References

[BOCK 88] Peter Bocker, *ISDN The Integrated Services Digital Network Concepts, Methods, Systems*, Berlin, Springer-Verlag, 1988.

[DIFF 76] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644-654, Nov. 1976.

[DOD 5200] Department of Defense Standard DOD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

[ECMA 138] ECMA-138, *Security in Open Systems Data Elements and Service Definitions*, European Computer Manufacturers Association, Geneva, Dec. 1989.

[ECMA TR/46] ECMA TR/46, *Security In Open Systems, A Security Framework*, European Computer Manufacturers Association, Geneva, 1988.

[ECON 90] "Telecommunications Survey", *The Economist*, vol. 314, no. 7645, March 10, 1990., pp. SURVEY 33.

[FIPS 46] FIPS PUB 46-1, *Data Encryption Standard (DES)*, NBS, 1977.

[FIPS 81] FIPS PUB 81, *DES Modes of Operation*, NBS, 1980.

[FIPS 74] FIPS PUB 74 *Guidelines for Implementing and Using the NBS Data Encryption Algorithm*, NIST, 1980.

[FIPS 140-1] DRAFT FIPS PUB 140-1, *Security Requirements of Cryptographic Modules (DRAFT)*, NIST, July 13, 1990

[FIPS 146] FIPS PUB 146-1, *Government Open Systems Interconnection Profile (GOSIP)*, Version 2.0, NIST, October 1990.

[HAYK 88] Martha E. Haykin and Robert B. Warner, *Smart Card Technology: New Methods for Computer Access Control*, NIST Special Publication 500-157, 1988

[I.100] CCITT Recommendation I.100, *Preamble and General Structure of I-Series Recommendations*, 1988.

[I.320] Recommendation I.320, *ISDN Protocol Reference Model*, CCITT, 1988.

[I.324] Recommendation I.324, *ISDN Protocol Reference Model*, CCITT, 1988.

[ISO 7498] ISO 7498, *Information Processing Systems - Open System Interconnection - Basic Reference Model*, International Standards Organization, Geneva, 1984.

[ISO 7498-2] ISO 7498-2-1988(E), *International Standard Security Architecture*, International Standards Organization, Geneva, 1988.

[ISO 7776] ISO 7776:1986, *Information Processing Systems - Data Communications - High-Level Data Link Control Procedures - Description of the X.25 LAPB Compatible DTE Data Link Control Procedures*, International Standards Organization, Geneva, 1986.

[ISO 8073] ISO 8073:1984, *Information Technology - Open Systems Interconnection - Transport Protocol Specification,* International Standards Organization, Geneva.

[[ISO 8208] ISO 8208:1987, *Information Processing Systems - Data Communications - X.25 Packet Level Protocol for Data Terminal Equipment*, International Standards Organization, Geneva, 1987.

[ISO 9594-8] ISO/IEC 9594-8, *Information Technology - Open Systems Interconnection - The directory - Part 8: Authentication Framework,* International Standards Organization, Geneva.

[JTC1 1] ISO/IEC JT1/SC 21 N 4207, DPxxxx-2, *Information Processing Systems - Security Frameworks for Open Systems - Part 2: Authentication Framework*, draft standard dated Dec 12, 1989.

[MIYA 88] Shoji Miyaguchi, Akira Shiraishi and Akihiro Shimizu, “Fast Data Encipherment Algorithm FEAL-8,” *Review of the Electrical Communications Laboratories*, Nippon Telegraph and Telephone Corporation, vol.36, no. 4, 1988, pp.433-437.

[P802.10] IEEE P802.10, *Standard for Interoperable Local Area Network (LAN) Security, Part A - The Model*, Unapproved Draft, December 9, 1989.

[Q.931] CCITT Recommendation Q.931, “ISDN user-network interface layer 3 specification, ” *Blue Book*, 1988.

[RIVE 90] R. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[SDN.301] Specification SDN.301, *SDNS Secure Data Network System Security Protocol 3 (SP3)*, Revision 1.5, 1989-05-15, reprinted in NISTIR 90-4250, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols*, National Institute of Standards and Technology, February 1990.

[SDN.401] Specification SDN.401, *SDNS Secure Network Systems Security Protocol 4 (SP4)*, Revision 1.3, 1989-05-02, reprinted in NISTIR 90-4250, *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols*, National Institute of Standards and Technology, February 1990.

[STAL 89] William Stallings, *ISDN: An Introduction*, New York, Macmillan, 1989.

[T1.607] T1.607-1990, *American National Standard for Telecommunications - Digital Subscriber Signalling System NO.1 - Layer 3 Signalling Specification for Circuit Switched Bearer Service*, ANSI, 1990. (USA national standard corresponding to [Q.931].)

[VERM 90] Pramode K. Verma, ed., *ISDN Systems, Architecture, Technology and Applications*, Englewood Cliffs, NJ, Prentice Hall, 1990.

[X.25] Recommendation X.25, "Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit," *Blue Book*, ITU, 1988.