Landmark Journal Articles Related to Cryptology Library-Posted (Course Reserves) OR Available on the Internet

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]**

BENNETT, C.H.; BRASSARD, C.; & EKERT, A. (1992). "Quantum Cryptography." *Scientific American,* 269: 26-33 (October 1992).

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

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]**

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

DIFFIE, W; & HELLMAN, M (1976). "New Directions in Cryptography." *IEEE Transactions on Information Theory,* vol. IT-22,(November 1976), PP. 644-654. **[9]**

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]**

GREEN, B.F.; SMITH, J.E.K.; & KLEM, L. (1959). "Empirical Tests of an Additive Random Number Generator." *J. ACM,* 6 (4): 527-537. Available on the Internet: http://portal.acm.org/dl.cfm ; click on "Journals" and follow the appropriate links. **[19]**

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

LEWIS, T.G.; & PAYNE, W.H. (1973). "Generalized Feedback Shift Register Pseudorandom Number Algorithm." *J. ACM,* **20:** 456-468. (July 1973). Available on the Internet: http://portal.acm.org/dl.cfm ; click on "Journals" and follow the appropriate links. **[20]**

PARK, S.; & MILLER, K. (1988). "Random Number Generators: Good Ones Are Hard to Find." *Communications of the ACM,* October 1988. Available on the Internet: http://portal.acm.org/dl.cfm ; click on "Journals" and follow the appropriate links. **[21v]**

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]**