

ISO 9979/0004

Application for Registration in ISO 9979 Register

1. ISO Entry Name: { iso standard 9979 des (4) }
2. Proprietary Name: Data Encryption Standard (DES) Algorithm
3. Intended Applications: Authentication; Confidentiality; Data Integrity
4. Cryptographic Interface Parameters
 - a. input block: 64 bits
 - b. output block: 64 bits
 - c. keylength: 64 bits (56 bits active; 8 bits parity)
 - d. initialising vector: 64 bits
 - e. controls: encrypt/decrypt; input data; output data; input key; mode select
 - f. status indicators: parity error; encrypt done; decrypt done; input done; output done; error(s)
5. Test Words: See FIPS 81 and NBS Special Publication 500-21
6. Name of Sponsoring Organization: National Communications System
NT
701 South Court House Road
Arlington, VA 22204-2198
USA
Tel: +1 (703) 692-2124
7. Date of Registration: to be assigned by NCC - 3 September 1994
8. National Standard: FIPS 46-2 and ANSI X3.92-1981
9. U.S. Export License and Patent Restrictions: Yes

References: FIPS 46-2 and ANSI X3.92-1981

Description of Algorithm: See FIPS 46-2
12. Modes of Operation: See FIPS 81
13. Other Information: None.