

A Short List of References on Cryptography

References

- [1] R. Anderson, and M. Roe. A5, 1994. Available at <http://jya.com/crack-a5.htm>
 - [2] Bluetooth CIG, Specification of the Bluetooth system, Version 1.1, February 22, 2001. Available from www.bluetooth.com.
 - [3] I. Mantin. Predicting and Distinguishing Attacks on RC4 Keystream Generator. *Eurocrypt Vol. 3494 of LNCS*, pp. 491-506, Springer-Verlag, 2005.
 - [4] G. Gong, K. C. Gupta, M. Hell, and Y. Nawaz, Towards a General RC4-like Keystream Generator, SKLOIS Conference on Information Security and Cryptology (CICS05), December 15-17, Beijing, China. Springer-verlag, 2006. (Download: <http://comsec.uwaterloo.ca>.)
 - [5] eSTREAM - *The ECRYPT Stream Cipher Project*, <http://www.ecrypt.eu.org/stream/>
 - [6] Y. Nawaz and G. Gong, WG: A family of stream ciphers with designed randomness properties, *Information Sciences*, Vol. 178, No. 7, April 1, 2008, pp. 1903-1916.
 - [7] National Bureau of Standards, Data Encryption Standard, FIPS Publication 46, U.S. Department of Commerce, 1977.
 - [8] National Institute of Standards and Technology, Advanced Encryption Standard, FIPS-197, <http://csrc.nist.gov/archive/aes/index.html>, 2000.
- General References for Cryptography:
- [9] D. Stinson, *Cryptography, Theory and Practice*, CRC Press, Second edition, 2000.
 - [10] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Second edition, Prentice Hall, 1999.
 - [11] J. Menezes and P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.