theory,* November 1976. **[9]**

Diffie, W.; & Hellman, M. (1977). "Exhaustive Cryptanalysis of the NBS Data Encryption Standard." *IEEE Computer,* June 1977.

Diffie, W.; & Hellman, M. (1979). "Privacy and Authentication: An Introduction to Cryptography." *Proceedings of the IEEE,* March 1979.

Diffie, Whitfield (1988). "The First Ten Years of Public-Key Cryptography." *Proceedings of the IEEE,* May 1988.

ElGamal, Taher (1985). "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." *IEEE Transactions on Information Theory,* July 1985.

Ellis, J. H. (1970). “The Possibility of Secure Non-Secret Digital Encryption.” *CESG Report.* URL: http://www.cesg.gov.uk/publications/media/nsecret/possnse.pdf **[7]**

Ellis, J. H. (1987). “The History of Non-Secret Encryption.” *CESG Report.* URL: http://www.cesg.gov.uk/publications/media/nsecret/ellis.pdf **[7]**

Feistel, H/ (1973). "Cryptography and Computer Privacy." *Scientific American,* **228** (5): 15-23 (May 1973). **[11]**

Feistel, H.; Notz, W.; & Smith, J. (1975). "Some Cryptographic Techniques for Machine-to-Machine Data Communications." *Proceedings of the IEEE,* November 1975.

GARDNER, MARTIN (1977). "A New Kind of Cipher That Would Take Millions of Years to Break." *Scientific American,* (August 1977). Available on the Internet: http://www.fortunecity.com/emachines/e11/86/cipher1.html **[12]**

HEYS, H.; & TAVARES, S. (1995). "Avalanche Characteristics of Substitution-Permutation Encryption Networks." *IEEE Transactions on Computers,* September 1975.

JOHNSON, M. (1997). *Steganography.* URL: http://isse.gmu.edu/~njohnson/stegdoc/ [See also other documents at a closely related URL: http://isse.gmu.edu/~njohnson/Steganography/]

JURISIC, A.; & MENEZES, A. (1997). "Elliptic Curves and Cryptography." *Dr. Dobb's Journal,* April 1997. **[15]**

KALISKI, B.; & ROBSHAW, M. (1996). "Multiple Encryption: Weighing Security and Performance." *Dr. Dobb's Journal,* January 1996. **[16]**

KENT, S. (1977). "Encryption-Based Protection for Interactive User/Computer Protection. *Proceedings of the Fifth Data Communications Symposium,* September 1977.

KOHNFELDER, LOREN M. (1978). "Towards a Practical Public-Key Cryptosystem." Bachelor's Thesis, MIT. **[18]**

MATYAS, S. (1991). "Key Handling with Control Vectors." *IBM Systems Journal,* No2, 1991. **[19]**

MATYAS, W.; LE, A.; & ABRAHAM, D. (1991). "A Key-Management Scheme Based on Control Vectors." *IBM Systems Journal,* **30**.(2), 175-191. **[19]**

PARK, S.; & MILLER, K. (1988). "Random Number Generators: Good Ones Are Hard to Find." *Communications of the ACM,* October 1988.

RIVEST, R.; SHAMIR, A.; & ADELMAN, L. (1978). "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." *Communications of the ACM,* February 1978.

RIVEST, R. (1995). "The RC5 Encryption Algorithm." *Dr. Dobb's Journal,* January 1995.

ROBSHAW, M. (1995). *Block Ciphers.* RSA Laboratories Technical Report TR-601, August 1995.

ROBSHAW, M. (1996). *On Recent Results for MD2, MD4, and MD5.* RSA Laboratories Bulletin, 12 November 1996.

RUBIN, A. (1997). "An Experience Teaching a Graduate Course in Cryptography. *Cryptologia,* April 1997.

WILLIAMSON, M. J. (1974). “Non-Secret Encryption Using a Finite Field.” *CESG Report,* January 1974. URL: http://www.cesg.gov.uk/publications/media/nsecret/secenc.pdf **[7]**

WILLIAMSON, M. J. (1976). “Thoughts on Cheaper Non-Secret Encryption.” *CESG Report,* August 1976. URL: http://www.cesg.gov.uk/publications/media/nsecret/cheapnse.pdf **[7]**

YIN, Y. (1997). "The RC5 Encryption Algorithm: Two Years On." *CryptoBytes,* Winter 1997.

ZENG, KENCHENG; YANG, CHUNG-HUANG; WEI, DAH-YEA; & RAO, T.R.N (1991). "Pseudorandom Bit Generators in Stream-Cipher Cryptography.” *IEEE Computer,* **24** (2), 8-17 (February 1991). **[30]**

Please mail your suggestions for additions or changes to this list to: Abzugcx@JMU.edu