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

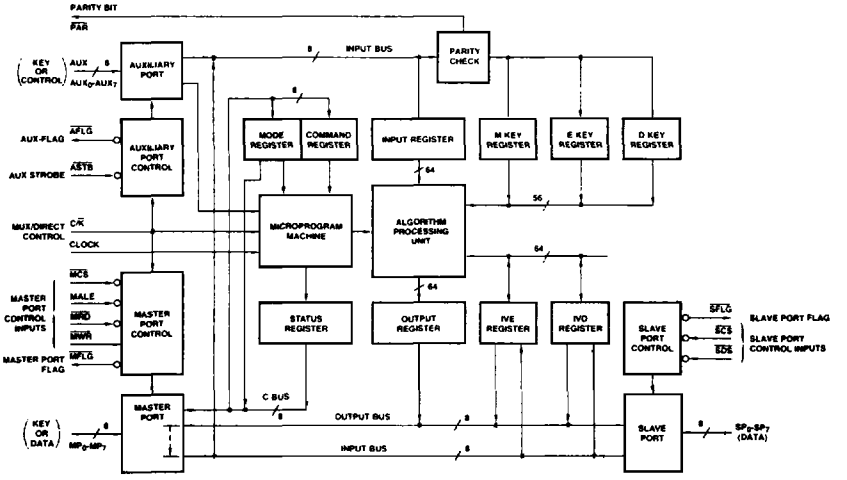
The Am9568 Data Ciphering Processor is an N-channel silicon gate LSI product containing the circuitry necessary to encrypt and decrypt data using the National Bureau of Standards Encryption Algorithm. It is designed to be used in a variety of environments, including dedicated controllers, communication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



BD003370

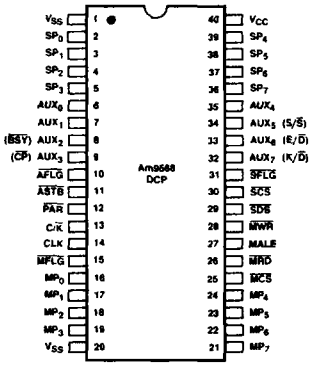
RELATED PRODUCTS

Part No.	Description
Am9518/Z8068	Data Ciphering Processor

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

Refer to page 7-1 for Essential Information on Military Devices

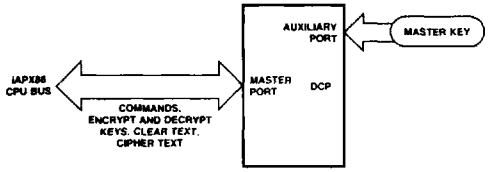
CONNECTION DIAGRAM
Top View



CD005200

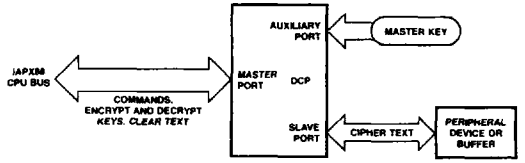
Note: Pin 1 is marked for orientation

DCP DATA FLOW OPTIONS



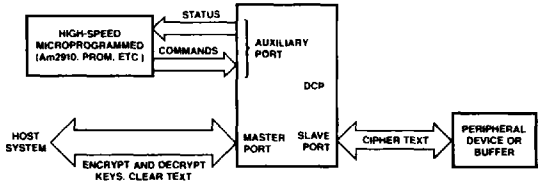
AF002480

Single-Port Configuration, Multiplexed Control



AF002490

Dual-Port Configuration, Multiplexed Control

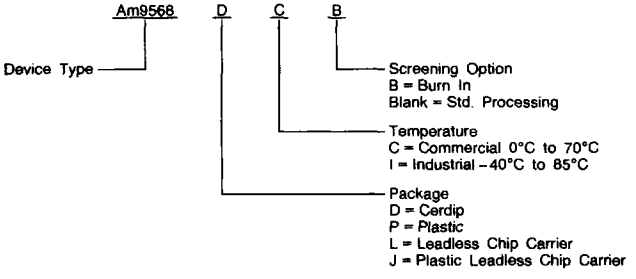


AF002500

Dual-Port Configuration, Direct Control

ORDERING INFORMATION

AMD products are available in several packages and operating ranges. The order number is formed by a combination of the following: Device number, speed option (if applicable), package type, operating range and screening option (if desired).



Valid Combinations	
Am9568	DC, DCB, PC, DI, PCB, PI, PIB, DIB, LC, LCB, LI, LIB

Valid Combinations

Consult the local AMD sales office to confirm availability of specific valid combinations, check for newly released valid combinations and/or obtain additional data on AMD's standard military grade product.

Refer to page 7-1 for Essential Information on Military Devices

PIN DESCRIPTION

Pin No.	Name	I/O	Description
40	V_{CC}		+5 Volt Power Supply.
1, 20	V_{SS}		Ground (2 pins).
14	CLK	I	(Clock, TTL levels). An external timing source is input via the CLK pin. The Master and Slave Port Data Strobe signals ($\overline{MRD}$, $\overline{MWR}$, $\overline{SDS}$) must change synchronously with this clock input, as must AUX_5-S/$\overline{S}$ in Direct Control Mode (C/$\overline{K}$ HIGH). In addition, the Auxiliary, Master and Slave Port Flag outputs ($\overline{AFLG}$, $\overline{MFLG}$ and $\overline{SFLG}$) will change synchronously with the clock.
13	C/$\overline{K}$	I	(Control/Key Mode Control). This input is the primary control over the operating characteristics of the DCP. A LOW input on C/$\overline{K}$ places the DCP into Multiplexed Control Mode, enabling programmed access to internal registers through the Master Port and enabling input of keys through the Auxiliary Port. A HIGH input on C/$\overline{K}$ specifies operation in Direct Control Mode, wherein several of the Auxiliary Port pins become direct control/status signals which can be driven/sensed by high-speed controller logic (such as the Am29116 or Am2901/Am2903-based processors), and access to internal registers through the Master Port is limited to the Input or Output Register.
16-19 24-21	MP_0-MP_7	I/O	(Master Port Bus). These eight bidirectional lines are used to specify internal register addresses in Multiplexed Control Mode (see C/$\overline{K}$) and to input and output data. The Master Port provides software access to the Status, Command and Mode Registers, as well as the Input and Output Registers. The three-state Master Port outputs will be enabled only when the Master Port is selected by Master Port Chip Select ($\overline{MCS}$) LOW and when Master Port Read ($\overline{MRD}$) is strobed LOW. MP_0 is the low-order bit. Data and key information are entered into this port with the most significant byte in first.
25	$\overline{MCS}$	I	(Master Port Chip Select). This active LOW input signal is used to select the Master Port. In Multiplexed Control Mode (C/$\overline{K}$ low), the level on $\overline{MCS}$ is latched internally on the falling edge of Master Port Address Latch Enable (MALE). This latched level is retained as long as MALE is LOW; when MALE is HIGH, the latch becomes transparent and the internal signal will follow the $\overline{MCS}$ input. In Direct Control Mode (C/$\overline{K}$ HIGH), no latching of Master Port Chip Select occurs; the level on $\overline{MCS}$ is passed directly to the internal select circuitry irrespective of state of Master Port Address Latch Enable (MALE).
27	MALE	I	(Master Port Address Latch Enable). In Multiplexed Control Mode (C/$\overline{K}$ low), an active HIGH signal on this pin indicates the presence of valid address and chip select information at the Master Port. This information will be latched internally on the falling edge of Address Latch Enable. When C/$\overline{K}$ is HIGH (Direct Control Mode), MALE may be HIGH or LOW without affecting DCP operation.
26	$\overline{MRD}$	I	(Master Port Read Data). This active LOW input is used in coincidence with a valid Master Port Chip Select ($\overline{MCS}$), to indicate that data is to be placed on MP_0-MP_7 for an output operation. Master Port Read ($\overline{MRD}$) and Master Port Write ($\overline{MWR}$) are normally mutually exclusive; if both go LOW simultaneously, the DCP is reset to ECB Mode and all flags go inactive.
28	$\overline{MWR}$	I	(Master Port Write). This input signal indicates to the DCP that valid data is present on MP_0-MP_7 for an input operation. The trailing edge of $\overline{MWR}$ latches the data in the selected internal register. If $\overline{MWR}$ and $\overline{MRD}$ both go LOW simultaneously, the DCP is reset.
15	$\overline{MFLG}$	O	(Master Port Flag). This active LOW flag is used to indicate the need for a data transfer into or out of the Master Port during normal ciphering operation. Depending upon control bits written to the Mode Register (see Register Description), the Master Port will be associated with either the Input Register or the Output Register. If data is to be transferred through the Master Port to the Input Register, the $\overline{MFLG}$ reflects the contents of the Input Register; after any Start command is entered, $\overline{MFLG}$ will go active (LOW) whenever the Input Register is not full. $\overline{MFLG}$ is forced HIGH by any command other than a Start. Conversely, if the Master Port is associated with the Output Register, $\overline{MFLG}$ reflects the contents of the Output Register (except in Single Port configuration – see Detailed Description). $\overline{MFLG}$ will go active (LOW) whenever the Output Register is not empty. In Single Port Configuration, the Master Port Flag reflects the contents of the Input Register, while the Slave Port Flag ($\overline{SFLG}$, see below) is associated with the Output Register.
2-5 39-36	SP_0-SP_7	I/O	(Slave Port Bus). The Slave Port provides a second data input/output interface to the DCP, allowing overlapped input, output and ciphering operations. The tri-state Slave Port outputs will be driven only when Slave Port Chip Select ($\overline{SCS}$) and Slave Port Data Strobe ($\overline{SDS}$) are both LOW and $\overline{SFLG}$ = 0, and the internal Port Control Configuration allows output to the Slave Port. SP_0 is the LOW order bit. Data entered or retrieved through this port is the most significant byte in/out first.
30	$\overline{SCS}$	I	(Slave Port Chip Select). This active LOW signal is logically combined with Slave Port Data Strobe ($\overline{SDS}$) to facilitate Slave Port data transfers in a bus environment. $\overline{SCS}$ is not latched internally, and may be tied permanently LOW without impairing Slave Port operation.
29	$\overline{SDS}$	I	(Slave Port Data Strobe). This active LOW input, in coincidence with Slave Port Chip Select ($\overline{SCS}$) LOW, indicates to the DCP that valid data is on the SP_0-SP_7 lines for an input operation, or that data is to be driven onto the SP_0-SP_7 lines for output. The direction of data flow is determined by control bits in the Mode Register (see Register Description).
31	$\overline{SFLG}$	O	(Slave Port Flag). This active LOW output indicates the state of either the Input Register or the Output Register, depending on control bits in the Mode Register. In Single Port Configuration, $\overline{SFLG}$ will go active whenever the Output Register is not empty during normal processing. In Dual Port Configuration, $\overline{SFLG}$ will reflect the content of whichever register is associated with the Slave Port. If the Input Register is assigned to the Slave Port, $\overline{SFLG}$ will go active whenever the Input Register is not full, once any of the Start commands has been entered; $\overline{SFLG}$ will be forced inactive if any other command is entered. Conversely, if the Slave Port is assigned to the Output Register, $\overline{SFLG}$ will go active whenever the Output Register is not empty.

Refer to page 7-1 for Essential Information on Military Devices

Pin Description (Cont.)

Pin No.	Name	I/O	Description
6-9 35-32	AUX_0-AUX_7	I/O	(Auxiliary Port Bus, Bidirectional). When the DCP is operated in Multiplexed Control Mode (C/$\overline{K}$ LOW), these eight lines form a key-byte input port which may be used to enter the Master and Session Keys. In fact, this port is the only path available for entering the Master Key. (session keys may alternatively be entered via the Master Port.) AUX_0 is the low-order bit and is considered to be the parity bit in key bytes. The most significant byte is entered first. When the DCP is operated in Direct Control Mode, (C/$\overline{K}$ HIGH), the Auxiliary Port's key-entry function is disabled and five of the eight lines become direct control/status lines for interfacing to high-speed microprogrammed controllers. In this case, AUX_0, AUX_1 and AUX_4 have no function (they may be tied HIGH), and the other pins are defined as below.
34	AUX_5-S/$\overline{S}$	I	(Start/$\overline{Stop}$). When this pin goes LOW (Stop),below the DCP will follow the sequence that would normally occur were a Stop command to be entered. Conversely, when this pin goes HIGH, a sequence equivalent to a Start Encryption or Start Decryption command will be followed. At the time AUX_5-S/$\overline{S}$ goes HIGH, the level on AUX_6-E/$\overline{D}$ (see below) selects either the Start Encryption or Start Decryption interpretation.
32	AUX_7-K/$\overline{D}$	I	(Key/$\overline{Data}$). When this signal goes HIGH, the DCP initiates a key-data input sequence as if a Load Clear E (or D) Key Through Master Port command had been entered. The level on AUX_6-E/$\overline{D}$ will determine whether the subsequently entered clear-key bytes are written into the E Key Register (E/$\overline{D}$ HIGH) or the D Key Register (E/$\overline{D}$ LOW). AUX_7-K/$\overline{D}$ and AUX_5-S/$\overline{S}$ are mutually exclusive control lines; when one goes active (HIGH), the other must be and remain inactive (LOW) until the first returns to an inactive state. In addition, both lines must be inactive (LOW) whenever a transition occurs on C/$\overline{K}$ (entering or exiting Direct Control Mode).
33	AUX_6-E/$\overline{D}$	I	(Encrypt/$\overline{Decrypt}$). When AUX_5-S/$\overline{S}$ goes HIGH, initiating a normal data ciphering operation, this input specifies whether the ciphering algorithm is to encrypt (E/$\overline{D}$ HIGH) or decrypt (LOW). When AUX_7-K/$\overline{D}$ goes HIGH, initiating entry of key bytes, the level on AUX_6-E/$\overline{D}$ specifies whether the bytes are to be written into the E Key Register (E/$\overline{D}$ HIGH) or the D Key Register (E/$\overline{D}$ LOW). The AUX_6-E/$\overline{D}$ input is not latched internally, and must be held constant whenever one or more of AUX_5-S/$\overline{S}$, AUX_7-K/$\overline{D}$, AUX_2-$\overline{BSY}$, or AUX_3-$\overline{CP}$ are active. Failure to maintain the proper level on AUX_6-E/$\overline{D}$ during loading or ciphering operations will result in scrambled data in the internal registers.
8	AUX_2-$\overline{BSY}$	O	(Busy). This active-low status output gives a hardware indication that the ciphering algorithm is in operation. AUX_2-$\overline{BSY}$ is driven by the BSY bit in the Status Register (see Register Description), such that when the BSY bit is "1" (active), AUX_2-$\overline{BSY}$ is LOW.
9	AUX_3-$\overline{CP}$	O	(Command Pending). This active-low status output gives a hardware indication that the DCP is ready to accept input of key bytes following a LOW-to-HIGH transition on AUX_7-K/$\overline{D}$. AUX_3-$\overline{CP}$ is driven by the CP bit in the Status Register, such that when the CP bit is "1" (active), AUX_3-$\overline{CP}$ is LOW.
11	$\overline{ASTB}$	I	(Auxiliary Port Strobe). The rising (trailing) edge of $\overline{ASTB}$ strobes the key data on pins AUX_0-AUX_7 into the appropriate internal key register in Multiplexed Control Mode (C/$\overline{K}$ LOW). This input is ignored unless $\overline{AFLG}$ and C/$\overline{K}$ are both LOW. One byte of key data is entered on each $\overline{ASTB}$, most significant byte first.
10	$\overline{AFLG}$	O	(Auxiliary Port Flag). This active LOW output signal indicates that the DCP is expecting key data to be entered on pins AUX_0-AUX_7. This can occur only when C/$\overline{K}$ is LOW and a Load Key Through AUX Port command has been entered. $\overline{AFLG}$ will remain active (LOW) during input of all eight bytes and will go inactive with the leading edge of the eighth strobe ($\overline{ASTB}$).
12	$\overline{PAR}$	O	(Parity). The DCP checks all key bytes for correct (odd) parity as they are entered through either the Master Port (Multiplexed or Direct Control Mode) or the Auxiliary Port (Multiplexed Control Mode only). If any key byte contains even parity, the PAR bit in the Status Register is set to "1" and $\overline{PAR}$ goes LOW. (See Parity Checking of Keys.) Least significant bit of key data is the parity.

DETAILED DESCRIPTION

The overall design of the DCP, as shown in the block diagram on the next page, is optimized for high data throughput. Data bytes can be transferred through both the Master and Slave Ports, and key bytes can be written through both the Auxiliary and Master Ports. Three 8-bit buses, Input, Output and C Bus, carry data and key bytes between the ports and the internal registers. Three 56-bit, write-only key registers are provided for the Master (M) Key, the Encryption (E) Key and the Decryption (D) Key. Parity checking is provided on incoming key bytes. Two 64-bit registers are provided for Initializing Vectors (IVE and IVD) required for chained (feedback) ciphering modes. Three 8-bit registers (Mode, Command and Status) are accessible through the Master Port for interfacing to a host microprocessor, such as the iAPX86.

Algorithm Processing

The DCP's Algorithm Processing Unit (see the block diagram) is designed to encrypt and decrypt data according to the National Bureau of Standards Date Encryption Standard (DES), as specified in Federal Information Processing Standards Publication 46.

The DES specifies a method for encrypting 64-bit blocks of clear data ("plain text") into corresponding 64-bit blocks of "cipher text." The DCP offers three ciphering methods selected by the Cipher Type field of the Mode Register: Electronic Code Book (ECB), Cipher Block Chain (CBC) and Cipher Feedback (CFB). These methods are implemented in accordance with Federal Information Processing Standards Publication 46. Electronic Code Book (ECB) is a straightforward implementation of the DES: 64 bits of clear data in, 64 bits of cipher text out, with no cryptographic dependence between blocks. Cipher Block Chain (CBC) also operates on blocks of 64 bits, but includes a feedback step which chains consecutive blocks so that repetitive data in the plain text (such as ASCII blanks) does not yield repetitive cipher text. CBC also provides an error extension characteristic valuable in protecting against fraudulent data insertions and deletions. Cipher Feedback (CFB) is an additive stream cipher method in which the DES generates a pseudorandom binary stream which is then exclusive-OR'd with the clear data to form the cipher text. The cipher text is then fed back to form a portion of the next DES input block. The DCP implements 8-bit cipher feedback with one byte wide data input, output, and feedback

Refer to page 7-1 for Essential Information on Military Devices

paths. This method is useful for low speed, character-at-a-time serial communications.

Multiple Key Registers

The DCP provides the necessary registers to implement a multiple-key or Master Key system. In such an arrangement, a single Master Key, stored in the DCP M Key Register, is used only to encrypt session keys for transmission to remote DES equipment, and to decrypt session keys received from such equipment. The M Key Register may be loaded (with plain text) only through the Auxiliary Port, using the Load Clear M Key command. (See Commands.)

In addition to the M Key Register, the DCP contains two session key registers: the E Key Register, used to encrypt clear text, and the D Key Register, used to decrypt cipher text.

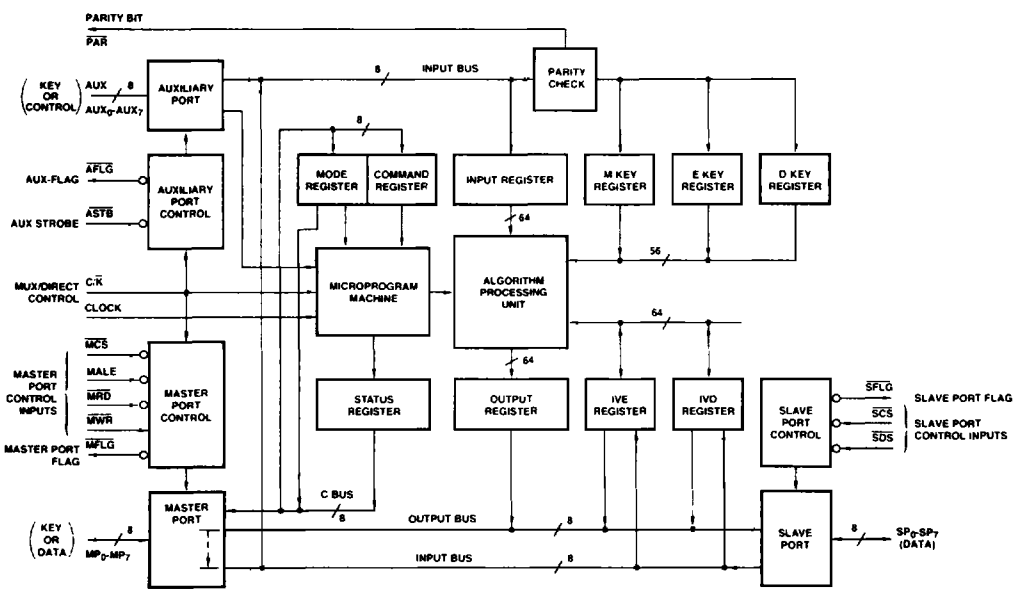
All three registers are loaded by writing commands like Load Clear E Key through Master Port into the Command Register, and then writing the eight bytes of key data to the port when the Command Pending = "1" in the Status Register. (See Commands.)

Operating Modes: Multiplexed Control vs. Direct Control

The DCP can be operated in either of two basic interfacing modes determined by the logic level on the C/$\overline{K}$ input pin. In Multiplexed Control Mode (C/$\overline{K}$ LOW), the DCP is internally configured to allow a host CPU to directly address five of the internal Control/Status/Data Registers and thereby control the device via mode and command values written to these registers. Also, in Multiplexed Control Mode, the Auxiliary Port is enabled for key-byte input.

If the logic level on C/$\overline{K}$ is brought HIGH, the DCP enters Direct Control Mode, and the Auxiliary Port pins are converted into direct hardware status or control signals that are capable of instructing the DCP to perform a functionally complete subset of its cipher processing at very high throughputs. This operating mode is particularly well-suited for ciphering data for high-speed peripheral devices, such as magnetic disk or tape.

Am9568 DCP BLOCK DIAGRAM



BD003370

Data Flow

Bits M_2, M_3 of the Mode Register control the flow of data into and out of the DCP through the Master and Slave Ports. Three basic configurations are provided: Single Port and two Dual Port configurations.

Single Port Configuration

The simplest configuration occurs when the Mode Register configuration bits are set to Master Port only. Under this operating configuration the Encrypt/Decrypt bit (M_4) controls the processing of data. Data to be encrypted or decrypted is written to the Master Port Input Register address. To facilitate monitoring of the Input Register status, the $\overline{MFLG}$ signal goes LOW when the Input Register is not full. Data is read by the host CPU through the Master Port Output Register address. $\overline{SFLG}$ goes LOW when the Output Register is not empty. Thus, $\overline{MFLG}$ redefined as a Master Input Flag and $\overline{SFLG}$ is redefined as a Master Output Flag.

Dual Port, Master Port Clear Configuration

In the Dual Port configurations, both the Master and Slave Ports are used for data entry and removal. In the Master Port Clear configuration, clear text for encryption can be entered only through the Master Port, and clear text resulting from decryption can be read out only through the Master Port. Cipher text can be handled only through the Slave Port. The actual direction of data flow is controlled either by the Encrypt/Decrypt bit (M_4) in the Mode Register or by the Start Encryption or Start Decryption commands. If encryption is specified, clear data will flow through the Master Port to the

Refer to page 7-1 for Essential Information on Military Devices

Input Register, and cipher data will be available at the Slave Port when it is ready to be read out of the Output Register. For decryption, the process is reversed: cipher data being written to the Input Register through the Slave Port and clear data being read from the Output Register through the Master Port.

Dual Port, Slave Port Clear Configuration

This configuration is identical to the previously described Dual Port, Master Port Clear configuration, except that the direction of ciphering is reversed. That is, all data flowing in or out of the Master Port is cipher text, and all data at the Slave Port is clear text.

Master Port Read/Write Timing

The DCP's Master Port is designed to operate with multiplexed address-data buses, such as the 8086/8088 processors. Several features of the Master Port logic should be stressed.

- The level on Master Port Chip Select ($\overline{MCS}$) is latched internally on the falling (trailing) edge of Master Port Address Latch Enable (MALE), thus relieving external address decode circuitry of the responsibility for latching chip select at address time.
- The levels on MP_1, MP_2 are also latched internally on the falling edge of MALE and are subsequently decoded to enable reading and writing of the DCP's internal registers (Mode, Command, Status, Input and Output). Again, this eliminates the need for external address latching and decoding.
- Data transfers through the Master Port are controlled by the levels and transitions on Master Port Read ($\overline{MRD}$) and Master Port Write ($\overline{MWR}$). Note that data transfers do not disturb either the chip-select or address latches, so that once the DCP and a particular register have been selected, any number of reads or writes of that register can be accomplished without intervening address cycles. This feature could greatly speed up loading keys and data, given the necessary transfer control external to the DCP.

Loading Keys and Initializing Vector (IV) Registers

Because the key and initializing vector registers are not directly addressable through any of the DCP's ports, keys and vector data must be loaded (and, in the case of vectors, read out) via "command data sequences" (see Commands). Most of the commands recognized by the DCP are of this type: a Load or Read command is written to the Command Register through the Master Port; the command processor responds by asserting the Command Pending output; the user then either writes eight bytes of key or vector data through the Master or Auxiliary Port, as appropriate to the specific command, or reads eight bytes of vector data from the Master Port.

In Direct Control Mode, only the E Key and D Key registers can be loaded; the M Key and IV Registers are inaccessible. Loading the E and D Key registers is accomplished by asserting the proper state on the AUX_6-E/$\overline{D}$ input (HIGH for E Key, LOW for D Key) and then raising the AUX_7-K/$\overline{D}$ input, indicating that key loading is required. The command processor will attach the proper Key Register to the Master Port and assert the AUX_3-$\overline{CP}$ (Command Pending) signal (active-low). The eight key bytes may then be written to the Master Port. In Multiplexed Control Mode, all key and vector registers are writable, and all but the Master (M) Key Register may be loaded with encrypted, as well as clear, data. If the operation is a Load Encrypted command, the subsequent data written to the Master or Auxiliary Port (as appropriate) is routed first to the Input Register and decrypted before being written into the specified Key or Vector Register.

Parity Checking of Keys

Key bytes are considered to contain seven bits of key information and one parity bit. By DES designation, the low-order bit is the parity bit. The parity checking circuit is enabled whenever a byte is written to one of three Key Registers. The output of the parity detection circuit is connected to pin $\overline{PAR}$, and the state of this pin is reflected in Status Register bit PAR (S_3). Status Register bit PAR goes to "1" whenever a byte with even parity (an even number of "1"s) is detected. In addition to the PAR bit, the Status Register has a Latched Parity Bit (LPAR, S_4) which is set to "1" whenever the Status Register PAR bit goes to "1." Once set, the LPAR bit is not cleared until a reset occurs or a new Load Key command is issued.

When an encrypted key is entered, the parity detect logic operates only after the decrypted key is available. The encrypted data is not checked for parity. The $\overline{PAR}$ signal will reflect the state of the decrypted bytes on a byte-to-byte basis, as they are clocked through the parity check logic on their way to the Key Register. Thus, the time $\overline{PAR}$ indicates the status of a byte of decrypted key data may be as short as four clock cycles. The LPAR bit in the Status Register will indicate if any erroneous bytes of data were entered.

Initialization

The DCP can be reset in several ways:

1. By the "Software Reset" command,
2. By a hardware reset, which occurs whenever both $\overline{MRD}$ and $\overline{MWR}$ go LOW simultaneously for 1 clock,
3. By writing to the Mode Register, and
4. By aborting any command.

All these sequences are the same internally, except that loading the Mode Register does not subsequently reset the Mode Register.

Once a reset process starts, the DCP is unable to respond to further commands for approximately five clock cycles.

If a power-up hardware reset is used, the leading edge of the reset signal should not occur until approximately 1 ms after V_{CC} has reached normal operating voltage. This delay time is needed for internal signals to stabilize.

Register Description

The registers in the DCP which can be directly addressed through the Master Port are shown with their addresses in Figure 1. A brief description of these registers and others not directly accessible is given below.

Command Register

Data written to the 8-bit, write-only Command Register through the Master Port is interpreted as an instruction. A detailed description of each command is given under Commands, and the commands and their binary representations are summarized in Figure 2.

Status Register

The bit assignments in the read-only Status Register are shown in Figure 4. The $\overline{PAR}$, $\overline{AFLG}$, $\overline{SFLG}$ and $\overline{MFLG}$ bits indicate the status of the like-named output pins, as do the bits Busy and Command Pending when the DCP is in Direct Control Mode (C/$\overline{K}$ HIGH). In each case, the output signal will be active LOW when the corresponding status bit is a "1." The Parity bit indicates the parity of the most recently entered key byte. The LPAR bit, on the other hand, indicates whether any key byte with even parity has been encountered since the last Reset or Load Key command.

The Busy bit will be a "1" whenever the ciphering algorithm unit is actively encrypting or decrypting data, either as a

Refer to page 7-1 for Essential Information on Military Devices

response to a command such as Load Encrypted Key (in which case the Command Pending bit will be a "1"), or in the ciphering of regular text (indicated by the Start/Stop bit being a "1"). The Busy bit will remain a "1" even after ciphering is complete if the ciphered data cannot be transferred to the Output Register because that register still contains output from a previous ciphering cycle. Busy will be "0" at all other times, including if no ciphering is possible because no data has been written to the Input Register.

The Command Pending bit will be set to "1" by any command whose execution requires the transfer of data to or from a non-addressable internal register, such as when writing key bytes to the E Key Register or reading bytes from the IVE Register. Thus, Command Pending will be set following all commands except the three Start commands, the Stop command and the Software Reset command. Command Pending will return to "0" after all eight bytes have been transferred following Load Clear, Read Clear or Read Encrypted commands, and after data has been transferred, decrypted and loaded into the desired register following Load Encrypted commands.

The Start/Stop bit is set to "1" when one of the Start commands is entered, and is reset to "0" whenever a reset occurs or when a new command other than a Start is entered.

C/$\overline{K}$	MP2	MP1	$\overline{MRD}$	$\overline{MWR}$	$\overline{MCS}$	Register Addressed
0	X	0	1	0	0	Input Register
0	X	0	0	1	0	Output Register
0	0	1	1	0	0	Command Register
0	0	1	0	1	0	Status Register
0	1	1	X	X	0	Mode Register
X	X	X	X	X	1	No Register Accessed
1	X	X	1	0	0	Input Register
1	X	X	0	1	0	Output Register

Figure 1. Master Port Register Addresses

Hex Code	Command
90	Load Clear M Key through Auxiliary Port
91	Load Clear E Key through Auxiliary Port
92	Load Clear D Key through Auxiliary Port
11	Load Clear E Key through Master Port
12	Load Clear D Key through Master Port
B1	Load Encrypted E Key through Auxiliary Port
B2	Load Encrypted D Key through Auxiliary Port
31	Load Encrypted E Key through Master Port
32	Load Encrypted D Key through Master Port
85	Load Clear IVE through Master Port
84	Load Clear IVD through Master Port
A5	Load Encrypted IVE through Master Port
A4	Load Encrypted IVD through Master Port
8D	Read Clear IVE through Master Port
8C	Read Clear IVD through Master Port
A9	Read Encrypted IVE through Master Port
A8	Read Encrypted IVD through Master Port
39	Encrypt with Master Key
41	Start Encryption
40	Start Decryption
C0	Start
E0	Stop
00	Software Reset

Figure 2. Command Codes in Multiplexed Control Mode

Pins				Command initiated
C/$\overline{K}$	AUX7 - K/$\overline{D}$	AUX6 - E/$\overline{D}$	AUX5 - S/$\overline{S}$	
H	L	L	↑	Start Decryption
H	L	H	↑	Start Encryption
H	L	X	↓	Stop
H	↑	L	L	Load D Key Clear through Master Port
H	↑	H	L	Load E Key Clear through Master Port
H	↓	X	L	End Load Key Command
H	H	X	H	Not Allowed
L	Data	Data	Data	AUX Pins Become Key-Byte Inputs

Figure 3. Implicit Command Sequences in Direct Control Mode

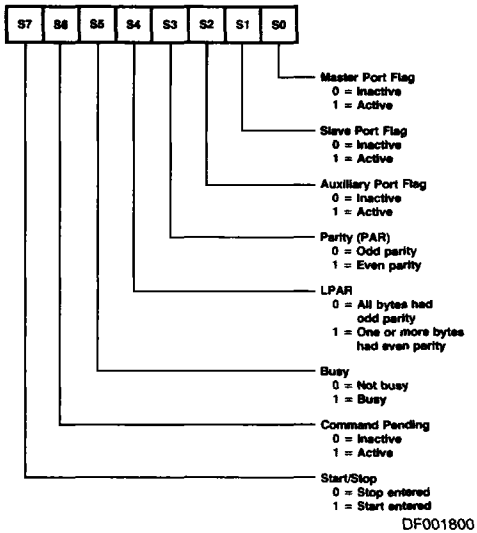


Figure 4. Status Register Bit Assignments

Mode Register

Bit assignments in this 5-bit read/write register are shown in Figure 5. The Cipher Type bits (M_1, M_0) indicate to the DCP which ciphering algorithm is to be used. On reset, the Cipher Type defaults to Electronic Code Book.

Configuration bits (M_3, M_2) indicate which data ports are to be associated with the Input and Output Registers and flags. When these bits are set to the Single Port, Master Only configuration (M_3, M_2 = 10), the Slave Port is disabled, and no manipulation of Slave Port Chip Select ($\overline{SCS}$) or Data Strobe ($\overline{SDS}$) can result in data movement through the Slave Port; all data transfers are accomplished through the Master Port. Both $\overline{MFLG}$ and $\overline{SFLG}$ are used in this configuration; $\overline{MFLG}$ gives the status of the Input Register and $\overline{SFLG}$ the Output Register.

When the Configuration Bits are set to one of the Dual Port configurations (M_3, M_2 = 00 or 01), both the Master and Slave

Refer to page 7-1 for Essential Information on Military Devices

Ports are available for input and output. When M_3, M_2 = 01 (the default configuration), the Master Port handles clear data while the Slave Port handles encrypted data. Configuration M_3, M_2 = 00 reverses this assignment. Actual data direction at any particular moment is controlled by the Encrypt/Decrypt bit.

The Encrypt/Decrypt bit (M_4) instructs the DCP algorithm processor to encrypt or decrypt the data from the Input Register using the ciphering method specified by the Cipher Type bits. The Encrypt/Decrypt bit also controls data flow within the DCP. For example, when the configuration bits are "01" (Dual Port, Master Clear, Slave Encrypted) and the Encrypt/Decrypt bit is "1" (encrypt), clear data will flow into the DCP through the Master Port and encrypted data will flow out through the Slave Port. When the Encrypt/Decrypt bit is set to "0" (decrypt), data flow reverses.

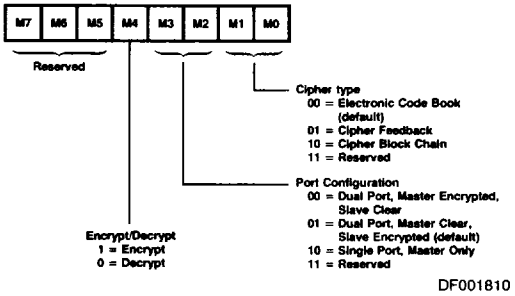


Figure 5. Mode Register Bit Assignments

Input Register

The 64-bit, write-only Input Register is organized to appear to the user as eight bytes of push down storage. A status circuit monitors the number of bytes that have been stored. The register is considered empty when the data stored in it has been or is being processed; it is considered full when one byte of data has been entered in Cipher Feedback or when eight bytes of data have been entered in the Electronic Code Book or Cipher Block Chain. If the user attempts to write data into the Input Register when it is full, the Input Register will disregard the attempt; no data in the register will be destroyed.

Output Register

The 64-bit, read-only Output Register is organized to appear to the user as eight bytes of pop-up storage. A status circuit detects the number of bytes stored in the Output Register. The register is considered empty when all the data stored in it has been read out by the host CPU, and is considered full if it still contains one or more bytes of output data. If a user attempts to read data from the Output Register when it is empty, the buffers driving the output bus will remain in a three-state condition.

The following multibyte registers cannot be directly addressed, but are loaded or read in response to commands written to the Command Register. (See Commands.)

M, E, D Key Registers

There are three 64-bit, write-only key registers in the DCP: the Master (M) Key Register; the Encrypt (E) Key Register; and the Decrypt (D) Key Register. The Master Key can be loaded only with clear data through the Auxiliary Port. The Encrypt and Decrypt Keys can be loaded in any of four ways: (1) as clear data through the Auxiliary Port; (2) as clear data through the Master Port; (3) as encrypted data through the Auxiliary Port; or (4) as encrypted data through the Master Port. In the last two cases, the encrypted data is first routed to the Input Register, decrypted using the M Key, and finally written to the target key register from the Output Register.

Initializing Vector Registers

Two 64-bit registers are provided to store feedback values for Cipher Feedback and Block Chained ciphering methods. One Initializing Vector (IVE) Register is used during encryption; the other (IVD), during decryption. Both registers can be loaded with either clear or encrypted data through the Master Port (in the latter case, the data is decrypted before being loaded into the IV Register), and both may be read out either clear or encrypted through the Master Port. (See Commands.)

Encrypt/ Decrypt M4	Port Configuration M3	M2	Input Register Flag	Output Register Flag
0	0	0	$\overline{\text{MFLG}}$	$\overline{\text{SFLG}}$
0	0	1	$\overline{\text{SFLG}}$	$\overline{\text{MFLG}}$
0	1	0	$\overline{\text{MFLG}}$	$\overline{\text{SFLG}}$
1	0	0	$\overline{\text{SFLG}}$	$\overline{\text{MFLG}}$
1	0	1	$\overline{\text{MFLG}}$	$\overline{\text{SFLG}}$
1	1	0	$\overline{\text{MFLG}}$	$\overline{\text{SFLG}}$

Figure 6. Association of Master Port Flag ($\overline{\text{MFLG}}$) and Slave Port Flag ($\overline{\text{SFLG}}$) with Input and Output Registers

Commands

All operations of the DCP result from command inputs, which are entered in Multiplexed Control Mode by writing a command byte to the Command Register. Command inputs are entered in Direct Control Mode by raising and lowering the logic levels on the AUX_7-K/$\overline{D}$, AUX_6-E/$\overline{D}$ and AUX_5-S/$\overline{S}$ pins. Figure 2 shows all commands that may be given in Multiplexed Control Mode. Figure 3 shows that subset executable in Direct Control Mode.

Load Clear M Key Through Auxiliary Port (90_H)

Load Clear E Key Through Auxiliary Port (91_H)

Load Clear D Key Through Auxiliary Port (92_H)

These commands override the data flow specifications set in the Mode Register and cause the Master (M), Encrypt (E), or Decrypt (D) Key Register to be loaded with eight bytes written to the Auxiliary Port. After the Load command is written to the Command Register, the Auxiliary Port Flag ($\overline{\text{AFLG}}$) will go

Refer to page 7-1 for Essential Information on Military Devices

active (LOW) and the corresponding bit in the Status Register (S_2) will go to "1," indicating that the device is able to accept key bytes at the Auxiliary Port pins. Additionally, the Command Pending bit (S_6) will go to "1" during the entire loading process.

Each byte is written by placing an active LOW signal on the Auxiliary Port Strobe ($\overline{ASTB}$) once data has been set up on the Auxiliary Port pins. The actual write process occurs on the rising (trailing) edge of $\overline{ASTB}$. (See Switching Characteristics for exact set-up, strobe width, and hold times.)

The Auxiliary Port Flag ($\overline{AFLG}$) will go inactive immediately after the eighth strobe goes active (LOW). However, the Command Pending bit (S_6) will remain "1" for several more clock cycles, until the key loading process is completed. All key bytes are checked for correct (odd) parity as they are entered (see Parity Checking).

Load Clear E Key Through Master Port (11_H)

Load Clear D Key Through Master Port (12_H)

These commands are available in both Multiplexed Control and Direct Control Modes. They override the data flow specifications set in the Mode Register and attach the Master Port inputs to the Encrypt (E) or Decrypt (D) Key Register, as appropriate, until eight key bytes have been written. In Multiplexed Control Mode, the command is initiated by writing the Load command to the Command Register. In Direct Control Mode, the command is initiated by raising the AUX_7-K/$\overline{D}$ control input while the AUX_5-S/$\overline{S}$ input is LOW. In this later case, the level on AUX_6-E/$\overline{D}$ determines which key register is written (HIGH = E Register).

Once the command has been recognized, the Command Pending bit (S_6 in the Status Register) will go to "1," and in Direct Control Mode, AUX_3-$\overline{CP}$ will go active (LOW), indicating that key entry may proceed. The host system then writes exactly eight bytes to the Master Port (at the Input Register address in Multiplexed Control Mode). When the key register has been loaded, Command Pending will return to "0," and in Direct Control Mode, the AUX_3-$\overline{CP}$ output will go inactive, indicating that the DCP can accept the next command.

Load Encrypted E Key Through Auxiliary Port ($B1_H$)

Load Encrypted D Key Through Auxiliary Port ($B2_H$)

Execution of these commands (in Multiplexed Control Mode only) is similar to the Load Clear E (or D) Key Through Auxiliary Port, except that key bytes are first decrypted using the Electronic Code Book algorithm and the Master (M) Key, and then loaded into the appropriate key register after having passed through the parity check logic (see Parity Checking).

The Command Pending bit (S_6) will be "1" during the entire decrypt-and-load operation. In addition, the Busy bit (S_5) will be "1" during the actual decryption process.

Load Encrypted E Key Through Master Port (31_H)

Load Encrypted D Key Through Master Port (32_H)

These commands (in Multiplexed Control Mode only) are similar in effect to Load Clear E (or D) Key Through Master Port, except that key bytes are initially decrypted using the Electronic Code Book algorithm and the Master (M) Key, and then loaded byte-by-byte into the target key register after having passed through the parity check logic (see Parity Checking).

The Command Pending bit (S_6) will be "1" during the entire necrypt-and-load operation. In addition, the Busy bit (S_5) will be "1" during the actual decryption process.

Load Clear IVE Register Through Master Port (85_H)

Load Clear IVD Register Through Master Port (84_H)

These commands (in Multiplexed Control Mode only) are virtually identical to Load Clear E (or D) Key Through Master Port except that the data written to the Input Register address is routed to the Encryption Initializing Vector (IVE) or Decryption Initializing Vector (IVD) Register instead of a key register, and no parity checking occurs. Command Pending (S_6) is a "1" during the entire loading process.

Load Encrypted IVE Register Through Master Port ($A5_H$)

Load Encrypted IVD Register Through Master Port ($A4_H$)

These commands are analogous to the Load Encrypted E (or D) Key Through Master Port commands. The data flow specifications set in the Mode Register are overridden, and the eight vector bytes are decrypted using the Decryption (D) Key and the Electronic Code Book algorithm. The resulting clear vector bytes are loaded into the target Initializing Vector Register, and no parity checking occurs. The Busy bit (S_5) does not go to "1" during the decryption process, but Command Pending (S_6) will be "1" during the entire decryption-and-load operation.

Read Clear IVE Register Through Master Port ($8D_H$)

Read Clear IVD Register Through Master Port ($8C_H$)

The effect of these commands (in Multiplexed Control Mode only) is to override the data flow specifications set in the Mode Register and to connect the appropriate Initializing Vector Register to the Master Port at the Output Register address. In this state, each IV Register appears as eight bytes of FIFO storage. The first byte of data will be available 6 clocks after the loading of the command register. The Command Pending bit will be set to "1" and will remain a "1" until sometime after the eighth byte is read out. The host system has the responsibility to read out exactly eight bytes.

Read Encrypted IVE Register Through Master Port ($A9_H$)

Read Encrypted IVD Register Through Master Port ($A8_H$)

The effect of these commands (in Multiplexed Control Mode only) is to override the specifications set in the Mode Register and to encrypt the contents of the specified Initializing Vector Register using the Electronic Code Book algorithm and the Encrypt (E) Key. The resulting cipher text is placed in the Output Register from which it can be read out as eight bytes through the Master Port. During the actual encryption process, the Busy bit (S_5) will be "1." When Busy goes to "0," the encrypted vector bytes are ready to be read out. Command Pending (S_6) will be "1" during the entire encryption-and-output process and will go to "0" when the eighth byte is read out. The host system is responsible for reading out exactly eight bytes.

Encrypt with Master (M) Key (39_H)

This command, in Multiplexed Control Mode only, overrides the data flow specifications set in the Mode Register and causes the DCP to accept eight bytes from the Master Port, which are written to the Input Register. When eight bytes have been received, the DCP encrypts the input using the Master (M) Key. The encrypted data is loaded into the Output Register, where it may be read out through the Master Port. The Command Pending (S_6) and Busy (S_5) bits are used to sense the three phases of this operation. Command Pending goes to "1" as soon as the Input Register can accept data. When exactly eight bytes have been entered, the Busy bit will go to "1" until the encryption process is complete.

When Busy goes to "0," the encrypted data is available to be read out. Command Pending will return to "0" when the eighth byte has been read.

Refer to page 7-1 for Essential Information on Military Devices

Start Encryption (41_H)

Start Decryption (40_H)

Start ($C0_H$)

The three "Start" commands begin normal data ciphering by setting the Start/Stop bit (S_7) in the Status Register to "1." The Start Encryption and Start Decryption commands explicitly specify the ciphering direction by forcing the Encrypt/Decrypt bit (M_4) in the Mode Register to "1" or "0," respectively; whereas, Start uses the current state of the Encrypt/Decrypt bit, as specified in a previous Mode Register load.

When a Start command has been entered, the Port Status Flag ($\overline{MFLG}$ or $\overline{SFLG}$) associated with the Input Register will become active (LOW), indicating that data may be written to the Input Register to begin ciphering.

In Direct Control Mode, the Start command is issued by raising the level on the AUX_5-S/$\overline{S}$ input (see Figure 3). The ciphering direction is specified by the level on AUX_6-E/$\overline{D}$. If AUX_6-E/$\overline{D}$ is HIGH when AUX_5-S/$\overline{S}$ goes HIGH, the command is Start Encryption; if AUX_6-E/$\overline{D}$ is LOW, it is Start Decryption.

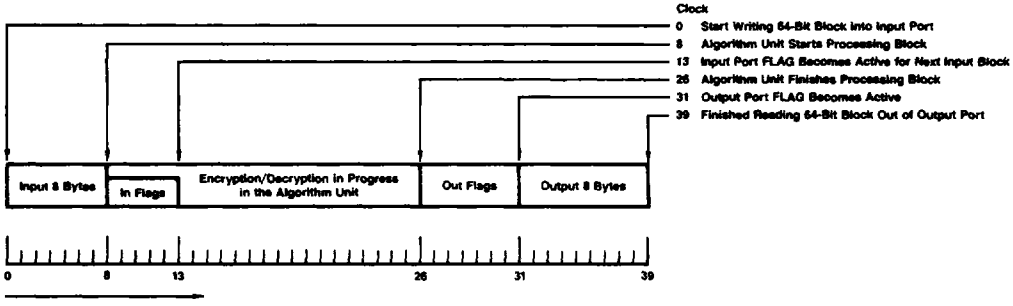
Stop ($E0_H$)

The Stop command clears the Start/Stop bit (S_7) in the Status Register to "0." This causes the input flag ($\overline{MFLG}$ or $\overline{SFLG}$) to become inactive and inhibits the loading of any further input into the Algorithm Unit. If ciphering is in progress (Busy bit (S_5) is "1" or AUX_2-$\overline{BSY}$ is active), it will finish, and any data in the Output Register will remain accessible (except in CFB Mode). In CFB Mode, the last byte of data must be read out before issuing the STOP command.

In Direct Control Mode, the Stop command is implied when the signal level on the AUX_5-S/$\overline{S}$ input goes from HIGH to LOW (see Figure 3).

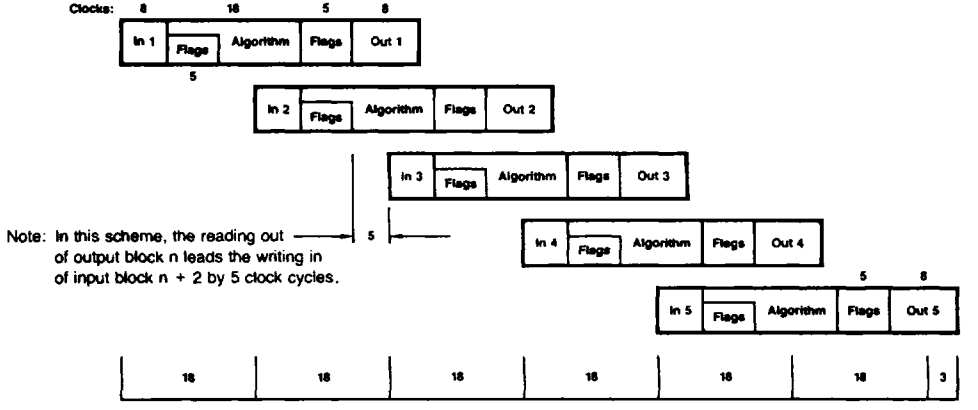
Software Reset (00_H)

This command has the same effect as a hardware reset ($\overline{MRD}$ and $\overline{MWR}$ low): it forces the DCP back to its default configuration, and all processing flags go into Inactive Mode. The default configuration includes setting the Mode Register to *Electronic Code Book Cipher Type* and *Dual Port Configuration* with Master Port clear, Slave Port encrypted.



Detailed Timing of One Block DF001820

Pipelining Scheme A: Minimum Timing Operation



DF001831

For n blocks, total number of clock pulses = (n + 1) x 18 + 3.

Am9568: Timing for Pipelined, Dual-Port Operation

ABSOLUTE MAXIMUM RATINGS

Storage Temperature ..... −65 to +150°C
Voltage on Any Pin with
Respect to Ground..... −0.5 to +7.0V
Power Dissipation 1.5W

Stresses above those listed under ABSOLUTE MAXIMUM RATINGS may cause permanent device failure. Functionality at or above these limits is not implied. Exposure to absolute maximum ratings for extended periods may affect device reliability.

OPERATING RANGES

Grade	T_A	V_{CC}	V_{SS}
Commercial	0°C to 70°C	5V ±5%	0V
Industrial	−40°C to 85°C	5V ±10%	0V

Operating ranges define those limits over which the functionality of the device is guaranteed.

DC CHARACTERISTICS over operating range unless otherwise specified

Parameters	Description	Test Conditions	Min	Typ	Max	Units
V_{IL}	Input Low Voltage		−0.5		.8	Volts
V_{IH}	Input High Voltage		2.2		V_{CC}	Volts
V_{OL}	Output Low Voltage	I_{OL} = 3.2mA			.40	Volts
V_{OH}	Output High Voltage	I_{OH} = −400μA	2.4			Volts
I_I	Input Leakage Current	$V_{SS} \leq V_{IN} \leq V_{CC}$			±10	μA
I_{OZ}	Output Leakage Current	V_{SS} = +.40 $\leq V_{IN} \leq V_{CC}$			±10	μA
I_{CC}	Supply Current (AVER.)			150	250	mA

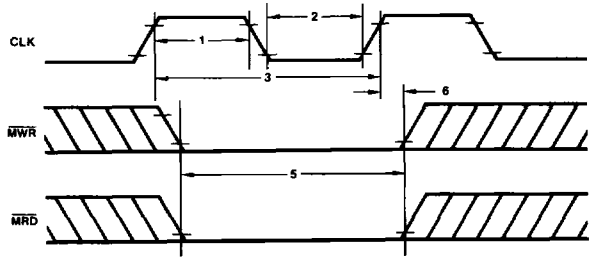
Refer to page 7-1 for Essential Information on Military Devices

Am9568 SWITCHING CHARACTERISTICS (Note 1)

The table below specifies the guaranteed performance of this device over the commercial operating range of 0 to +70°C with V_{CC} from 4.75V to 5.25V. All data are in nanoseconds. Switching tests are made with inputs and outputs measured at 0.8V for a LOW and 2.0V for a HIGH. Outputs are fully loaded, with $C_L \geq 50pF$. See Switching Waveform figures following table for graphic illustration of timing parameters.

SWITCHING CHARACTERISTICS over operating range unless otherwise specified

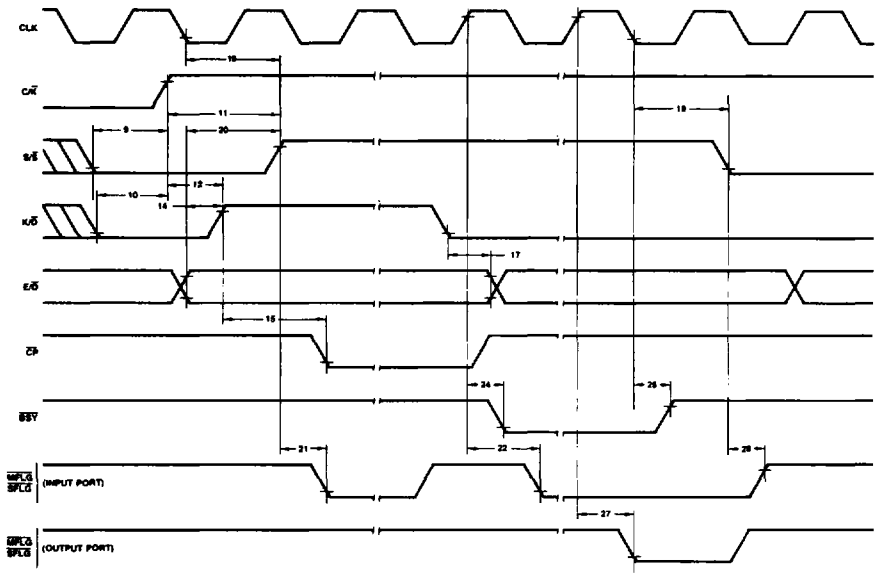
Number	Description	Min	Typ	Max	Units
Clock					
1	Clock Width HIGH (TWH)	115			ns
2	Clock Width LOW (TWL)	115			ns
3	Clock HIGH to Next Clock HIGH (Clock Cycle, TC)	250		1000	ns
Reset					
5	$\overline{MRD}$ • $\overline{MWR}$ LOW to $\overline{MRD}$ • $\overline{MWR}$ HIGH (Reset Pulse Width) (Note 12)	TC			ns
6	Clock HIGH to $\overline{MRD}$ • $\overline{MWR}$ HIGH	0		50	ns
Direct Control Mode					
9	S/$\overline{S}$ LOW to C/$\overline{K}$ HIGH (Set-up) (Note 12)	3TC			ns
10	K/$\overline{D}$ LOW to C/$\overline{K}$ HIGH (Set-up) (Note 12)	3TC			ns
11	C/$\overline{K}$ HIGH to S/$\overline{S}$ HIGH (Note 12)	6TC			ns
12	C/$\overline{K}$ HIGH TO K/$\overline{D}$ HIGH (Note 12)	6TC			ns
14	E/$\overline{D}$ VALID to K/$\overline{D}$ HIGH (Set-up) (Note 12)	3TC			ns
15	K/$\overline{D}$ HIGH to $\overline{CP}$ LOW			300	ns
17	K/$\overline{D}$ LOW to E/$\overline{D}$ INVALID (Hold) (Note 12)	TC			ns
19	Clock LOW to S/$\overline{S}$ VALID	20		80	ns
20	E/$\overline{D}$ VALID to S/$\overline{S}$ HIGH (Setup) (Note 12)	3TC			ns
21	S/$\overline{S}$ HIGH to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Input Flag)			230	ns
22	Clock HIGH to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Input Flag) (Note 2)			230	ns
24	Clock HIGH to $\overline{BSY}$ LOW			300	ns
25	Clock LOW to $\overline{BSY}$ HIGH			230	ns
27	Clock HIGH to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Output Flag)			230	ns
28	S/$\overline{S}$ LOW to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Port Input Flag) (Note 3)			230	ns
Multiplexed Control Mode – Master Port					
32	MALE Width (HIGH)	40			ns
34	$\overline{MCS}$ LOW to MALE LOW (Set-up)	0			ns
35	MALE LOW to $\overline{MCS}$ HIGH (Hold)	30			ns
36	Address INVALID to MALE LOW (Address Set-up Time)	15			ns
37	MALE LOW to Address INVALID (Address Hold Time)	25			ns



WF004490

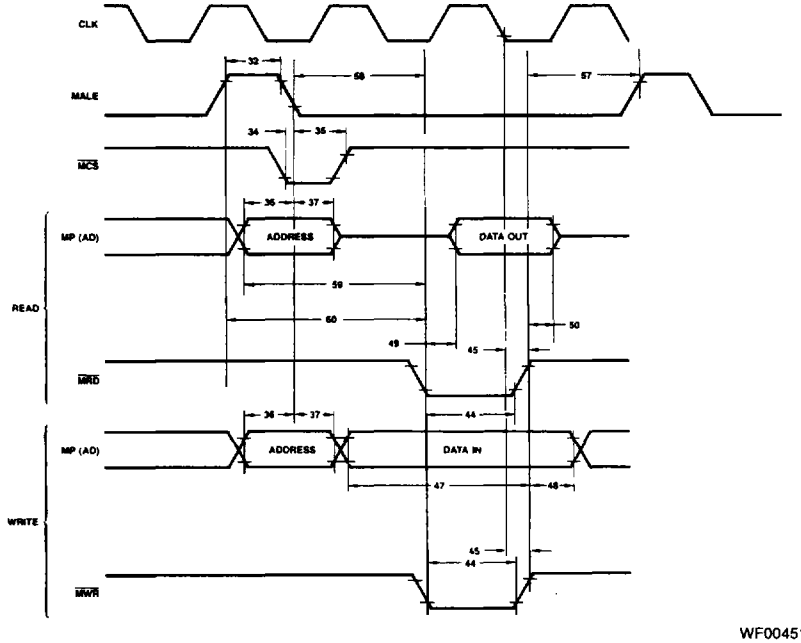
CLOCK AND RESET

Refer to page 7-1 for Essential Information on Military Devices



WF004500

CONTROL AND STATUS SIGNALS (DIRECT CONTROL MODE)



WF004510

MASTER PORT, MULTIPLEXED CONTROL MODE READ/WRITE

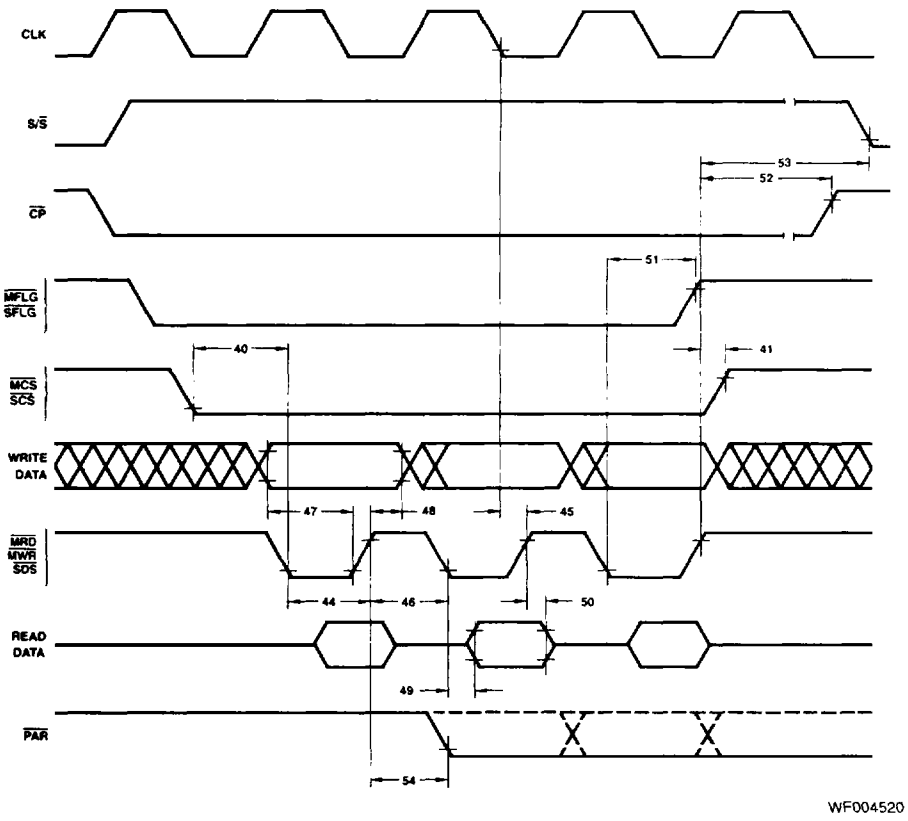
Refer to page 7-1 for Essential Information on Military Devices

SWITCHING CHARACTERISTICS over operating range unless otherwise specified

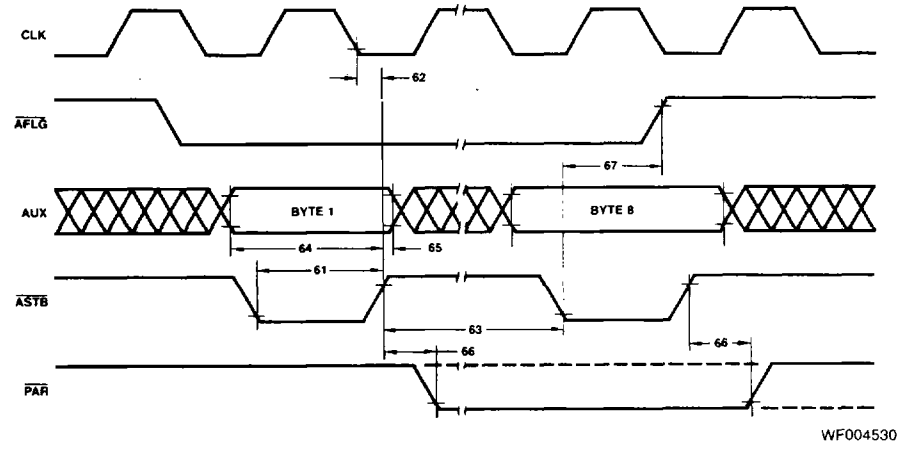
Number	Descripton		Min	Typ	Max	Units
Master/Slave Port Read/Write						
40	$\overline{MCS}$ LOW to $\overline{MRD}$, $\overline{MWR}$ LOW (Select Set-up) (Note 4)		60			ns
	$\overline{SCS}$ LOW to $\overline{SDS}$ LOW (Select Set-up) (Note 4)		100			
41	$\overline{MRD}$, $\overline{MWR}$ HIGH to $\overline{MCS}$ HIGH (Select Hold) (Note 4)		50			ns
	$\overline{SDS}$ HIGH to $\overline{SCS}$ HIGH (Select Hold) (Note 4)		25			
44	$\overline{MRD}$, $\overline{MWR}$ LOW to $\overline{MRD}$, $\overline{MWR}$ HIGH	Width – Write, Data Read	150		1000	ns
		Width – Status Register Read	215		1000	
	$\overline{SDS}$ LOW to $\overline{SDS}$ HIGH (Read, Write)		125		1000	
45	Clock LOW to $\overline{MRD}$, $\overline{MWR}$ HIGH (Note 11)		0		TWL – 85	ns
	Clock LOW to $\overline{SDS}$ HIGH (Note 11)		0		TWL – 65	
46	$\overline{MRD}$, $\overline{MWR}$ HIGH to $\overline{MRD}$, $\overline{MWR}$ LOW (Data Strobe Recovery Time)		150			ns
	$\overline{SDS}$ HIGH to $\overline{SDS}$ LOW (Data Strobe Recovery Time)		125			
47	Write Data VALID to $\overline{MWR}$ ($\overline{SDS}$) HIGH	Set-up Time – Key Load (Note 8)	125			ns
		Set-up Time – Data Write	125			
		Set-up Time – Command/Mode Register Write	125			
48	$\overline{MWR}$ HIGH to Write Data INVALID (Hold Time)		20			ns
	$\overline{SDS}$ HIGH to Write Data INVALID (Hold Time)		25			
49	$\overline{MRD}$ LOW to Read Data VALID	Read Access Time – Status Register			215	ns
		Read Access Time – Data			150	
	$\overline{SDS}$ LOW to Read Data VALID	Read Access Time – Status Register			200	ns
		Read Access Time – Data			120	
50	$\overline{MRD}$ ($\overline{SDS}$) HIGH to Read Data INVALID (Hold Time)		5		85	ns
51	$\overline{MRD}$, $\overline{MWR}$ LOW to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Last Strobe) (Note 5)				150	ns
	$\overline{SDS}$ LOW to $\overline{SFLG}$ HIGH (Last Strobe) (Note 5)				125	
52	$\overline{MWR}$ HIGH to $\overline{CP}$ HIGH (Note 4), (Note 12) (Last Strobe – Key Load)				TC – 520	ns
53	$\overline{MRD}$, $\overline{MWR}$ ($\overline{SDS}$) HIGH to S/$\overline{S}$ LOW (Hold Time) (Note 10), (Note 12)		4TC			ns
54	$\overline{MWR}$ HIGH to $\overline{PAR}$ VALID (Key Write)				220	ns
57	$\overline{MRD}$, $\overline{MWR}$ HIGH to MALE HIGH		75			ns
58	MALE LOW to $\overline{MRD}$, $\overline{MWR}$ LOW		25			ns
59	Address Valid to $\overline{MRD}$, $\overline{MWR}$ LOW (to guarantee 49)		100			ns
60	MALE HIGH to $\overline{MRD}$, $\overline{MWR}$ LOW		100			ns
Auxiliary Port Key Entry						
61	$\overline{ASTB}$ LOW to $\overline{ASTB}$ HIGH (Width)		160			ns
62	Clock LOW to $\overline{ASTB}$ HIGH (Note 11)		0		TWL – 65	ns
63	$\overline{ASTB}$ HIGH to Next $\overline{ASTB}$ LOW (Recovery Time)		250			ns
64	Write-Data VALID to $\overline{ASTB}$ HIGH (Data Set-up Time)		200			ns
65	$\overline{ASTB}$ HIGH to Write-Data INVALID (Data Hold Time)		80			ns
66	$\overline{ASTB}$ HIGH to $\overline{PAR}$ VALID				200	ns
67	$\overline{ASTB}$ LOW to $\overline{AFLG}$ HIGH (Last Strobe)				230	ns

Notes:
1. All input transition times assumed ≤ 20ns, except clock which is ≤ 10ns.
2. Parameter 22 applies to all input blocks except the first (when S/$\overline{S}$ first goes HIGH).
3. When S/$\overline{S}$ goes inactive (LOW) in Direct Control Mode, the flag associated with the input port will turn off.
4. Direct Control Mode only.
5. In Cipher Feedback, the Port Flag ($\overline{MFLG}$ or $\overline{SFLG}$) will go inactive following the leading edge of the first data strobe ($\overline{MRD}$, $\overline{MWR}$ or $\overline{SDS}$); in all other modes and operations, the flags go inactive on the eighth data strobe.
6. Do not remove K/$\overline{D}$ until $\overline{CP}$ is inactive (HIGH).
7. Do not change E/$\overline{D}$ until $\overline{MFLG}$ ($\overline{SFLG}$) is inactive (HIGH).
8. 200ns min if parity check is needed.
9. In Cipher Feedback, $\overline{BSY}$ must be inactive (HIGH) before S/$\overline{S}$ goes inactive (LOW).
10. $\overline{AFLG}$ must go active (LOW) before $\overline{ASTB}$ goes inactive (LOW).
11. TWL is the clock width (LOW) (number 2).
12. TC is the clock cycle time (number 3).

Refer to page 7-1 for Essential Information on Military Devices



MASTER (SLAVE) PORT READ/WRITE



AUXILIARY-PORT KEY ENTRY

Refer to page 7-1 for Essential Information on Military Devices