Am9568

Data Ciphering Processor
(DCP)

DISTINCTIVE CHARACTERISTICS

- **Encrypts and decrypts data**
  Implements National Bureau of Standards Data Encryption Standard (DES) algorithm
- **Throughput over 1.5M bytes per second**
  Operates at data rates fast enough for disk controllers, high-speed DMA, telecommunication channels
- **Supports three ciphering options**
  Electronic Code Book for disk applications, Cipher Block Chain for high-speed telecommunications, and Cipher Feedback for low-to-medium speed, byte-oriented communications
- **Three separate key registers on one chip**
  Separate registers for encryption key, decryption key and master key improve system security and throughput by eliminating need to reload keys frequently.
- **Three separate data ports provide flexible interface, improved security**
  The DCP utilizes a Master Port, Slave Port and Key Port. Functions of the three ports can be programmed by the user to provide for simple interface to iAPX86 and Am2900 systems and to provide total hardware separation of encrypted data, clear data and keys.

GENERAL DESCRIPTION

The Am9568 Data Ciphering Processor is an N-channel silicon gate LSI product containing the circuitry necessary to encrypt and decrypt data using the National Bureau of Standards Encryption Algorithm. It is designed to be used in a variety of environments, including dedicated controllers, communication concentrators, terminals and peripheral task processors in general processor systems.

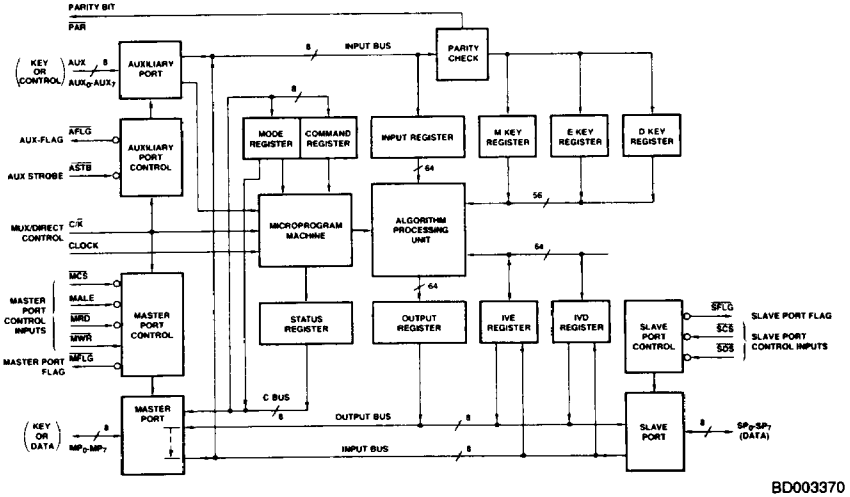
The DCP provides a high throughput rate using Cipher Feedback, Electronic Code Book or Cipher Block Chain operating modes. Separate ports for key input, clear data and enciphered data enhance security.

The system communicates with the DCP using commands entered in the Master Port and through auxiliary control lines. Once set up, data can flow through the DCP at high speeds because input, output and ciphering activities are all performed concurrently. External DMA control can easily be used to enhance throughput in some system configurations.

This device is designed to interface directly to the iAPX86, 88 CPU bus and, with a minimum of external logic, to the 2900 and 8051 families of processors.

BLOCK DIAGRAM

NTExport of this device from the United States is subject to control by the U.S. Department of State.



BD003370

Publication #	Rev.	Amendment
05178	B	/0

Issue Date: April 1985