

ID MOS Digital I.P. SHORTFORM

IM110: Data Encryption standard

PRODUCT DESCRIPTION

This The D.E.S. is a FIPS approved cryptographic algorithm. Encrypting data converts it to an unintelligible form called cipher.

Decrypting cipher converts the data back to its original form called plaintext.

Enciphering and deciphering operations are based on up to 3 binary numbers called "keys"

FEATURES

- 3 implementations of the DES algorithm : single DES (1 cryptographic key), triple DES EDE-2 (2 cryptographic keys), triple DES EDE-3 (3 cryptographic keys)
- Automatic encrypting/decrypting by entering plain word / cipher word.
- Distinct addresses for reading and writing
- Enciphering/Deciphering duration :
 - single DES : 16 clock periods
 - DES EDE-2 : 36 clock periods
 - DES EDE-3 : 54 clock periods
- Data bus can be 8, 16, 32 or 64-bit length

BLOCK DESCRIPTION

