NEWBRIDGE MICROSYSTEMS

CA20C03A & CA20C03W

DES ENCRYPTION PROCESSORS

- **The CA20C03A is an improved version of the DES encryption processor designed by Newbridge Microsystems, while the CA20C03W is the Western Digital WD20C03A silicon sold and supported exclusively by Newbridge Microsystems. The information in this document applies to both the CA20C03A and CA20C03W (referred to jointly as CA20C03A/W) unless stated otherwise.**
- **Data transfer rates up to 3.85 Mbytes per second for CA20C03A**
- **Encrypt and decrypt using Data Encryption Standard (DES) adopted by the U.S. Department of Commerce, National Bureau of Standards (NBS) - publication FIPS PUB 46 (1-15-1977)**
- **Validated by the National Institute for Standards and Technology (NIST) in accordance with the procedures specified in NBS publication 500-20**
- **Electronic Code Book (ECB) and Cipher Block Chaining (CBC)**
- **Encrypt and decrypt 64-bit data words using 56-bit key words**
- **Parity check on key word loading**
- **Key stored in device is not externally accessible**
- **Standard 8-bit microprocessor interface**
- **Battery Back-up capability of internal key register for CA20C03A**
- **Low power CMOS with TTL I/O compatibility**
- **Available in PLCC, PDIP, and TQFP packages**

The Newbridge Microsystems CA20C03A and CA20C03W *DES Encryption Processors* are designed to encrypt and decrypt 64-bit blocks of data using the algorithm specified in the Federal Information Processing Data Encryption Standard - publication FIPS PUB 46 (1-15-1977). DES is the standard data encryption algorithm used for file and communications encryption, and as such is widely established in the security, finance and banking industries. The CA20C03A/W encrypt 64-bit clear text words using 56-bit, user-specified keys to produce 64-bit cipher text words. When reversed, the cipher text words are decrypted to produce the original clear text words.

If your application requires strictly WD2001 mode then please contact the factory for documentation.

The CA20C03A/W are implemented in low power CMOS technologies with TTL compatible I/O. They are offered in 28-pin PDIP, 28-lead PLCC, and 44-pin TQFP packaging.

Application areas for the CA20C03A/W DES chips span a diverse industrial base of financial, information processing, telecommunications and data communications companies.

- Secure Brokerage transactions
- Electronic fund transfers
- Secure banking/business accounting
- Mainframe communications
- Remote and host computer communications
- Secure disk or magnetic tape data storage
- Secure packet-switching transmission

3

Table 3-1 : CA20C03A/W Transfer Rates

Product Code	Data Transfer Rates - ECB Mode (Mbytes per Second)	System Clock
CA20C03W-5	0.40	5 MHz
CA20C03W-8	0.64	8 MHz
CA20C03A-5	0.77	5 MHz
CA20C03A-10	1.54	10 MHz
CA20C03A-16	2.46	16 MHz
CA20C03A-20	3.08	20 MHz
CA20C03A-25	3.85	25 MHz

Warning: These devices cannot be shipped outside North America without written authorization from Canadian External Affairs and Department of National Defence or the US State Department and Department of Defence.

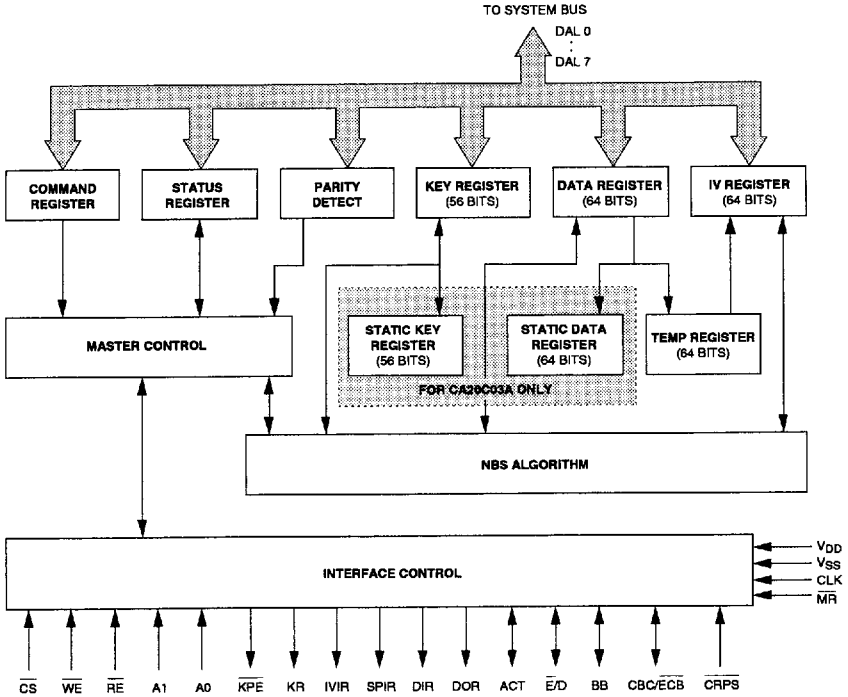
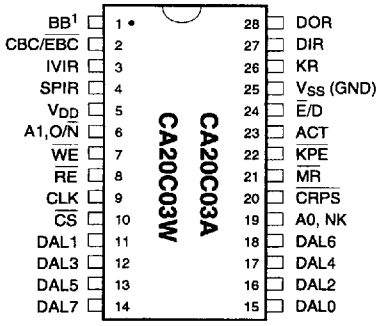
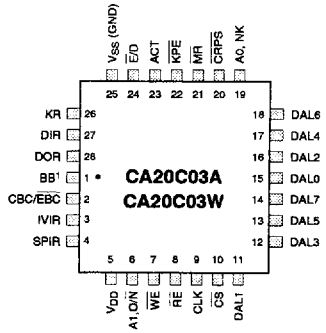


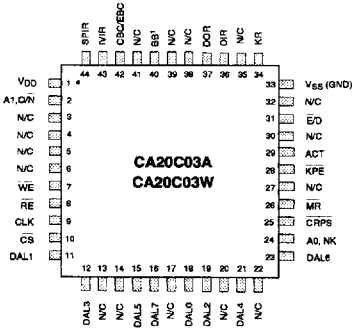
Figure 3-1 : CA20C03A/W Block Diagram



a) 28-pin PDIP



b) 28-pin PLCC



c) 44-pin TQFP

Figure 3-2 : CA20C03A/W Pin Configurations

Note 1: For the CA20C03W device, pin 1 is a no connect (N/C) for the PDIP and PLCC packages, pin 40 is a N/C for the TQFP package.

Table 3-2 : Pin Description

Symbol	Pin			Type	Name and Function
	PLCC	PDIP	TQFP		
A0, NK	19	19	24	I	**Address 0, New Key:** When $\overline{CRPS}$ is logic 1 or open, a high on this input addresses the Command or Status Register (see Table 3-18). When $\overline{CRPS}$ and A1, O/$\overline{N}$ are logic 0, a high on this input requests that a new key be loaded in the Key Register. Device responds by activating the KR pin.
A1, O/$\overline{N}$	6	6	2	I	**Address 1, Old/New:** When $\overline{CRPS}$ is logic 1 or open, and this input is logic 1, the Status Register is addressed ($\overline{CS}$ = 0, A0 = 1). When this input is logic 0, the Command Register is addressed ($\overline{CS}$ = 0, A0 = 1). This input is ignored when A0 = 0. Note that this input has an internal pull-up resistor. (CA20C03A silicon only) When $\overline{CRPS}$ is logic 0 (low) and this input is logic 0, the device is in CA20C03A/W mode. When this input is logic 1, the device is in WD2001 mode. The only way to return to CA20C03A/W mode from WD2001 mode is to reset the device. *Caution: In WD2001 mode, pin 6 of the CA20C03A device must not be connected to +12V as it will irreparably damage the device. The CA20C03W may have this pin connected to +12V without harm to the device.*
ACT	23	23	29	I/O	**Activate:** When $\overline{CRPS}$ is logic 1 or open, this pin is an output reflecting the status of the *Activate* bit (bit 1) of the Command Register. When $\overline{CRPS}$ is logic 0, this pin is an input that overrides the Activate bit of the Command Register.
BB	1	1	40	I/O	**Battery Back-up Key:** When $\overline{CRPS}$ is logic 1 (open), this pin is an output reflecting the status of the *battery back-up key* bit (bit 5) of the Command Register. When $\overline{CRPS}$ is logic 0 or low, this pin is an input that overrides the *battery back-up key* bit. This pin is a no connect for the CA20C03W device.
CBC/$\overline{ECB}$	2	2	42	I/O	**Cipher Block Chaining/Electronic Code Book:** When $\overline{CRPS}$ is logic 1 or open, this pin is an output pin reflecting the status of CBC/$\overline{ECB}$ bit (bit 7) of the Command Register. When $\overline{CRPS}$ is logic 0, this pin is an input pin and overrides the CBC/$\overline{ECB}$ bit of the Command Register.
CLK	9	9	9	I	**Clock:** System clock input.
$\overline{CRPS}$	20	20	25	I	**Command Register Pin Select:** This input selects DAL bus or input pin programming of the Command Register. $\overline{CRPS}$ high or open selects DAL bus programming. $\overline{CRPS}$ low selects input pin programming.This input incorporates an internal pull-up resistor.
$\overline{CS}$	10	10	10	I	**Chip Select:** $\overline{CS}$ is made low to access registers within the device.
DAL 7 - 0	11-18	11-18	11,12,15, 16,18,19,2 1,23	I/O	**Data Lines:** Eight active true, tri-state, bi-directional I/O lines used for information transfer to and from the DES device. All *Command Register, Status Register, Key Word* and *Data Word* transfers are via this bus.
DIR	27	27	36	O	**Data-In Request:** This output is active high when the DES device is requesting that byte of the *Data Word* be written into the Data Register (The Data Register is automatically addressed when DIR is active, unless overridden by A0).
DOR	28	28	37	O	**Data-Out Request:** This output is active high when the DES device is requesting that a byte of the *Data Word* be read from the Data Register (The Data Register is automatically addressed when the DOR is active, unless overridden by A0).
E/D	24	24	31	I/O	**Encrypt/Decrypt:** When $\overline{CRPS}$ is high or open, this pin is an output reflecting the status of the *Encrypt/Decrypt* bit (bit 3) of the Command Register. When $\overline{CRPS}$ is low, this pin is an input pin that overrides the *Encrypt/Decrypt* bit of the Command Register.

Table 3-2 : Pin Description Cont'd

Symbol	Pin			Type	Name and Function
	PLCC	PDIP	TQFP		
IVIR	3	3	43	O	**Initial Vector-In Request:** This output is active high when the device is requesting that a byte of the *IV Word* be written into the IV register (The IV register is automatically addressed when IVIR is active, unless overridden A0).
$\overline{KPE}$	22	22	28	O	**Key Parity Error:** This output is active low when enabled via the Command Register bit 2 (KEOE) and a parity error has been detected during loading of the Key Register.
KR	26	26	34	O	**Key Request:** This output is active high when the DES device is requesting that a byte of the *Key Word* be written into the Key Register. (The Key Register is automatically addressed when KR is active, unless overridden by A0.)
$\overline{MR}$	21	21	26	I	**Master Reset:** $\overline{MR}$ active low resets the Command and Status Registers and resets internal circuitry. (Requires active clock for reset operation.)
$\overline{RE}$	8	8	8	I	**Read Enable:** The contents of the selected register are placed on the DAL bus lines when $\overline{CS}$ and $\overline{RE}$ are made low.
SPIR	4	4	44	O	**Special Pattern-In:** This output is active high during battery back-up mode, when the device is requesting that a byte of the *Special Pattern Word* be written into the Data Register (The Data Register is automatically addressed when SPIR is active, unless overridden by A0).
V_{DD}	5	5	1	-	**Power Supply:** +5 V ±10%
V_{SS}	25	25	33	-	**Ground:** Ground
$\overline{WE}$	7	7	7	I	**Write Enable:** Information on the DAL bus lines is written into the selected register when $\overline{CS}$ and $\overline{WE}$ are made low.

3

Table 3-3a : AC Characteristics For CA20C03A (5, 10, 16 MHz)
T_A = 0 to 70 °C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V

Symbol	Parameter	Test Condition	Limits 5MHz		Limits 10MHz		Limits 16MHz		Unit
			Min	Max	Min	Max	Min	Max	
t_{BR}	$\overline{RE}\uparrow$ to next $\overline{RE}\downarrow$		2CLK		2CLK		2CLK		ns
t_{BW}	$\overline{WE}\uparrow$ to next $\overline{WE}\downarrow$		2CLK		2CLK		2CLK		ns
t_{CY}	Clock cycle time			200		100		62.5	ns
t_{DAR}	DOR↑, DOA↑ from $\overline{RE}\uparrow$			2CLK+30		2CLK+30		2CLK+30	ns
t_{DAW}	KR↑, DIR↑, IVIR↑, SPIR↑,KA↑ and DIA↑ from $\overline{WE}\uparrow$			2CLK+30		2CLK+30		2CLK+30	ns
t_{DDR}	DOR↓ from $\overline{RE}\downarrow$			150		80		50	ns
t_{DDW}	KR↓, DIR↓, IVIR↓, SPIR↓ from $\overline{WE}\downarrow$	CLOAD = 50 pF		150		80		50	ns
t_{DF}	$\overline{RE}\uparrow$ to DAL float		10	100	10	50	5	35	ns
t_{DH}	DAL hold from $\overline{WE}\uparrow$		20		15		10		ns
t_{DSR}	DOA↓ from $\overline{RE}\downarrow$			1CLK+30		1CLK+30		1CLK+30	ns
t_{DSW}	KA↓, DIA↓ from $\overline{WE}\downarrow$			1CLK+30		1CLK+30		1CLK+30	ns
t_{DVW}	DAL setup WE↑		80		40		30		ns
t_{MR}	Master reset pulse width		2CLK		2CLK		2CLK		µs
t_{RACH}	A0, A1, CS hold from $\overline{RE}\uparrow$		0		0		0		ns
t_{RACS}	A0, A1, CS setup to $\overline{RE}\downarrow$		25		15		5		ns
t_{RD}	$\overline{RE}$ pulse width		200		100		60		ns
t_{RDV}	$\overline{RE}\downarrow$ to DAL valid	CLOAD = 50pF		150		90		50	ns
t_{WACH}	A0, A1, CS hold from $\overline{WE}\uparrow$		0		0		0		ns
t_{WACS}	A0, A1,CS setup to $\overline{WE}\downarrow$		25		15		5		ns
t_{WR}	$\overline{WE}$ Pulse Width		125		95		60		ns

Notes for Tables 3a, 3b, and 3c:

1. All output timing specifications reflect the following:
   High Output 2.0V, Low Output 0.8V
2. Clock Input: Clock signal duty cycle is 50% ±10%. There is no minimum frequency.
3. t_{MR} is 2 CLKS in all cases for the CA20C03A device.
4. Time between consecutive $\overline{RE}$ or $\overline{WE}$ pulses: $t_{BR} = t_{BW} = 2$ Clock periods *minimum*.
5. ACT, E/D, and CBC/$\overline{ECB}$ are valid 2CLK↓ + 450 ns from $\overline{WE}\uparrow$ of a Command Register write operation (for CA20C03W in WD2001 mode).
6. $\overline{KPE}$ output is valid within 2CLK↓ + 450 ns from $\overline{WE}\uparrow$ of a write of a *Key Word* byte that results in a parity error (for CA20C03W in WD2001 mode).
7. ACT, E/D, BB and CBC/$\overline{ECB}$ are valid 2CLK↓ + 30 ns from $\overline{WE}\uparrow$ of a Command Register write operation (for CA20C03A).
8. $\overline{KPE}$ output is valid within 1CLK↓ + 30 ns from $\overline{WE}\uparrow$ of a write of a *Key Word* byte that results in a parity error (for CA20C03A).
9. $\overline{DOA}$, $\overline{KA}$ and $\overline{DIA}$ pertain to the WD2001 mode (refer to CA20C01 data sheet).

Table 3-3b : AC Characteristics For CA20C03A (20, 25 MHz)
T_A = 0 to 70 °C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V

Symbol	Parameter	Test Condition	Limits 20MHz		Limits 25MHz		Unit
			Min	Max	Min	Max	
t_{BR}	$\overline{RE}\uparrow$ to next $\overline{RE}\downarrow$		2CLK		2CLK		ns
t_{BW}	$\overline{WE}\uparrow$ to next $\overline{WE}\downarrow$		2CLK		2CLK		ns
t_{CY}	Clock cycle time			50		40	ns
t_{DAR}	DOR↑, DOA↑ from $\overline{RE}\uparrow$			2CLK+30		2CLK+30	ns
t_{DAW}	KR↑, DIR↑, IVIR↑, SPIR↑,KA↑ and DIA↑ from $\overline{WE}\uparrow$			2CLK+30		2CLK+30	ns
t_{DDR}	DOR↓ from $\overline{RE}\downarrow$			40		35	ns
t_{DDW}	KR↓, DIR↓, IVIR↓, SPIR↓ from $\overline{WE}\downarrow$	CLOAD = 50 pF		40		35	ns
t_{DF}	$\overline{RE}\uparrow$ to DAL float		5	25	5	20	ns
t_{DH}	DAL hold from $\overline{WE}\uparrow$		5		5		ns
t_{DSR}	DOA↓ from $\overline{RE}\downarrow$			1CLK+30		1CLK+30	ns
t_{DSW}	KA↓, DIA↓ from $\overline{WE}\downarrow$			1CLK+30		1CLK+30	ns
t_{DVW}	DAL setup WE↑		20		20		ns
t_{MR}	Master reset pulse width		2CLK		2CLK		µs
t_{RACH}	A0, A1, CS hold from $\overline{RE}\uparrow$		0		0		ns
t_{RACS}	A0, A1, CS setup to $\overline{RE}\downarrow$		5		5		ns
t_{RD}	$\overline{RE}$ pulse width		50		40		ns
t_{RDV}	$\overline{RE}\downarrow$ to DAL valid	CLOAD = 50pF		45		35	ns
t_{WACH}	A0, A1, CS hold from $\overline{WE}\uparrow$		0		0		ns
t_{WACS}	A0, A1,CS setup to $\overline{WE}\downarrow$		5		5		ns
t_{WR}	$\overline{WE}$ Pulse Width		45		35		ns

Notes for Tables 3a, 3b, and 3c continued:

10. KR activation is valid within 2CLK↓ + 30 ns from $\overline{WE}\uparrow$ (for CA20C03A) and 3CLK↓ + 450 ns (for CA20C03W in WD2001 mode) from $\overline{WE}\uparrow$ of a write operation that programs a 1 into the COMMAND REGISTER ACTIVATE bit (or from a ACT input↑, if $\overline{CRPS}$ = 0).
11. Initial DIR activation is valid within 20CLK↓ + 30 ns from $\overline{WE}\uparrow$ (for CA20C03A) and 49 CLK↓ + 450 ns (for CA20C03W in WD2001 mode) of the 8th write into the Key Register.
12. Initial DOR activation is valid within 20CLK↓ + 30 ns from $\overline{WE}\uparrow$ (for CA20C03A) and 49 CLK↓ + 450 ns (for CA20C03W in WD2001 mode) of the 8th write into the Data Register.
13. When reading the Data Register (in response to DOR), subsequent data bytes are made available internally to the DAL output buffers within 2CLK↓ + 30 ns from $\overline{RE}\uparrow$ (for CA20C03A) and 2 CLK↓ + 450 ns (for CA20C03W in WD2001 mode).
14. After reading the Data Register in response to DORs, DIR is activated and valid within 2CLK↓ + 30 ns from $\overline{RE}\uparrow$ (for CA20C03A) and 2 CLK↓ + 450 ns (for CA20C03W in WD2001 mode) of the 8th read from the Data Register.
15. All output timings assume CLOAD = 50pF.

Table 3-3c : AC Characteristics For CA20C03W (5, 8 MHz)
T_A = 0 to 70 °C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V

Symbol	Parameter	Test Condition	Limits 5MHz		Limits 8MHz		Limits 10MHz		Unit
			Min	Max	Min	Max	Min	Max	
t_{BR}	$\overline{RE}\uparrow$ to next $\overline{RE}\downarrow$		2CLK		2CLK		2CLK		ns
t_{BW}	$\overline{WE}\uparrow$ to next $\overline{WE}\downarrow$		2CLK		2CLK		2CLK		ns
t_{CY}	Clock cycle time			200		125		100	ns
t_{DAR}	DOR↑, DOA↑ from $\overline{RE}\uparrow$			2CLK+45		2CLK+20		2CLK+20	ns
t_{DAW}	KR↑, DIR↑, IVIR↑, SPIR↑, KA↑ and DIA↑ from $\overline{WE}\uparrow$			2CLK+140		2CLK+80		2CLK+60	ns
t_{DDR}	DOR↓ from $\overline{RE}\downarrow$			150		100		80	ns
t_{DDW}	KR↓, DIR↓, IVIR↓, SPIR↓ from $\overline{WE}\downarrow$	CLOAD = 50 pF		150		100		80	ns
t_{DF}	$\overline{RE}\uparrow$ to DAL float		20	100	17	50	15	45	ns
t_{DH}	DAL hold from $\overline{WE}\uparrow$		30		25		25		ns
t_{DSR}	DOA↓ from $\overline{RE}\downarrow$			1CLK+25		1CLK+20		1CLK+20	ns
t_{DSW}	KA↓, DIA↓ from $\overline{WE}\downarrow$			1CLK+120		1CLK+20		1CLK+20	ns
t_{DVW}	DAL setup WE↑		80		40		40		ns
t_{MR}	Master reset pulse width		1		1		1		µs
t_{RACH}	A0, A1, CS hold from $\overline{RE}\uparrow$		0		0		0		ns
t_{RACS}	A0, A1, CS setup to $\overline{RE}\downarrow$		30		25		15		ns
t_{RD}	$\overline{RE}$ pulse width		220		150		100		ns
t_{RDV}	$\overline{RE}\downarrow$ to DAL valid	CLOAD = 50pF		150		115		90	ns
t_{WACH}	A0, A1, CS hold from $\overline{WE}\uparrow$		0		0		0		ns
t_{WACS}	A0, A1,CS setup to $\overline{WE}\downarrow$		30		25		15		ns
t_{WR}	$\overline{WE}$ Pulse Width		125		100		95		ns

Figure 3-3 : Typical Key or Data Register Load Timing

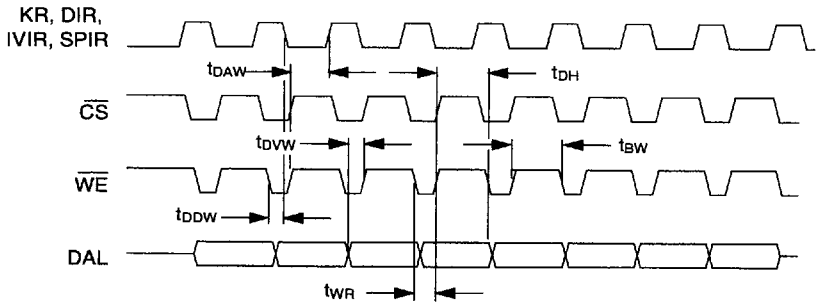
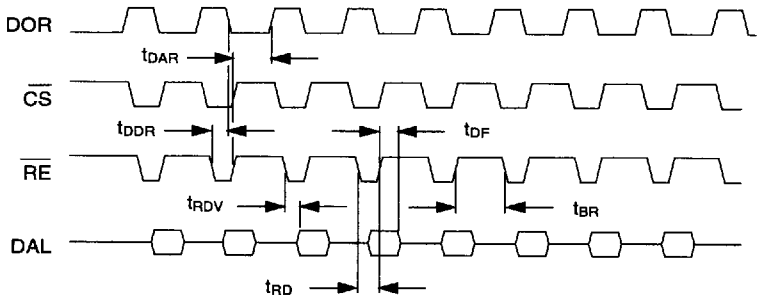


Figure 3-4 : Typical Register Read Timing



3

Figure 3-5 : Read Timing

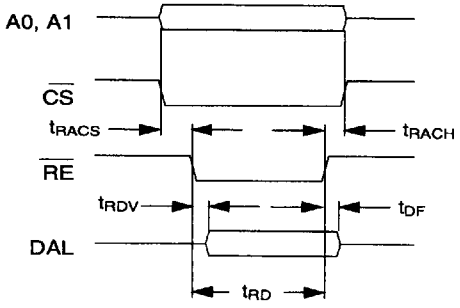
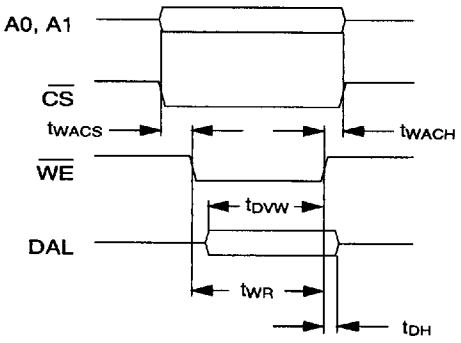


Figure 3-6 : Write Timing



USING THE CA20C03A TO ATTAIN MAXIMUM THROUGHPUT

In order to obtain maximum throughput from the CA20C03A, the number of cycles used to perform I/O operations is minimized. The throughput is dictated by eight bytes written to the device plus 20 cycles for processing, plus eight bytes read from the device for each 64-bit block. If the data sheet is followed explicitly, it would take 24 cycles per I/O operation for a total of 48 cycles (i.e. three cycles for each byte written to or read from the device as dictated by t_{BW} timing parameters). So for each 64-bit block, 48 plus 20, or 68 cycles are required, giving a maximum throughput of:
8bytes/(68 cycles x (40ns/cycle) = 2.95 MBytes/s.

The number of cycles per byte can be reduced to two by following a few simple timing rules. The timing parameters t_{BW} and t_{BR} specify two cycles between the rising edge of a read or write and the falling edge of the next read or write. Figure 3-7 shows this timing and hence the three clock cycles per byte. In actual fact, two falling edges of the clock are required between the rising edge of a read or write and the falling edge of the next read or write. Figure 3-8 shows how two cycles are achieved in this case. So for each 64-bit block, 32 plus 20, or 52 cycles are required, giving a maximum throughput of:
8bytes/(52 cycles x (40ns/cycle) = 3.85 MBytes/s

Two new timing parameters, t_1 and t_2, are introduced (see Figure 3-8), and modifications are made to $\overline{WR}$ and $\overline{RD}$ (see Table 3-5 below).

Table 3-4 : Maximum Throughput I/0 Timing For The CA20C03A Device

Symbol	5 MHz		10 MHz		16 MHz		20 MHz		25 MHz		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
t_{WR}	125	185	65	85	30	45	25	35	20	25	ns
t_{RD}	125	185	65	85	30	45	25	35	20	25	ns
t_{RDV}	125		65		30		25		25		ns
t_1	2		2		2		2		2		ns
t_2	13		13		13		13		13		ns

Note: The following timing parameters only apply when the timing of Figure 8 is used.

Figure 3-7 : Typical I/O Timing

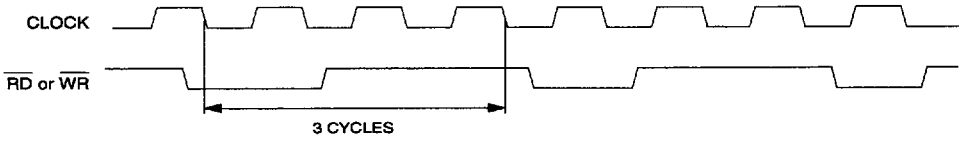


Figure 3-8 : Maximum Throughput Timing For The CA20C03A Device

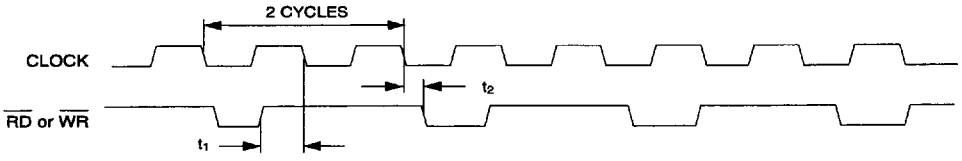


Table 3-5 : DC Characteristics (T_A = 0 to 70 °C, V_{DD} = +5.0V ± 10%, V_{SS} = 0V)

Symbol	Parameter	Test Conditions	Limits		Unit
			Min	Max	
I_{IL}	Input leakage current	V_{IH} = 5.5 V	-10	+10	µA
		V_{IL} = 0 V	-10	+10	µA
I_{LL}	Input low current only on CA20C03A $\overline{CRPS}$, A1, O/$\overline{N}$ pins.	V_{IL} = 0 V (note 3)		1	mA
	Input low current only on CA20C03W $\overline{CRPS}$ pin.			**1.6**	**mA**
I_{OL}	Output leakage current	0 V ≤ V_{IN} ≤ V_{DD}	-10	10	µA
I_{DDOP}	Operating current	V_{IN} = V_{DD} or V_{SS} V_{DD} = 5.5 V, Outputs open (note 3)		2 **15**	mA/MHz **mA**
I_{DDSB}	Standby current	V_{IN} = V_{DD} or V_{SS} V_{DD} = 5.5 V, Outputs open (note 5)		1.0 (0.1 Typ)	µA
V_{IH}	Voltage input high		2.4		V
V_{IL}	Voltage input low (all inputs)			0.8	V
V_{OH}	Voltage output high	I_{OH} = -100 µA	2.8		V
V_{OL}	Voltage output low	I_{OL} = +1.6 mA		0.4	V
V_{BB}	Min. battery back-up voltage	(note 4)	2.0		V
I_{DR}	Data retention current in battery back-up mode	V_{BB} = 2.0 V (note 4)		15.0	µA

Notes:

1. I_{IL} applies only to inputs without pull-up resistors.
2. I_{LL} applies only to inputs with pull-up resistors.
3. Values given in bold type face refer to CA20C03W. All other values apply to both device types.
4. Battery back-up mode applies to only the CA20C03A device.
5. Applies to the CA20C03A device only.

Table 3-6 : Recommended Operating Conditions

DC Supply Voltage (V_{DD})	+4.5 V to +5.5 V
Power Dissipation (P_{DD})	1 W
Ambient Operating Temperature (T_A Commercial)	0° to +70°C

The power dissipation figure is based on typical internal logic dissipation plus the worst case set of outputs simultaneously active with maximum rated loads.

Table 3-7 : Absolute Maximum Ratings

DC Supply Voltage (V_{DD})	-0.3 to +7.0 V
Input Voltage (V_{IN})	-0.3 to VDD +0.3 V
DC Input Current (I_{IN})	-10 to +10 mA
Storage Temperature, plastic (T_{STG})	-40° to +125°C

Stresses beyond those listed above may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to maximum rating conditions for extended periods may affect device reliability.

FUNCTIONAL DESCRIPTION

The CA20C03A/W Data Encryption Standard (DES) devices consist of eight registers, two ciphering options, the DES algorithm and key parity checking. The CA20C03A also contains the necessary logic to implement a Battery Back-up Key option.

The eight registers include a 56-bit Key Register, a 64-bit Data Register, a 64-bit Initial Vector Register, a 64-bit Temp Register, two 8-bit registers for both command and status, a 56-bit Static Key Register, and a 64-bit Static Data Register. A block diagram of the CA20C03A/W is shown in Figure 1.

The CA20C03A devices can be programmed for encryption or decryption using either the *Electronic Code Book* (ECB) or *Cipher Block Chaining* (CBC) modes with or without a *Battery Back-up Key.* The CA20C03W device can be programmed in ECB or CBC modes of encryption without a Battery Back-up Key. Data is encrypted or decrypted with a 64-bit, user-defined *Key Word.* Data encrypted with a given *Key Word* can be decrypted only using the same *Key Word.*

The Key Register is loaded by the system with eight successive bytes beginning with the most significant byte of the key. Parity is checked on each byte of the *Key Word* as it is loaded into the Key Register. The least significant bit (DAL0) of each 8-bit byte is reserved for odd parity for that byte and is not used in the algorithm calculation (see Table 3-8 and Table 3-9 below for Key Word loads and Data loads and reads).

Table 3-8 : Format for *Key Word* Loads

7	6	5	4	3	2	1	Parity
DAL7	DAL6	DAL5	DAL4	DAL3	DAL2	DAL1	DAL0

Table 3-9 : Format for Data Loads and Reads

7	6	5	4	3	2	1	0
DAL7	DAL6	DAL5	DAL4	DAL3	DAL2	DAL1	DAL0

In a mode without a *Battery Back-up Key*, the *Key Word* is requested after each activation and should be loaded into the Key Register. The Static Key Register and Static Data Register are not used in this mode.

In a mode with a *Battery Back-up Key*, the *Key Word* is requested only when the user requests a new key by programming the Command Register, or when the *Key Word* stored in the Static Key Register is found no longer valid after power-up key verification. In this mode, the *Key Word* is loaded into the Static Key Register, and a special 64-bit pattern is requested and encrypted by the CA20C03A. The encrypted pattern is loaded in the Static Data Register.

During power-down or power failure, the contents of these two Static Registers are retained by the battery back-up power. As soon as the power is up again, the contents in the Static Data Register are used to verify and validate the contents in the Static Key Register during the key verification process.

When the CA20C03A/W is programmed for the Cipher Block Chaining (CBC) mode, the *Initial Vector* (IV) is requested by the device after the *Key Word* is loaded into the Key Register and is ready to be used for encryption or decryption. The Initial Vector Register is loaded with eight successive bytes (most significant byte first) of *Initial Vector* data at the start of each encryption or decryption process.

To encrypt plain data, the Data Register is loaded with eight successive bytes (most significant byte first) of the first plain text block. The contents of the Data Register are then added (modulo 2) to the contents of the Initial Vector Register one bit at a time. The modified text is then encrypted to the DES algorithm and the resulting encrypted (cipher) text is loaded into the Initial Vector Register for the next block of plain text to be modified, as well as being ready to be read out. This cycle is repeated until all required data is encrypted. To decrypt encrypted data, the Data Register is loaded with eight successive bytes (8-bit) of the first cipher text block. The contents of the Data Register are loaded into the Temp Register and at the same time they are decrypted to the DES algorithm. The resulting text in the Data Register is added (modulo 2) with the contents of the Initial Vector Register. The contents of the Initial Vector Register becomes plain text and are loaded into the Data Register, ready to be read out. The contents of the Temp Register are then loaded into the Initial Vector Register to allow for the next block of cipher text to be decrypted. This cycle is repeated until all required data is decrypted.

When the CA20C03A/W is programmed for Electronic Code Book (ECB) mode, neither the Initial Vector Register nor the Temp Register are used. The *Data Word* is requested by the device after the *Key Word* is loaded in the Key Register and ready to be used for encryption or decryption. In both encryption and decryption, the Data Register is loaded with eight successive bytes (8-bit) of text, then the contents of the Data Register go through the DES algorithm calculation. The resulting text in the Data Register is ready to be read out. It is read by reading eight successive bytes (8-bit).

The data transfer into or out of the device's registers (Key Register, Data Register, IV Register) through the DAL bus is accomplished by loading or reading out eight successive bytes (8-bit). The first byte written to or read from these registers is always the most significant byte. The data transfer between registers (Key Register, Static Key Register, Data Register, Static Data Register, IV Register and Temp Register) is performed internally and automatically by this device.

REGISTER DESCRIPTIONS

Table 3-10 : Command Register

This 8-bit read/write register controls the operation of the CA20C03A/W. It is normally loaded only once for an entire encryption or decryption process.

Bits	Function							
7-0	CBC/$\overline{\text{ECB}}$	NK	BB	n/u	E/D	KEOE	ACT	N/O

Name	Description
NEW/OLD (N/O)	When logic 0, the DES device is backward compatible with the WD2001 device in both hardware & software. When logic 1, the DES device is in CA20C03A/W mode.
ACTIVATE (ACT)	This bit must be logic 1 for encrypt/decrypt operation. When this bit is set from logic 0 to logic 1, one of the following events happen: • Initiates loading the Key Register in non-battery back-up key mode. • Initiates loading the Key Register in Battery Back-up Key mode while NK (command bit) is logic 1 • Initiates *Special Pattern-in Request* in Battery Back-up Key mode while NK = 0 and KV (status bit) is logic 1. • Initiates a *Data-in Request* in *Battery Back-up Key* mode while NK = 0, KV = 0, and CBC/$\overline{\text{ECB}}$ (command bit) is logic 0. • Initiates an *Initial Vector-in Request* in *Battery Back-up Key* mode while NK = 0, KV = 0 and CBC/$\overline{\text{ECB}}$ = 1.
KEY ERROR OUTPUT	When logic 0, the KEY PARITY ERROR output pin ($\overline{\text{KPE}}$) remains inactive regardless of the status of the KEY PARITY ERROR bit (status bit 5). When logic 1, the KEY PARITY ERROR output pin is active when the KPE bit (status bit 5) is logic 1. This bit set to logic 1 upon a $\overline{\text{MASTER RESET}}$.
ENCRYPT/DECRYPT (E/D)	When logic 0, data is to be encrypted. When logic 1, data is to be decrypted.
n/u	Not used.
BATTERY BACK-UP KEY (BB)	When logic 0, the DES device is in non-battery back-up key mode. When logic 1, the DES device is in *Battery Back-up Key* mode. This bit is only used in the CA20C03A device.
NEW KEY REQUEST (NK)	This bit is ignored in non-battery back-up key mode. While in *Battery Back-up Key* mode, a *key request* is initiated when NK = 1, or the device skips the key loading process and does either the Cipher Block Chaining process or the Electronic Code process when NK = 0. This bit is only used in the CA20C03A device.
CIPHER BLOCK CHAINING/ $\overline{\text{ELECTRONIC CODE BOOK}}$ (CBC/$\overline{\text{EBC}}$)	When logic 0, the DES device encrypts/decrypts data using the Electronic Code Book method. When logic 1, the DES device encrypts/decrypts data using the Cipher Block Chaining method.

Note: All bits of the Command Register are reset to logic 0 upon $\overline{\text{MASTER RESET}}$ when $\overline{\text{CRPS}}$ = 1, except bit 2 (KEOE) which is set to 1. When $\overline{\text{CRPS}}$ = 0, this register is disregarded after $\overline{\text{MASTER RESET}}$.

Table 3-11 : Status Register

This 8-bit read-only register monitors the status of the device.

Bits	Function							
7-0	DOR	DIR	KPE	KR	IVIR	SPIR	RLK	KV

Name	Description
KEY VERIFICATION REQUEST (KV)	If the $\overline{CRPS}$ pin is logic 1, this bit is set each time the N/O bit of the Command request (KV) Register is set from logic 0 to logic 1. If the $\overline{CRPS}$ pin is logic 0 and N/O is logic 0, this bit is set upon each $\overline{MASTER\ RESET}$. It is reset at the end of the *Key Verification* process while the *Key* is valid, or at the end of the *Key Reloading* process. This bit is only used in the CA20C03A device.
RELOAD KEY REQUEST (RLK)	This bit is set when the user requests a new Key (NK = 1) in *Battery Back-up Key* mode (BB = 1) or at the end of the *Key Verification* process when the Key is found not valid. When this bit is set, the *Key Reloading* process starts. This bit is reset at the end of the *Key Reloading* process. The reset occurs when the encrypted *Special Pattern* (encrypted by the new loaded *Key*) is loaded into the Static Data Register from the Data Register. If this bit becomes set, it can only be cleared through the *Key Reloading* process or by performing a Master Reset (i.e. deactivating the device by writing to the command registers will not reset this bit). This bit is only used in the CA20C03A device.
SPECIAL PATTERN-IN REQUEST (SPIR)	This bit is set to logic 1 when the ACT bit is programmed from logic 0 to logic 1, BB = 1, NK = 0, and KV = 1, or when KR is reset from logic 1 to logic 0 and RLK = 1. It is reset upon loading of the last (8th) byte of the *Special Pattern* into the Data Register. This bit is only used in the CA20C03A device.
INITIAL VECTOR-IN REQUEST (IVIR)	This bit is set to logic 1 upon one of the following conditions: • Completion of Key Register loading while BB = 0 and CBC/$\overline{ECB}$ = 1. • Completion of *Key Reloading* process while BB = 1 and CBC/$\overline{ECB}$ = 1 (CA20C03A device only). • Completion of *Key Verification* process and the *Key* being found valid while BB = 1 and CBC/$\overline{ECB}$ = 1 (CA20C03A device only). • The ACT bit is set from logic 0 to logic 1 while BB = 1, NK = 0, KV = 0 and CBC/$\overline{ECB}$ = 1 (CA20C03A device only). This bit is reset upon loading of the last (8th) byte of the *Initial Vector.*
KEY REQUEST (KR)	This bit is set to logic 1 when ACT is programmed from logic 0 to logic 1 and BB = 0 or, when RLK is set internally from logic 0 to logic 1 (CA20C03A device only). It is reset upon loading of the last (8th) byte of the Key Register.
KEY PARITY ERROR (KPE)	This bit is set internally upon detection of a parity error during loading of the Key Register. It is reset when ACT is programmed from logic 1 to logic 0 (i.e., the device is deactivated).
DATA-IN REQUEST (DIR)	This bit is set to logic 1 upon one of the following conditions: • Completion of Key Register loading while BB = 0 and CBC/$\overline{ECB}$ = 0. • Completion of the *Key Reloading* process while BB = 1 and CBC/$\overline{ECB}$ = 0 (CA20C03A device only). • Completion of the *Key Verification* process and the *Key* being found valid while BB = 1 and CBC/$\overline{ECB}$ = 0 (CA20C03A device only). • The ACT bit is set from logic 0 to logic 1 while BB = 1, NK = 0, KV = 0 and CBC/$\overline{ECB}$ = 0 (CA20C03A device only). • Completion of IV Register loading while BB = 1 and CBC/$\overline{ECB}$ = 1 (CA20C03A device only). • Completion of Data Register reading (i.e.: the last *Data-out Request* has been serviced by an 8-byte read and the Data Register is now emptied and ready to be loaded with the next Data Word). This bit is reset upon loading of the last (8th) byte of the Data Register.
DATA-OUT REQUEST (DOR)	This bit is set upon completion of the internal encrypt/decrypt calculation of a *Data Word.* It is reset upon reading the last (8th) byte of the Data Register.

Note: Upon $\overline{MASTER\ RESET}$ and $\overline{CPRS}$ is logic 1, the Status Register is not addressable because the device comes up in the WD2001 mode. Once the Command Register is programmed into the new mode (write 1 to the N/O bit) the Status Register is addressable and will have all bits reset to 0, except the KV bit which is set to a logic 1. When $\overline{CPRS}$ = 0 and A1, O/$\overline{N}$ = 0, all bits are reset to 0 except KV (bit 0) which is set to logic 1.

Table 3-12 : KEY Register (Load Only)

This 56-bit register contains the *Key* which is used to encrypt or decrypt the data with the DES algorithm. The Key Register can be loaded with eight successive bytes only when there is a *Key Request* (status bit and output). The Key Register can also be parallel loaded from Static Key Register in Battery Back-up Key mode. This is a *write-only* register.

DATA Reg. Bits	55..49	48..42	•••	15..07	06..00
DAL Bits	7..1	7..1	•••	7..1	7..1
Byte Loaded	1st	2nd	•••	7th	8th

Table 3-13 : STATIC KEY Register (CA20C03A Only)

This 56-bit register contains the current *Key* for data encryption and decryption using the DES algorithm. The Static Key Register is updated when a new *Key* is loaded into the Key Register and when the device is programmed for *Battery Back-up* mode. The contents of this register are retained by battery power during power-down or power failure. If the device is programmed for a mode without a Battery Back-up Key, this register is not used. The register is not accessible to the user.

DATA Reg. Bits	55..49	48..42	•••	15..07	06..00
DAL Bits	7..1	7..1	•••	7..1	7..1
Byte Loaded	1st	2nd	•••	7th	8th

Table 3-14 : DATA Register

This 64-bit register contains the plain or cipher text either to be read out or that has been loaded in. During encryption, the Data Register is loaded with plain text and contains cipher text to be read out. During decryption, the Data Register is loaded with cipher text and contains plain text to be read out. The Data Register is always read or loaded with eight successive bytes (8-bit).

The Data Register can only be loaded when there is a *Data-in Request* or *Special Pattern-in Request* (Status bit and Output). Similarly, the Data Register can only be read when there is a *Data-out Request* (Status bit and Output). However, when the device is programmed for a mode with Battery Back-up, the contents of this register can be parallel loaded into the Static Data Register when the special pattern for key verification is encrypted.

DATA Reg. Bits	63..56	55..48	•••	15..8	07..00
DAL Bits	7..0	7..0	•••	7..0	7..0
Byte Loaded	1st	2nd	•••	7th	8th

Table 3-15 : STATIC DATA Register (CA20C03A Only)

This 64-bit register contains the encrypted special pattern for key verification. When the device is programmed for a mode with a Battery Back-up, the Static Data Register is updated whenever a new key is loaded in. The special pattern is loaded in the Data Register and encrypted by the new key, then the new encrypted special pattern is loaded into the Static Data Register. The contents of this register are retained by battery power during power-down or power failure. If the device is programmed for a mode without a Battery Back-up Key, the Register is not used. This register is not accessible to the user.

DATA Reg. Bits	63..56	55..48	•••	15..8	07..00
DAL Bits	7..0	7..0	•••	7..0	7..0
Byte Loaded	1st	2nd	•••	7th	8th

Table 3-16 : INITIAL VECTOR (IV) Register

This 64-bit register contains the initial vector or cipher text for the *Cipher Block Chaining* mode. This register is first loaded with the eight successive bytes (8-bit) of the Initial Vector Register for the first block of plain or cipher text. After the current text in the Data Register (plain or cipher) has been processed (encrypted or decrypted), this register is loaded with the current cipher text from the Data Register (encrypt) or the next block of text from the Temp Register (decrypt). This register is not used in the *Electronic Code Book* mode.

DATA Reg. Bits	63..56	55..48	•••	15..8	07..00
DAL Bits	7..0	7..0	•••	7..0	7..0
Byte Loaded	1st	2nd	•••	7th	8th

Table 3-17 : TEMP Register

This 64-bit register is a temporary storage place used in the *Cipher Block Chaining* mode. This register temporarily stores the current cipher text, before this text is loaded into the IV Register during the decryption process. This register is loaded with the eight bytes of cipher text from the Data Register. It is not used in the *Electronic Code Book* mode and is not accessible to the user.

DATA Reg. Bits	63..56	55..48	•••	15..8	07..00
DAL Bits	7..0	7..0	•••	7..0	7..0
Byte Loaded	1st	2nd	•••	7th	8th

DES ENCRYPTION MODES

Electronic Code Book (ECB) Mode Overview

The Electronic Code Book is a direct implementation of the DES algorithm in which the same plain text always generates the same ciphered text for a given cryptographic key. The CA20C03A/W determines the codebook entries each time. A single bit error or change, in either the input text block or the key, causes an average bit error rate of 50% for its output block. However, an error in one text block does not affect any other block. In other words, there is no error extension between blocks generated using the ECB mode.

The input and output block size is fixed at 64 bits. Since data blocks are independently ciphered, this mode is suitable for disk applications (see Figure 9).

The ECB mode has the weakness that identical block of plain text generate identical blocks of ciphered text. This violates one of the basic laws of encryption security, namely: never encrypt a given piece of information the same way twice as it makes it easier for an attacker to break the code. This shortcoming in the ECB mode is resolved by the Cipher Block Chaining mode.

Cipher Block Chaining (CBC) Mode Overview

The Cipher Block Chaining mode also operates on 64 bit data blocks, but preprocesses the information before passing it to the DES algorithm. An input data block is first EXORed with a 64 bit *Initial Vector* (IV), then processed by the DES algorithm. The resulting ciphered-output block is loaded into the IV Register, to be EXORed with the next input block. This chaining of cipher text blocks provides different outputs for identical input blocks. It also gives an error extension characteristic which protects against fraudulent data insertion, deletion or alteration in a block sequence (see Figure10). A one-bit error in the input text block, the key or the *Initial Vector* causes an average error rate of 50% in all subsequent output blocks. Thus, the CBC mode is far better suited to high-speed data communications applications.

Cipher Feedback (CFB) and Output Feedback (OFB)

These two DES modes can be implemented with the CA20C03A/W using the ECB mode with additional software overhead. For more information refer to the publication: *Cryptography and Data Security*, by D. Denning, Addison-Wesley Publishing Company, Inc., 1982.

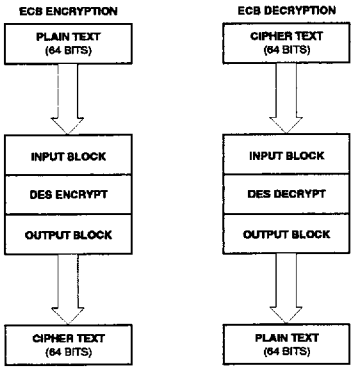


Figure 3-9 : Electronic Codebook (ECB) Mode

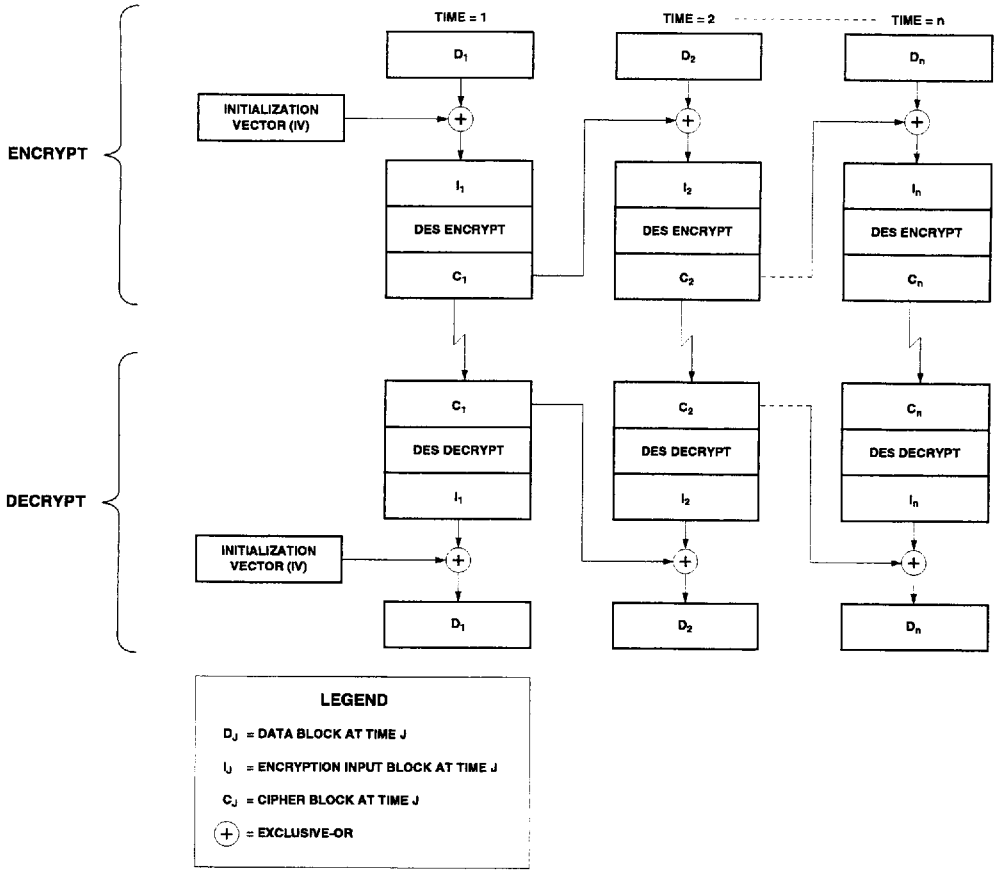


Figure 3-10 : Cipher Block Chaining (CBC) Mode

CA20C03A/W MODES of OPERATION

The CA20C03A/W can operate in two major encryption modes: Electronic Code Book (ECB) mode and Cipher Block Chaining (CBC) mode (each an implementation of the DES algorithm). Each of these two modes can be selected with or without Battery Back-up, giving a total of four operational modes (for the CA20C03A):

- Electronic Code Book without a Battery Back-up Key
- Cipher Block Chaining without a Battery Back-up Key
- Electronic Code Book with a Battery Back-up Key
- Cipher Block Chaining with a Battery Back-up Key

The CA20C03W only supports the non Battery Back-up modes of encryption. The CA20C03A/W can also be programmed to operate in a WD2001 mode, which offers ECB type encryption only. When the N/O bit is programmed to logic 1, the device is in the CA20C03A/W mode, and either ECB or CBC type encryption modes can be selected. When the N/O bit is logic 0, the device is in WD2001 mode. All modes are described in more detail below.

WD2001 Compatibility Mode

To ensure backward compatibility with the WD2001 device, the CA20C03A/W can also be programmed to emulate functions in the WD2001 (ECB mode only). This is determined by the setting of bit 0 (N/O) in the Command Register, which indicates whether the CA20C03A/W is in WD2001 mode (ECB) or in CA20C03A/W mode (ECB or CBC). When the N/O bit is programmed to logic 0, the device is in the WD2001 mode (ECB) and only the Command/Status, Data, and Key Registers are then available. The pinouts and the operation of the device and the functions of the three registers in this mode are exactly the same as in the WD2001 (refer to CA20C01 data sheet for detailed operational information). If WD2001 mode is in use in a CA20C03A device, pin 6 of the device can be connected to +5 V, or left unconnected. If WD2001 mode is in use with a CA20C03W device, then pin 6 can still be connected to +12 V without harming the device.

***Caution:** Pin 6 of a CA20C03A device must not be connected to +12 V as it will irreparably damage the device.*

Electronic Code Book without a Battery Back-up Key

The CA20C03A/W operates in this mode when bit 5 (BB), and bit 7 (CBC/$\overline{\text{ECB}}$) in the Command Register are set to logic 0. After the device is selected to be in this mode, it is initiated by setting bit 1 (ACT) in the Command Register to logic 1. The CA20C03A/W responds by activating the KEY REQUEST (KR, pin 26) output.

A0 must be deactivated (to allow the CA20C03A/W to internally address the Key Register) before loading the 64-bit *Key Word* into the Key Register. The Key Register is loaded with eight successive bytes (8-bit) by activating$\overline{\text{WE}}$ eight times (with $\overline{\text{CS}}$ active).

When $\overline{\text{WE}}$ is activated, the CA20C03A/W deactivates the KEY REQUEST (KR) output. When $\overline{\text{WE}}$ is deactivated, the CA20C03A/W activates the KR output. The CA20C03A/W activates eight *Key Requests* to fill up the Key Register.

Table 3-18 : CA20C03A/W Register Select

Register	$\overline{\text{CS}}$	A0	A1	$\overline{\text{CRPS}}$
Status	0	1	1	1
Command	0	1	0	1
Key, IV and Data	0	0	X	1

X = Don't care

The KR output can either be used for asynchronous handshaking (as in DMA control) or, after the first activated KR, further activations can be ignored and the Key Register can be loaded synchronously (as in programmed I/O) by eight successive activations of $\overline{\text{WE}}$.

Each byte of the *Key Word* is checked for odd parity when it is loaded into the Key Register (see Figure 3-11). If a parity error is detected, the CA20C03A/W sets bit 5 (KPE, KEY PARITY ERROR) in the Status Register to logic 1. If bit 2 (KEOE, KEY ERROR OUTPUT ENABLE) in the Command Register has been set, the device also activates the $\overline{\text{KPE}}$ (pin 22) output. Bit 5 (KPE, KEY PARITY ERROR) in the Status Register is reset to logic 0 when bit 1 (ACT, ACTIVATE) in the Command Register is reset to logic 0.

After loading the eighth byte of the *Key Word* into the Key Register, the CA20C03A/W sets DIR, DATA-IN REQUEST in the Status Register and activates the DATA-IN REQUEST (DIR, pin 27) output (see Figure 3-12). The 64-bit *Data Word* should then be loaded into the Data Register, which is loaded in the same manner as the Key Register by eight successive activations of DATA-IN REQUEST (DIR, pin 27) output and $\overline{\text{WE}}$ input.

After the eighth (last) byte of the *Data Word* has been loaded, the CA20C03A/W starts its operation internally by encrypting or decrypting the data to the DES algorithm. Upon completion of this operation, the encrypted or decrypted data is loaded into the Data Register, the CA20C03A/W sets bit 7 (DOR, DATA-OUT REQUEST) in the Status Register and activates the DATA-OUT REQUEST (DOR, pin 28) output (see Figure 3-13).

The *Data Word* must then be read from the Data Register in the same manner as it was loaded (by eight successive activations of DATA-OUT REQUEST output and $\overline{RE}$ input).

After the first request, further activations of the DIR and DOR outputs can be ignored and the Data Register can be loaded or read by eight successive activations of $\overline{WE}$ or $\overline{RE}$.

After the eighth (last) byte of the Data Register has been read, the CA20C03A/W reactivates the DATA-IN-REQUEST. The cycle of loading the Data Register, encrypting or decrypting of the data to the DES algorithm, and reading the new data from the Data Register is repeated until all required data has been encrypted or decrypted with the current *Key Word*. Figures 3-11 to 3-13 are flowcharts which will aid in the understanding of the device operation in this mode.

When this is completed, bit 1 (ACT, ACTIVATE) in the Command Register should be reset to logic 0 to lock the last *Key Word* loaded into the CA20C03A/W. This prevents the access and use by an unauthorized user. To resume operation, the *Activate* bit must be reset to logic 1. This activates the *Key Request* and a new Key must be loaded before the Data Register can be accessed.

Plain data is encrypted by loading it into the Data Register, and encrypted data is read from the Data Register after E/$\overline{D}$, $\overline{ENCRYPT}$ /DECRYPT in the Command Register has been set to logic 0.

Data is decrypted by loading it into the Data Register, and plain data is read from the Data Register after E/$\overline{D}$, $\overline{ENCRYPT}$ /DECRYPT in the Command Register has been set to logic 1.

Caution: *To accomplish switching from encryption to decryption (or vice versa) with the same Key Word before a Data Word transfer is initiated, A0 must be set to 1 and A1 to 0. The CA20C03A/W then overrides the internal addressing of the Data Register and addresses the Command Register, which can now be reprogrammed. When A0 is deactivated, the device then internally addresses the Data Register, while awaiting the loading of the next Data Word.*

Cipher Block Chaining without a Battery Back-up Key

The CA20C03A/W operates in this mode when bit 5 (BB) and bit 7 (CBC/$\overline{EBC}$) in the Command Register are set respectively to logic 0 and logic 1. Once the device is programmed in this mode, it can be initiated by setting bit 1 (ACT) in the Command Register to logic 1. The CA20C03A/W now responds by activating the KEY REQUEST (KR) output. Refer to Table 3-18 for register selection.

A0 must be deactivated (to address the Key Register internally), and the Key Register must be loaded with the 64-bit *Key Word* in the same manner as performed in the Electronic Code Book mode without a Battery Back-up Key.

When the eighth (last) byte of the *Key Word* is loaded in the Key Register, the CA20C03A/W sets bit 3 (IV-IN REQUEST) in the Status Register and activates the IV-IN REQUEST (IVIR) output. The 64-bit *Initial Vector Word* must then be loaded into the IV Register in the same manner as the Key Register was loaded, that is, by eight successive activations of IV-IN REQUEST output and $\overline{WE}$ input.

After the eighth (last) byte of the *Initial Vector Word* has been loaded, the CA20C03A/W sets bit 6 (DATA-IN REQUEST) in the Status Register and activates the DATA-IN REQUEST (DIR) output. The 64-bit *Data Word* must then be loaded into the Data Register in the same manner as the Key Register was loaded, that is, by eight successive activations of DATA-IN REQUEST output and $\overline{WE}$ input.

The plain text is loaded into the Data Register when the $\overline{ENCRYPT}$ /DECRYPT bit has been set to logic 0. When this is completed, that is, after the eighth (last) byte of the plain Data Word has been loaded into the device, the contents of the IV Register are added to the plain text consecutively bit by bit with modulo 2 arithmetic and the CA20C03A/W begins the internal calculation of the DES algorithm for the cipher text.

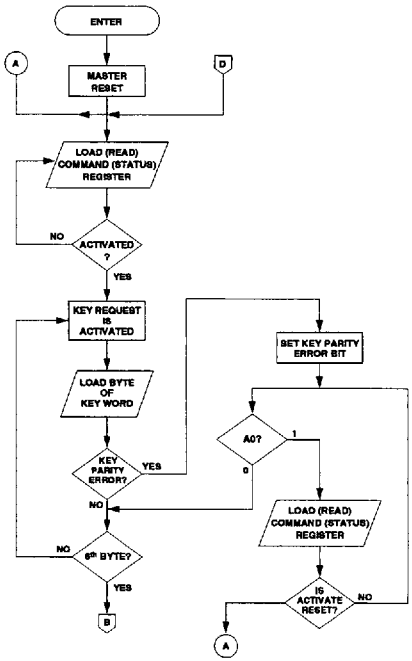


Figure 3-11 : Key Word Loading Procedure (ECB Mode Only)

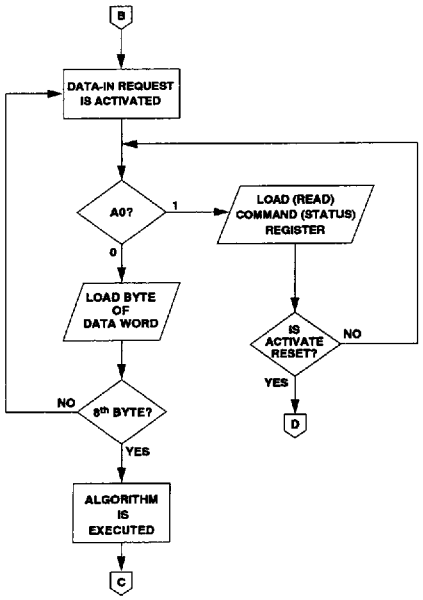


Figure 3-12 : Activating DIR Output Procedure (ECB Mode Only)

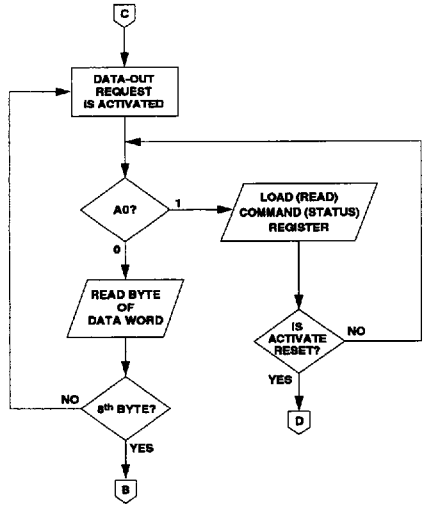


Figure 3-13 : Activating DOR Output Procedure (ECB Mode Only)

When completed, this data is loaded into both the Data Register and the IV Register (where it overrides the original *Initial Vector Word*). After (parallel) loading the new data into these two registers, the CA20C03A/W sets bit 7 (DATA-OUT REQUEST) in the Status Register and activates the DATA-OUT REQUEST (DOR) output.

The new cipher *Data Word* must then be read from the Data Register in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST output and $\overline{RE}$ input.

After the eighth (last) byte of the Data Register contents have been read, the CA20C03A/W reactivates the DATA-IN REQUEST and the next cycle can begin. This continues until all required (plain) data has been encrypted with the current Key Word in the manner previously described, that is, by:

- Loading the Data Register with plain text
- Adding the (previous) cipher text contents of the IV Register to the contents of the Data Register
- Calculating the DES algorithm for cipher text
- Loading it into the IV Register for operation (addition) to the 64-bit (plain) *Data Word*
- Reading it (cipher text) from the Data Register.

When decrypting, bits 1 (ACT) and bit 3 ($\overline{\text{ENCRYPT}}$ /DECRYPT) in the Command Register are set to 1 respectively. This activates the KEY REQUEST output indicating that the original key must now be loaded into the Key Register. After the key is loaded, the CA20C03A/W requests that the initial vector be loaded into the IV Register. When this is completed, the data request input pin is activated and the first eight bytes of cipher data need to be loaded into the Data Register. After the eight bytes of the cipher Data Word have been loaded into the device, the contents of the Data Register are transferred into the Temp Register and the CA20C03A/W begins the internal calculation of the DES algorithm for clear data. When completed, this data is added consecutively bit by bit to the contents of the IV Register using modulo 2 arithmetic. The modified plain text data is then loaded into the Data Register while the contents of the Temp Register are loaded into the IV Register, overriding the existing *Initial Vector.*

After completion of these operations, bit 7 (DATA-OUT REQUEST) in the Status Register is set and the DATA-OUT REQUEST (DOR) output is activated. The plain *Data Word* must then be read from the *Data Request* in the same manner as it was loaded, that is, by eight successive activations of DATA-OUT REQUEST output and $\overline{RE}$ input.

After the eighth (last) byte of the Data Register contents have been read, the CA20C03A/W reactivates the DATA-IN REQUEST and the next cycle can begin. This continues until all required (cipher) data has been decrypted with the current *Key Word* in the manner previously described:

- Load the Data Register with *cipher text*
- Load the contents of the Data Register into the Temp Register
- Calculate the DES algorithm for clear text
- Add the clear text contents in the Temp Register to the (previous) cipher text contents in the IV Register
- Load plain text into the Data Register
- Transfer the contents of the Temp Register to the IV Register for the next 64-bit cipher *Data Word*
- Read plain text from the Data Register.

As previously explained, for DATA-IN, IV-IN, and DATA-OUT, after the first request, further activations of DIR, IVIR, and DOR outputs aren't necessary. Loading the IV Register and the Data Register is performed by eight successive activations of $\overline{WE}$ and reading the Data Register is performed by eight successive activations of $\overline{RE}$.

When all required data has been encrypted or decrypted with the current *Key Word*, bit 1 (ACTIVATE) in the Command Register should be programmed to logic 0 to lock the last *Key* loaded into the CA20C03A/W. This prevents the access and use of it by an unauthorized user. To resume operation, the activate bit must be programmed to logic 1. This activates the *Key Request* and a new *Key* must be loaded before the Data Register can be accessed.

Caution: *At the end of each encrypted or decrypted file (or message), the CA20C03A/W is waiting for the Data Word, not for the reloading of the Initial Vector: that is, DIR output is active. In order to activate the IVIR output and re-load the Initial Vector, the device has to be restarted. This can be accomplished by deactivating the CA20C03A/W and then reactivating it once more. This forces the re-loading of the Key Word. This procedure should be followed even when it is desired to use the same Key Word for the encryption or decryption of the next file (or message).*

Electronic Code Book with a Battery Back-up Key

The CA20C03A operates in this mode when bit 5 (BB) and bit 7 (CBC/$\overline{ECB}$) in the Command Register are set respectively to logic 1 and logic 0 (this does not apply to the CA20C03W). After the device is programmed for this mode, it is initiated by setting the ACT bit in the Command Register to logic 1. The CA20C03A responds in one of the following ways:

- When bit 6 (NK, NEW KEY) in the Command Register is set to logic 1, the CA20C03A responds by setting bit 1 (RLK, RELOAD KEY) and bit 4 (KR, KEY REQUEST) in the Status Register. It also sets the KEY REQUEST output in the *Key Reloading* state.

  Caution: *The RLK bit can only be reset by the Key Reloading process or by performing a Master Reset. Deactivating the device by writing to the Command Register will not reset this bit.*

  A0 needs to be deactivated to allow the CA20C03A to select the Key Register internally and load it with the 64-bit *Key Word* (in the same manner as in the Electronic Code Book mode without a Battery Back-up Key). Refer to Table 16 for register selection.

  When the eighth (last) byte of the *Key Word* has been loaded into the Static Key Register then bit 2 (SPECIAL PATTERN-IN REQUEST) in the Status Register is set and the SPECIAL PATTERN-IN REQUEST (SPIR, pin 4) output is activated.

  The 64-bit *Special Pattern* must now be loaded into the Data Register in the same manner as the Key Register, that is, by eight successive activations of SPECIAL PATTERN-IN REQUEST input and WE input.

  When the eighth byte of the *Special Pattern* has been loaded into the Data Register, the device starts to encrypt the *Special Pattern Word* in Electronic Code Book mode. Upon completion of the DES algorithm calculation, the cipher data is then loaded into the Static Data Register, and the CA20C03A resets RELOAD KEY bit and the KEY VERIFICATION bit in the Status Register. The device is now out of the *Key Reloading* state and continues in Electronic Code Book mode by setting bit 6 (DATA-IN REQUEST) in the Status Register and activating the DATA-IN REQUEST (DIR, pin 27) output.

- When bit 6 (NEW KEY) in the Command Register is set to logic 0 and bit 0 (KEY VERIFICATION) in the Status Register is set to logic 1, the CA20C03A responds by setting bit 2 (SPECIAL PATTERN-IN) in the Status Register. The device also activates the SPECIAL PATTERN-IN (SPIR) output, loads the contents of the Static Key Register into the Key Register in order to encrypt the *Special Pattern*, and enters the *Key Verification* state.

  A0 must be deactivated (to allow the CA20C03A to address the Data Register internally) and the Data Register must be loaded with the 64-bit *Special Pattern Word* in the same manner as the Key Register was loaded, that is, by eight successive activations of SPECIAL PATTERN-IN REQUEST output and $\overline{WE}$ input.

  When the eighth byte of the Special Pattern has been loaded into the Data Register, the CA20C03A starts to encrypt the *Special Pattern Word* in the *Electronic Code Book* mode. Upon the completion of the DES algorithm calculation, the cipher data is compared with the contents of the Static Data Register.

  If they are not the same, the CA20C03A sets bit 1 (RELOAD KEY) and bit 4 (KEY REQUEST) in the Status Register and activates the KEY REQUEST (pin 26) output to start the *Key Reloading* process as was previously described. Upon the completion of the *Key Reloading* operation, the device sets bit 6 (DATA-IN REQUEST) in the Status Register and activate the DATA-IN REQUEST (DIR, pin 27) output to start the Electronic Code Book mode.

  If the new cipher data and contents of the Static Data Register are the same, the CA20C03A resets bit 0 (KEY VERIFICATION), sets bit 6 (DATA-IN REQUEST) in the Status Register, and activates the DATA-IN REQUEST (DIR, pin 27) output to start the *Electronic Code Book* mode.

- When bit 6 (NEW KEY) in the Command Register is set to logic 0 and bit 0 (KEY VERIFICATION) in the Status Register is set to logic 0, the CA20C03A loads the contents of the Static Key Register into the Key Register, sets bit 6 (DATA-IN REQUEST) in the Status Register and activates the DATA-IN REQUEST (DIR, pin 27) output to start the Electronic Code Book mode. The operation is the same as previously described in the *Electronic Code Book* mode without a *Battery Back-up Key*.

Note that to accomplish switching from encryption to decryption (or vice versa) without deactivating the CA20C03A, and before a *Data Word* transfer is initiated, A0 must be set to 1 and A1 to 0 to address the Command Register and override the addressing of the Data Register internally. The Command Register can now be re-programmed. When A0 is reset to logic 0, the CA20C03A will now address the Data Register internally while awaiting the loading of the next *Data Word*.

Cipher Block Chaining with a Battery Back-up Key

The CA20C03A operates in this mode when the BB and CBC/$\overline{ECB}$ bits in the Command Register are set to logic 1 (this does not pertain to the CA20C03W). After the device is programmed for this mode, it is initiated by setting the ACT bit in the Command Register to logic1.

The CA20C03A responds in one of the three ways previously described in the section *Electronic Code Book with a Battery Back-up Key*. However, after completion of the *Key Reload* or *Key Verification* operations, the device starts operating in the Cipher Block Chaining mode instead of the *Electronic Code Book* mode. It sets INITIAL VECTOR-IN REQUEST in the Status Register and activates the INITIAL VECTOR-IN REQUEST (IVIR) output.

When the CA20C03A is in the *Cipher Block Chaining* mode, its operation is the same as previously described in *Cipher Block Chaining without a Battery Back-up Key*. A sample battery back-up circuit is shown in Figure 14.

Note that at the end of each encrypted or decrypted file (or message), the CA20C03A is waiting for the *Data Word*, not for the reloading of the *Initial Vector*; that is, DIR output is active. In order to activate the IVIR output and re-load the Initial Vector, the device has to be re-started by deactivating and then reactivating it. This restart procedure forces the re-loading of the *Key Word* and should be followed even when the same *Key Word* is desired for the encryption or decryption of the next file (or message).

Command Select Option

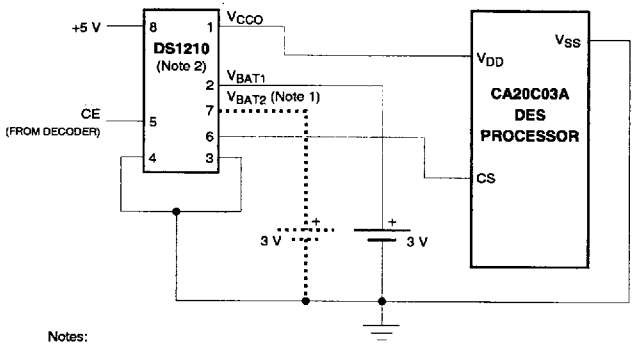
The CA20C03A/W can be programmed through the DAL bus lines or through the input pins. When the COMMAND REGISTER PIN SELECT ($\overline{\text{CRPS}}$, pin 20) input is set to logic 0, the (A1,O/$\overline{\text{N}}$), ACT, E/$\overline{\text{D}}$, BB, (A0,NK), and CBC/$\overline{\text{ECB}}$ pins are enabled as inputs which override bits 0, 1, 3, 5, 6, and 7 in the Command Register. This override allows input pins to control the CA20C03A/W. Bit 2 (KEOE) in the Command Register remains at logic 1.

The A1 and A0 bits are disregarded in this option, and the Command and Status Registers cannot be accessed using the DAL bus lines.

Note that the ACT pin must be toggled from logic 1 to logic 0 to clear a parity error detection when operating in this mode.

All other operations are the same as described previously.

Caution: *Upon* $\overline{\text{MASTER RESET}}$ *, while* $\overline{\text{CRPS}}$ *and A1,O/*$\overline{\text{N}}$ *pins are logic 0, the CA20C03A/W does not return to the 2001 mode, but stays in the CA20C03A/W mode and sets bit 0 (KV) in the Status Register.*



Notes:

1. V_{BAT2} is optional (use if double redundant back-up is required for failsoft operation).
2. Dallas Semiconductor DS1210 Non-volatile Controller.

Figure 3-14 : CA20C03A Battery Back-up Circuit Example

Table 3-19 : Test Data For Electronic Codebook (ECB) Mode

E-Key=D-Key= 0123456789ABCDEF		
Encryption		
Time	**Plain Text**	**Cipher Text**
1	4E6F772069732074	3FA40E8A984D4815
2	68652074696D6520	6A271787AB8883F9
3	666F7220616C6C20	893D51EC4B563B53
Decryption		
Time	**Cipher Text**	**Plain Text**
1	3FA40E8A984D4815	4E6F772069732074
2	6A271787AB8883F9	68652074696D6520
3	893D51EC4B563B53	666F7220616C6C20

Table 3-20 : Test Data For Cipher Block Chaining (CBC) Mode

E-Key = D-Key = 0123456789ABCDEF IVE = IVD = 1234567890ABCDEF		
Encryption		
Time	**Plain Text**	**Cipher Text**
1	4E6F772069732074	E5C7CDDE872BF27C
2	68652074696D6520	43E934008C389C0F
3	666F7220616C6C20	683788499A7C05F6
Decryption		
Time	**Cipher Text**	**Plain Text**
1	E5C7CDDE872BF27C	4E6F772069732074
2	43E934008C389C0F	68652074696D6520
3	683788499A7C05F6	666F7220616C6C20

Note for Table 3-19 and Table 3-20: The plain text in both cases is the ASCII code for "Now is the Time for all ...". These seven-bit characters are written in hexadecimal notation: 0, b6, b5, b4, b3, b2, b1, b0.

- **Encrypts/Decrypts data using National Bureau of Standards Data Encryption Standard (DES)**
- **High speed, pin and function compatible version of industry standard AMD AM9568, AM9518 and VLSI VM009**
- **Supports four standard ciphering modes: Electronic Code Book (ECB), Cipher Block Chaining (CBC), as well as 1 and 8 bit Cipher Feedback (CFB)**
- **Data rates greater than 11 Mbytes per second (25 MHz) in ECB or CBC modes**
- **Three separate registers for encryption, decryption and master keys improve system security and throughput by eliminating the need to reload keys frequently**
- **Fully static CMOS, TTL I/O compatible device, operates at up to 25MHz**
- **Low power consumption allows battery back-up of internal key registers**
- **Three separate programmable ports (master, slave and key data)**
- **Available in 44 pin PLCC and 40 pin PDIP and 44 pin TQFP packages**

The *Newbridge Microsystems* CA95C68/18/09 DES Data Ciphering Processors (DCPs) implement the National Bureau of Standards Data Encryption Standard (DES), FIPS PUB 46 (1-15-1977). The DCPs were designed to be used in a variety of environments where computer and communications security is essential.

The DCPs provide a high throughput rate (up to 11 Mbytes per second) using ECB or CBC modes of operation. The DCPs provide a unique 1 bit CFB mode as well as the standard 8 bit mode. Separate ports for key input, clear data and enciphered data enhance security for your application.

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

The CA95C68 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. The CA95C18 is designed to interface directly with Z8000, 68000 type bus interfaces.

The CA95C09 may be configured to behave as either the CA95C68 or the CA95C18 (see OPTION pin in Table 3-2), the only difference being the order of the signal names on the device package.

Table 3-1 : CA95C68/18/09 Data Transfer Rates

Product Code	Data Transfer Rates			System Clock (MHz)
	ECB or CBC Mode (Mbytes/s)	CFB-8 Mode (Mbytes/s)	CFB-1 Mode (Mbits/s)	
CA95Cxx – 5	2.22	0.27	0.27	5
CA95Cxx – 10	4.44	0.55	0.55	10
CA95Cxx – 16	7.10	0.88	0.88	16
CA95Cxx – 20	8.88	1.11	1.11	20
CA95Cxx – 25	11.11	1.38	1.38	25

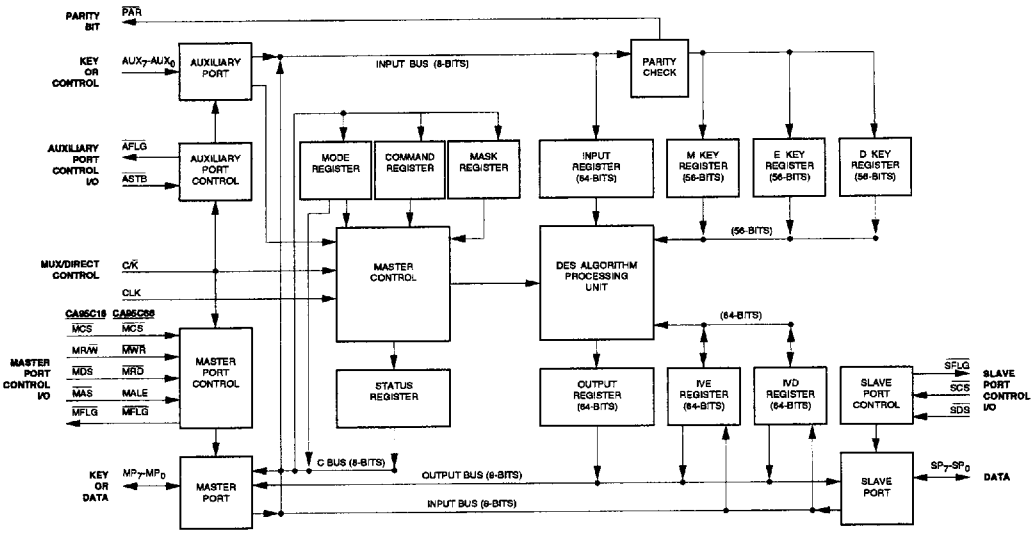


Figure 3-1 : CA95C68/18/09 Block Diagrams

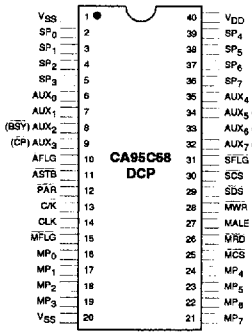


Figure 3-2 : CA95C68 40-Pin PDIP

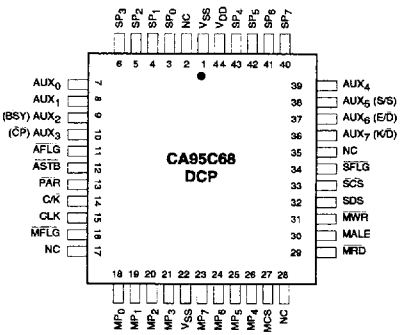


Figure 3-5 : CA95C68 44-Pin PLCC

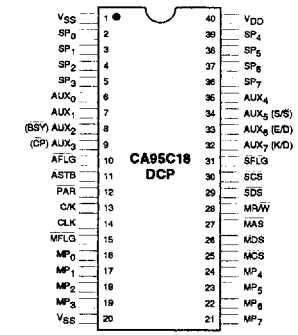


Figure 3-3 : CA95C18 40-Pin PDIP

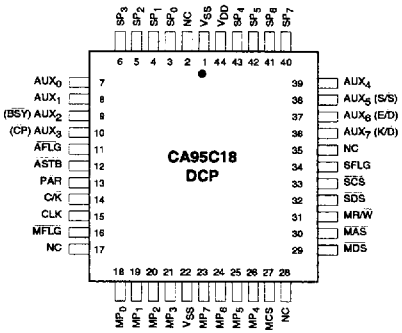


Figure 3-6 : CA95C18 44-Pin PLCC

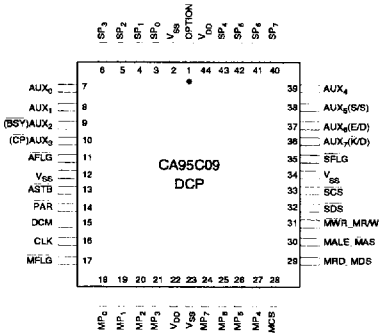


Figure 3-4 : CA95C09 44-Pin PLCC

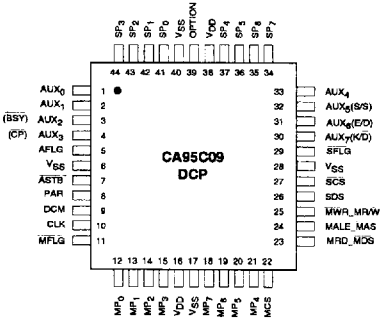


Figure 3-7 : CA95C09 44-Pin TQFP

Table 3-2 : Pin Description

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
CLK	14	15	16	10	I	**Clock:** An external timing source is input via this pin. The Master and Slave Port data strobe signals ($\overline{MWR}$, $\overline{MRD}$, $\overline{SDS}$ for CA95C68 and $\overline{MDS}$, $\overline{SDS}$ for CA95C18) must change synchronously with the clock input. In Direct Control Mode the AUX_5-S/$\overline{S}$ must also be synchronous. The output flags for the three ports ($\overline{AFLG}$, $\overline{MFLG}$, $\overline{SFLG}$) will all change synchronously with the clock.
C/$\overline{K}$	13	14	–	–	I	**Control/Key Mode Control:** This input controls the mode of operation of the DCP. The DCP enters into Multiplexed Control Mode when a low input is placed on the C/$\overline{K}$ pin, enabling programmed access to internal registers through the Master Port and enabling input of keys through the Auxiliary Port. In Direct Control Mode (C/$\overline{K}$ HIGH), several of the Auxiliary Port pins become direct control/status signals which can be driven/sensed by high-speed controller logic, and access to internal registers through the Master Port is limited to the Input and Output Registers.
DCM	–	–	15	9	I	**Direct Control Mode: (For CA95C09)** This input functions identical to the C/$\overline{K}$ input. (See C/$\overline{K}$ pin description).
MP_7 – MP_0	21-24 19-16	23-26 21-18	24-27 21-18	18-21 15-12	I/O	**Master Port Bus:** These eight bi-directional signals are used to input and output data, as well as specify the internal register addresses in Multiplexed Control Mode. The Master Port provides software access to the Status, Command, Mode, Mask, Input and Output Registers. For the CA95C68, the tri-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. For the CA95C18, the Master Port outputs are enabled when selected by $\overline{MCS}$, and when MR/$\overline{W}$ is HIGH and $\overline{MDS}$ is LOW. MP_0 is the low-order bit. Data and key information are entered into this port with the most significant byte first.
$\overline{MCS}$	25	27	28	22	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 maintained as long as MALE is LOW; when MALE is HIGH, the latch becomes transparent and the internal signal will follow the $\overline{MCS}$ input. No latching of $\overline{MCS}$ occurs in Direct Control Mode (C/$\overline{K}$ HIGH). The level on $\overline{MCS}$ is passed directly to the internal select circuitry regardless of the state of Master Port Address Latch Enable (MALE).

Table 3-2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
MALE	27	30	–	–	I	**Master Port Address Latch Enable: (For CA95C68)** 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 MALE. When C/$\overline{K}$ is HIGH (Direct Control Mode), MALE has no affect on DCP operation.
$\overline{MRD}$	26	29	–	–	I	**Master Port Read: (For CA95C68)** This active LOW input is used with a valid $\overline{MCS}$ to indicate that data is to be output on the Master Port bus. Master Port Read ($\overline{MRD}$) and Master Port Write ($\overline{MWR}$) are normally mutually exclusive; if both become active simultaneously, the DCP is reset to ECB Mode and all flags go inactive.
$\overline{MWR}$	28	31	–	–	I	**Master Port Write: (For CA95C68)** This active low input signal indicates to the DCP that valid data is present on MP_7-MP_0 for an input operation. The rising edge of $\overline{MWR}$ latches the data into the selected internal register. If $\overline{MWR}$ and $\overline{MRD}$ both go LOW simultaneously, the DCP is reset.
$\overline{MAS}$	27	30	–	–	I	**Master Port Address Strobe: (For CA95C18)** In Multiplexed Control Mode (C/$\overline{K}$ HIGH), a LOW on $\overline{MAS}$ indicates the presence of a valid chip select signal and address information. This information will be latched on the rising edge of $\overline{MAS}$. In Direct Control Mode, $\overline{MAS}$ has no affect on the DCP operation. The DCP will be reset if $\overline{MAS}$ and $\overline{MDS}$ both go low simultaneously.
$\overline{MDS}$	26	29	–	–	I	**Master Port Data Strobe: (For CA95C18)** This active low input is used in conjunction with a valid Master Port Chip Select ($\overline{MCS}$) to indicate that valid data is present on the MP_7-MP_0 bus for an input operation or that data is to be placed on the Master Port Bus during output. $\overline{MDS}$ and $\overline{MAS}$ are mutually exclusive; if they both go active simultaneously, the DCP is reset to ECB mode and all flags go inactive.
MR/$\overline{W}$	28	31	–	–	I	**Master Port Read/Write: (For CA95C18)** This input signal indicates to the DCP whether the current Master Port operation is a read (HIGH) where data is transferred from the device, or a write (LOW) where data is stored to an internal register. MR/$\overline{W}$ is not latched internally and must be held stable while $\overline{MDS}$ is LOW.

3

Table 3-2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
$\overline{MRD}$ – $\overline{MDS}$	–	–	29	23	I	**Master Port Read or Master Port Data Strobe: (For CA95C09)** When the OPTION pin is HIGH this input functions as $\overline{MRD}$. When the OPTION pin is LOW this input functions as $\overline{MDS}$. (See appropriate pin description).
MALE – $\overline{MAS}$	–	–	30	24	I	**Master Port Address Latch Enable or Master Port Address Strobe: (For CA95C09)** When the OPTION pin is HIGH this input functions as MALE and when OPTION is LOW it functions as $\overline{MAS}$. (See the appropriate pin description).
$\overline{MWR}$ – MR/$\overline{W}$	–	–	31	25	I	**Master Port Write or Master Port Read/Write: (For CA95C09)** When the OPTION pin is HIGH this input functions as $\overline{MWR}$ and when OPTION is LOW it functions as MR/$\overline{W}$. (See the appropriate pin description).
$\overline{MFLG}$	15	16	17	11	O	**Master Port Flag**: This active LOW flag indicates the need for a data transfer into or out of the Master Port during normal ciphering operation. The Master Port will be associated with either the Input or Output Register depending upon the setting of the Control bits in the Mode Register (See Register Description). If data is to be transferred through the Master Port to the Input Register, then $\overline{MFLG}$ 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 Functional Description). Whenever the Output Register is not empty $\overline{MFLG}$ will be active (LOW). In single port mode of operation, 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.
SP_7–SP_0	36-39 5-2	40-43 6-3	40-43 6-3	34-37 44-41	I/O	**Slave Port Bus**: This 8 bit bi-directional data bus provides a second input/output interface to the DCP, allowing overlapped input, ciphering and output operations. The tri-state Slave Port will be accessed only when the Mode Register is configured for dual port operation, Slave Port Chip Select ($\overline{SCS}$) and Slave Port Data Strobe ($\overline{SDS}$) are both LOW and $\overline{SFLG}$ =0. Data entered or retrieved through this port is the most significant byte in/out first (SP_7 is the most significant bit).

Table 3-2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
$\overline{SCS}$	30	33	33	27	I	**Slave Port Chip Select**: This active LOW signal is logically combined with the 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.
$\overline{SDS}$	29	32	32	26	I	**Slave Port Data Strobe**: This active LOW input, in conjunction with Slave Port Chip Select ($\overline{SCS}$) LOW indicates to the DCP that valid data is on the SP_7-SP_0 lines for an input operation, or that data is to be driven onto SP_7-SP_0 lines for output. The direction of data flow is determined by Control bits in the Mode Register. (See Register Description).
$\overline{SFLG}$	31	34	35	29	O	**Slave Port Flag**: This active LOW output indicates the state of either the Input Register or the Output Register, depending on the Mode Register configuration. 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.
AUX_7-AUX_0	32-35 9-6	36-39 10-7	36-39 10-7	30-33 4-1	I/O	**Auxiliary Port Bus**: 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. The Master Key can only be entered through this port but 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 of the key 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 on the following pages.
AUX_5 –S/$\overline{S}$	34	38	38	32	I	**Start/Stop**: In Direct Control Mode, when this pin goes LOW (Stop) the DCP will follow the sequence that would normally occur when a Stop Command is entered. Conversely, when this input 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/$\overline{D}$ selects either the Start Encryption or Start Decryption ciphering operation.
AUX_6 –E/$\overline{D}$	33	37	37	31	I	**Encrypt/Decrypt**: In Direct Control Mode, this input specifies whether the ciphering algorithm is to encrypt (E/$\overline{D}$ HIGH) or decrypt (E/$\overline{D}$ LOW) when AUX_5-S/$\overline{S}$ goes HIGH to initiate a normal data ciphering operation. 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. Corrupted data in the internal registers will occur if the proper level on AUX_6-E/$\overline{D}$ is not maintained during loading or ciphering operations.

3

Table 3-2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
AUX_7 –K/$\overline{D}$	32	36	36	30	I	**Key/Data**: In Direct Control Mode, when this signal goes HIGH, the DCP initiates a key-data input sequence as if a Clear E (or D) Key through the 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 inactive (LOW) and remain in this state until the first signal returns to an inactive state. Whenever a transition occurs on C/$\overline{K}$ (switching between Direct Control Mode and Multiplexed Control Mode) both of these signals must be inactive (LOW).
AUX_2 – $\overline{BSY}$	8	9	9	3	O	**Busy**: In Direct Control Mode, this active LOW status output gives a hardware indication that the ciphering algorithm is in operation. This status line is driven by the BSY bit in the Status Register, such that when the BSY bit is "1" (active), AUX_2-$\overline{BSY}$ is LOW.
AUX_3 – $\overline{CP}$	9	10	10	4	0	**Command Pending**: In Direct Control Mode, 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/$\overline{D}$. This signal line is driven by the $\overline{CP}$ bit in the Status Register, such that when the $\overline{CP}$ bit is "1" (active), AUX_3-$\overline{CP}$ is LOW.
$\overline{ASTB}$	11	12	13	7	I	**Auxiliary Port Strobe**: The rising edge of $\overline{ASTB}$ strobes the key-data on pins AUX_7-AUX_0 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 (most significant byte first) is entered on each $\overline{ASTB}$.

Table 3-2 : Pin Description Cont'd

Symbol	95C68/18		95C09		TYPE	Name and Function
	PDIP	PLCC	PLCC	TQFP		
$\overline{AFLG}$	10	11	11	5	O	**Auxiliary Port Flag**: This active LOW output signal indicates that the DCP is expecting key-data to be entered on the Auxiliary Port Bus. This can occur only when C/$\overline{K}$ is LOW (Multiplexed Control Mode) 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 falling edge of the eighth $\overline{ASTB}$.
$\overline{PAR}$	12	13	14	8	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 a "1" and $\overline{PAR}$ goes active (LOW). (See Parity Checking of Keys.). The Parity bit is the least significant bit of the key byte.
OPTION	–	–	1	39	I	**Option**: **(For CA95C09)** This input allows the user to configure the Master Port Control interface to function as either a CA95C68 or a CA95C18. When the OPTION pin is tied to V_{DD}, the device will function with the interface of a CA95C68. Conversely, tying the OPTION pin to V_{SS} will cause the DCP to function as a CA95C18. This OPTION pin must be tied to either V_{SS} or V_{DD}, or erratic operation of the device will occur. The CA95C09 DCP will perform identically to the CA95C68 or the CA95C18 (depending on the OPTION pin) with the only difference being the order of the signal names on the device package.
V_{DD}	40	44	44,22	16, 38	PWR	**Power Supply**: +5 Volts.
V_{SS}	1, 20	1, 22	2, 12 23, 34	6, 17 28, 40	GND	**Ground**: 0 Volts.

3

Table 3-3a : AC Characteristics (T_A + 0 to 70° C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V)

Number	Description
Clock	
t_1	CLK Width HIGH (t_{WH})
t_2	CLK Width LOW (t_{WL})
t_3	CLK HIGH to Next Clock HIGH (Clock Cycle, t_C)
Reset	
t_5	$\overline{MRD}$ • $\overline{MWR}$ LOW to $\overline{MRD}$ • $\overline{MWR}$ HIGH (Reset Pulse Width), (Note 11)
Direct Control Mode	
t_9	S/$\overline{S}$ LOW to C/$\overline{K}$ HIGH (Setup), (Note 11)
t_{10}	K/$\overline{D}$ LOW to C/$\overline{K}$ HIGH (Setup), (Note 11)
t_{11}	C/$\overline{K}$ HIGH to S/$\overline{S}$ HIGH (Note 11)
t_{12}	C/$\overline{K}$ HIGH to K/$\overline{D}$ HIGH (Note 11)
t_{13}	S/$\overline{S}$ LOW to E/$\overline{D}$ INVALID (Hold)
t_{14}	E/$\overline{D}$ VALID to K/$\overline{D}$ HIGH (Setup) (Note 11)
t_{15}	K/$\overline{D}$ HIGH • CLK ↓ to $\overline{CP}$ LOW
t_{17}	K/$\overline{D}$ LOW to E/$\overline{D}$ INVALID (Hold)
t_{18}	K/$\overline{D}$ LOW to S/$\overline{S}$ HIGH
t_{19}	S/$\overline{S}$ LOW to K/$\overline{D}$ HIGH
t_{20}	E/$\overline{D}$ VALID to S/$\overline{S}$ HIGH (Setup), (Note 11)
t_{21}	S/$\overline{S}$ HIGH • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Input Flag)
t_{23}	S/$\overline{S}$ LOW to E/$\overline{D}$ INVALID (Hold) (Note 11)
t_{24}	CLK LOW to $\overline{BSY}$ LOW
t_{25}	CLK LOW to $\overline{BSY}$ HIGH
t_{27}	ALGORITHM completed • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) LOW (Port Output Flag)
t_{28}	S/$\overline{S}$ LOW • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Port Input Flag), (Note 3)
t_{29}	CLK ↓ to K/$\overline{D}$ HIGH (Note 11)
t_{30}	CLK ↓ to S/$\overline{S}$ HIGH (Note 11)
Multiplexed Control Mode - Master Port	
t_{32}	For CA95C68: MALE Width (HIGH) For CA95C18: $\overline{MAS}$ Width (LOW)
t_{34}	For CA95C68: $\overline{MCS}$ LOW to MALE LOW (Setup) For CA95C18: $\overline{MCS}$ LOW to $\overline{MAS}$ HIGH (Setup)
t_{35}	For CA95C68: MALE LOW to $\overline{MCS}$ HIGH (Hold) For CA95C18: $\overline{MAS}$ HIGH to $\overline{MCS}$ HIGH (Hold)
t_{36}	For CA95C68: Address INVALID to MALE LOW (Address Setup Time) For CA95C18: Address INVALID to $\overline{MAS}$ HIGH (Address Setup Time)
t_{37}	For CA95C68: MALE LOW to Address INVALID (Address Hold Time) For CA95C18: $\overline{MAS}$ HIGH to Address INVALID (Address Hold Time)

Table 3-3b : AC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V

Number	5 MHz Limits		10 MHz Limits		16 MHz Limits		20 MHz Limits		25 MHz Limits		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
Clock											
t_1	85	–	40	–	27	–	20	_	17	–	ns
t_2	85	–	40	–	27	–	20	–	17	–	ns
t_3	200	–	100	–	62.5	–	50	–	40	–	ns
Reset											
t_5	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
Direct Control Mode											
t_9	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{10}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{11}	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	ns
t_{12}	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	$2t_C$	–	ns
t_{13}	40	–	20	–	15	–	10	–	5	–	ns
t_{14}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{15}	–	75	–	60	–	45	–	40	–	30	ns
t_{17}	40	–	20	–	15	–	10	–	5	–	ns
t_{18}	40	–	20	–	15	–	10	–	5	–	ns
t_{19}	40	–	20	–	15	–	10	–	5	–	ns
t_{20}	40	–	20	–	15	–	10	–	5	–	ns
t_{21}	–	75	–	60	–	45	–	40	–	30	ns
t_{23}	40	–	20	–	15	–	10	–	5	–	ns
t_{24}	–	75	–	60	–	45	–	40	–	30	ns
t_{25}	–	100	–	75	–	60	–	50	–	40	ns
t_{27}	–	75	–	60	–	45	–	40	–	30	ns
t_{28}	–	75	–	60	–	45	–	40	–	30	ns
t_{29}	3	t_C-25	3	t_C-25	3	t_C-25	1	t_C-20	1	t_C-20	ns
t_{30}	3	t_C-25	3	t_C-25	3	t_C-25	1	t_C-20	1	t_C-20	ns
Multiplexed Control Mode - Master Port											
t_{32}	75	–	50	–	30	–	20	–	12	–	ns
	75	–	50	–	30	–	20	–	12	–	ns
t_{34}	25	–	15	–	5	–	0	–	0	–	ns
	25	–	15	–	5	–	0	–	0	–	ns
t_{35}	35	–	30	–	20	–	15	–	10	–	ns
	35	–	30	–	20	–	15	–	10	–	ns
t_{36}	35	–	30	–	20	–	15	–	10	–	ns
	35	–	30	–	20	–	15	–	10	–	ns
t_{37}	35	–	30	–	20	–	15	–	15	–	ns
	35	–	30	–	20	–	15	–	15	–	ns

3

Table 3-3a : AC Characteristics (T_A + 0 to 70° C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V) Cont'd

Number	Description
Master/Slave Port Read/Write	
t_{40}	For CA95C68: $\overline{MCS}$ LOW to $\overline{MRD}$, $\overline{MWR}$ LOW (Select Setup), (Note 4) For CA95C18: $\overline{MCS}$ LOW to $\overline{MDS}$ LOW (Select Setup), (Note 4) For CA95C68/18: $\overline{SCS}$ LOW to $\overline{SDS}$ LOW (Select Setup)
t_{41}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$ HIGH to $\overline{MCS}$ HIGH (Select Hold), (Note 4) For CA95C18: $\overline{MDS}$ HIGH to $\overline{MCS}$ HIGH (Select Hold), (Note 4) For CA95C68/18: $\overline{SDS}$ HIGH to $\overline{SCS}$ HIGH (Select Hold)
t_{42}	MR/$\overline{W}$ VALID to $\overline{MDS}$ LOW (Setup)
t_{43}	$\overline{MDS}$ HIGH to MR/$\overline{W}$ INVALID (Hold)
t_{44}	For CA95C68: $\overline{MRD}$, $\overline{MRW}$ LOW to $\overline{MRD}$, $\overline{MRW}$ HIGH (Width-Write, Read) For CA95C18: $\overline{MDS}$ LOW to $\overline{MDS}$ HIGH (Width-Write, Read) For CA95C68/18: $\overline{SDS}$ LOW to $\overline{SDS}$ HIGH (Read, Write)
t_{45}	For CA95C68: CLK LOW to $\overline{MRD}$, $\overline{MWR}$ HIGH (Note 11) For CA95C18: CLK LOW to $\overline{MDS}$ HIGH (Note 11) For CA95C68/18: CLK LOW to $\overline{SDS}$ HIGH (Note 11)
t_{46}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$ HIGH to $\overline{MRD}$, $\overline{MWR}$ LOW (Data Strobe Recovery Time) For CA95C18: $\overline{MDS}$ HIGH to $\overline{MDS}$ LOW (Data Strobe Recovery Time) For CA95C68/18: $\overline{SDS}$ HIGH to $\overline{SDS}$ LOW (Data Strobe Recovery Time)
t_{47}	For CA95C68: Write Data VALID to $\overline{MWR}$ ($\overline{SDS}$) HIGH (Write Setup Time) For CA95C18: Write Data VALID to $\overline{MDS}$ ($\overline{SDS}$) HIGH (Write Setup Time)
t_{48}	For CA95C68: $\overline{MWR}$ HIGH to Write Data INVALID (Hold Time) For CA95C18: $\overline{MDS}$ HIGH to Write Data INVALID (Hold Time) For CA95C68/18: $\overline{SDS}$ HIGH to Write Data INVALID (Hold Time)
t_{49}	For CA95C68: $\overline{MRD}$ LOW to Read Data VALID (Read Access Time) For CA95C18: $\overline{MDS}$ LOW to Read Data VALID (Read Access Time) For CA95C68/18: $\overline{SDS}$ LOW to Read Data VALID (Read Access Time)
t_{50}	For CA95C68: $\overline{MRD}$ ($\overline{SDS}$) HIGH to Read Data INVALID (Hold Time) For CA95C18: $\overline{MDS}$ ($\overline{SDS}$) HIGH to Read Data INVALID (Hold Time)
t_{51}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$, ($\overline{SDS}$) LOW • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Last Strobe), (Note 5) For CA95C18: $\overline{MDS}$, ($\overline{SDS}$) LOW • CLK ↓ to $\overline{MFLG}$ ($\overline{SFLG}$) HIGH (Last Strobe), (Note 5)
t_{52}	For CA95C68: $\overline{MWR}$ HIGH • CLK ↓ to $\overline{CP}$ HIGH (Note 4,11), (Last Strobe-Key Load) For CA95C18: $\overline{MDS}$ HIGH • CLK ↓ to $\overline{CP}$ HIGH (Note 4,11), (Last Strobe-Key Load)
t_{53}	For CA95C68: $\overline{MRD}$, $\overline{MWR}$ ($\overline{SDS}$) HIGH to S/$\overline{S}$ LOW (Hold Time) (Note 11) For CA95C18: $\overline{MDS}$ ($\overline{SDS}$) HIGH to S/$\overline{S}$ LOW (Hold Time) (Note 11)
t_{54}	For CA95C68: $\overline{MWR}$ HIGH • CLK ↓ to $\overline{PAR}$ VALID (Key Write) For CA95C18: $\overline{MDS}$ HIGH • CLK ↓ to $\overline{PAR}$ VALID (Key Write)
t_{55}	For CA95C68: S/$\overline{S}$ HIGH to $\overline{MRD}$, $\overline{MWR}$, ($\overline{SDS}$) LOW (Setup Time) (Note 11) For CA95C18: S/$\overline{S}$ HIGH to $\overline{MDS}$, ($\overline{SDS}$) LOW (Setup Time) (Note 11)
t_{57}	$\overline{MRD}$, $\overline{MWR}$ HIGH to MALE HIGH $\overline{MDS}$ HIGH to $\overline{MAS}$ LOW
t_{58}	MALE LOW to $\overline{MRD}$, $\overline{MWR}$ LOW $\overline{MAS}$ HIGH to $\overline{MDS}$ LOW

Table 3-3b : AC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V Cont'd

Number	5 MHz Limits		10 MHz Limits		16 MHz Limits		20 MHz Limits		25 MHz Limits		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
Master/Slave Port Read/Write											
t_{40}	30	–	20	–	10	–	5	–	0	–	ns
	30	–	20	–	10	–	5	–	0	–	ns
	30	–	20	–	10	–	5	–	0	–	ns
t_{41}	35	–	30	–	20	–	10	–	5	–	ns
	35	–	30	–	20	–	10	–	5	–	ns
	35	–	30	–	20	–	10	–	5	–	ns
t_{42}	35	–	30	–	20	–	15	–	10	–	ns
t_{43}	35	–	30	–	20	–	15	–	15	–	ns
t_{44}	140	–	70	–	50	–	35	–	30	–	ns
	140	–	70	–	50	–	35	–	30	–	ns
	140	–	70	–	50	–	35	–	30	–	ns
t_{45}	5	t_C-25	5	t_C-25	5	t_C-25	2	t_C-25	2	t_C-25	ns
	5	t_C-25	5	t_C-25	5	t_C-25	2	t_C-25	2	t_C-25	ns
	5	t_C-25	5	t_C-25	5	t_C-25	2	t_C-20	2	t_C-20	ns
t_{46}	30	–	20	–	15	–	10	–	10	–	ns
	30	–	20	–	15	–	10	–	10	–	ns
	30	–	20	–	15	–	10	–	10	–	ns
t_{47}	60	–	30	–	20	–	15	–	10	–	ns
	60	–	30	–	20	–	15	–	10	–	ns
t_{48}	20	–	20	–	15	–	15	–	10	–	ns
	20	–	20	–	15	–	15	–	10	–	ns
	20	–	20	–	15	–	15	–	10	–	ns
t_{49}	–	60	–	50	–	45	–	35	–	35	ns
	–	60	–	50	–	45	–	35	–	35	ns
	–	60	–	50	–	45	–	35	–	35	ns
t_{50}	5	–	5	–	5	–	5	–	5	–	ns
	5	–	5	–	5	–	5	–	5	–	ns
t_{51}	–	75	–	50	–	40	–	35	–	30	ns
	–	75	–	50	–	40	–	35	–	30	ns
t_{52}	–	75	–	50	–	40	–	35	–	30	ns
	–	75	–	50	–	40	–	35	–	30	ns
t_{53}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{54}	–	75	–	50	–	40	–	35	–	30	ns
	–	75	–	50	–	40	–	35	–	30	ns
t_{55}	t_C	–	t_C	–	t_C	–	t_C	–	t_C	–	ns
t_{57}	140	–	70	–	30	–	20	–	10	–	ns
	140		70		30		20		10		
t_{58}	80	–	40	–	20	–	20	–	20	–	ns
	80		40		20		20		20		

3

Table 3-3a : AC Characteristics (T_A + 0 to 70° C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V) Cont'd

Number	Description
Auxiliary Port Key Entry	
t_{61}	$\overline{ASTB}$ LOW to $\overline{ASTB}$ HIGH (Width)
t_{62}	CLK LOW to $\overline{ASTB}$ HIGH (Note 11)
t_{63}	$\overline{ASTB}$ HIGH to Next $\overline{ASTB}$ LOW (Recovery Time)
t_{64}	Write-Data VALID to $\overline{ASTB}$ HIGH (Data Setup Time)
t_{65}	$\overline{ASTB}$ HIGH to Write-Data INVALID (Data Hold Time)
t_{66}	$\overline{ASTB}$ HIGH • CLK ↓ to $\overline{PAR}$ VALID
t_{67}	$\overline{ASTB}$ LOW • CLK ↓ to $\overline{AFLG}$ HIGH (Last Strobe)

Table 3-3b : AC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V Cont'd

Number	5 MHz Limits		10 MHz Limits		16 MHz Limits		20 MHz Limits		25 MHz Limits		Unit
	Min	Max	Min	Max	Min	Max	Min	Max	Min	Max	
Auxiliary Port Key Entry											
t_{61}	80	–	40	–	30	–	20	–	20	–	ns
t_{62}	5	t_C-20	5	t_C-20	5	t_C-20	5	t_C-20	5	t_C-20	ns
t_{63}	30	–	20	–	15	–	10	–	10	–	ns
t_{64}	40	–	20	–	15	–	10	–	5	–	ns
t_{65}	20	–	20	–	15	–	15	–	5	–	ns
t_{66}	–	75	–	50	–	40	–	35	–	30	ns
t_{67}	–	75	–	50	–	40	–	35	–	30	ns

Notes:

1) All input transition times assumed <5ns, except clock which is <3ns (for 25 MHz timing).
2) The appropriate input flag ($\overline{MFLG}$, $\overline{SFLG}$, $\overline{AFLG}$) goes active LOW after 1 CLK ↓ +30ns from the writing of a "Load" or "Start" command.
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 ($\overline{MCS}$ must be LOW for one falling edge during a read/write cycle).
5) In Cipher Feedback, the Port Flag ($\overline{MFLG}$ or $\overline{SFLG}$) will go inactive following the leading edge of the first data strobe ($\overline{MRD}$, $\overline{MWR}$, $\overline{MDS}$, or $\overline{SDS}$), in all other modes and operations, the flags go inactive on the eighth data strobe.
6) Do not change 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) In Cipher Feedback, $\overline{BSY}$ must be inactive (HIGH) before S/$\overline{S}$ goes inactive (LOW).
9) $\overline{AFLG}$ must go active (LOW) before $\overline{ASTB}$ goes active (LOW).
10) t_{WL} is the clock width LOW (number t_2).
11) t_C is the clock cycle time (number t_3).
12) All output timing specifications reflect the following: High output >1.5V, Low output <1.5V.
13) All output timings assume C_{LOAD} = 50pF.
14) When operating in Direct Control Mode, you must ensure that the K/$\overline{D}$ input is valid one clock cycle before you begin to load the key, or perform any data operations with the device.

3

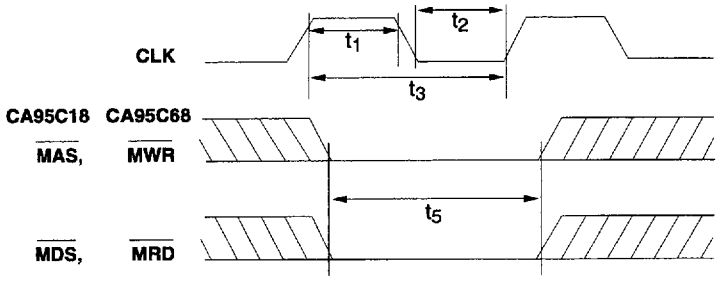


Figure 3-8 : CA95C68/18 Clock and Reset Timing

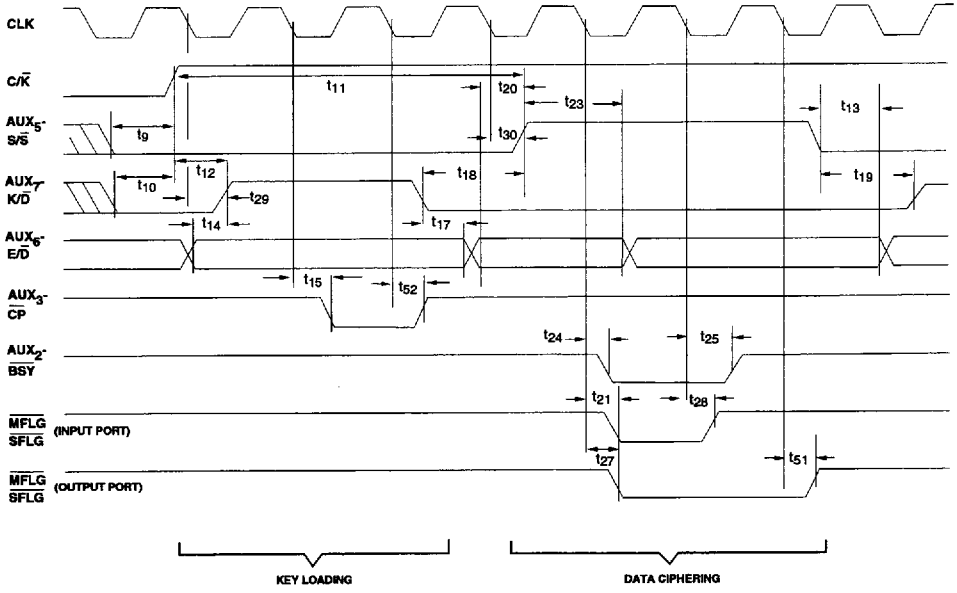


Figure 3-9 : CA95C68/18 Control and Status Signals Timing (Direct Control Mode)

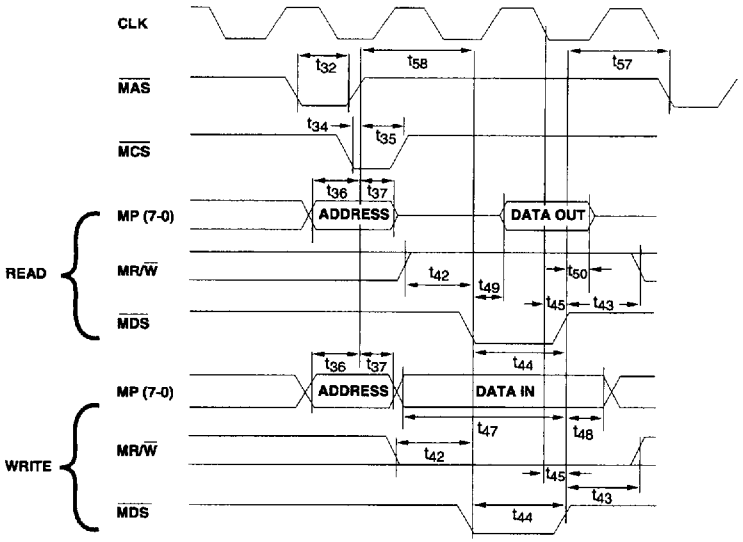
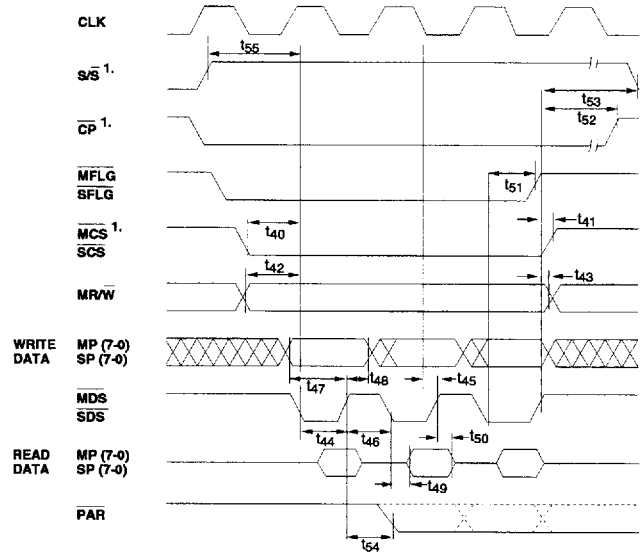


Figure 3-10 : CA95C68 Master Port, Multiplexed Control Mode Read/Write



1. These signals are only used for Read/Write Timing in Direct Control Mode of operation.

Figure 3-11 : CA95C68 Master (Slave) Port Read/Write Timing

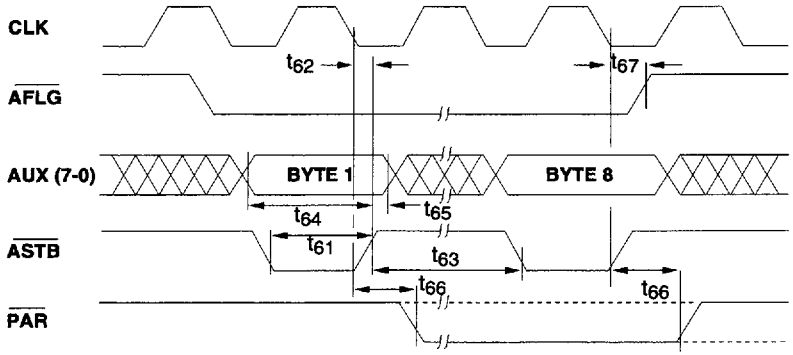


Figure 3-12 : CA95C68/18 Auxiliary - Port Key Entry Timing

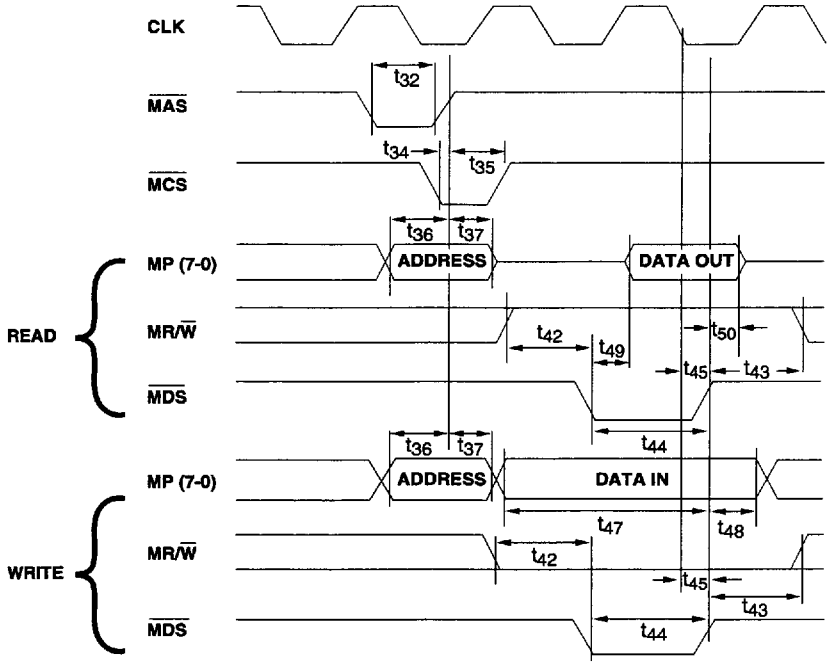
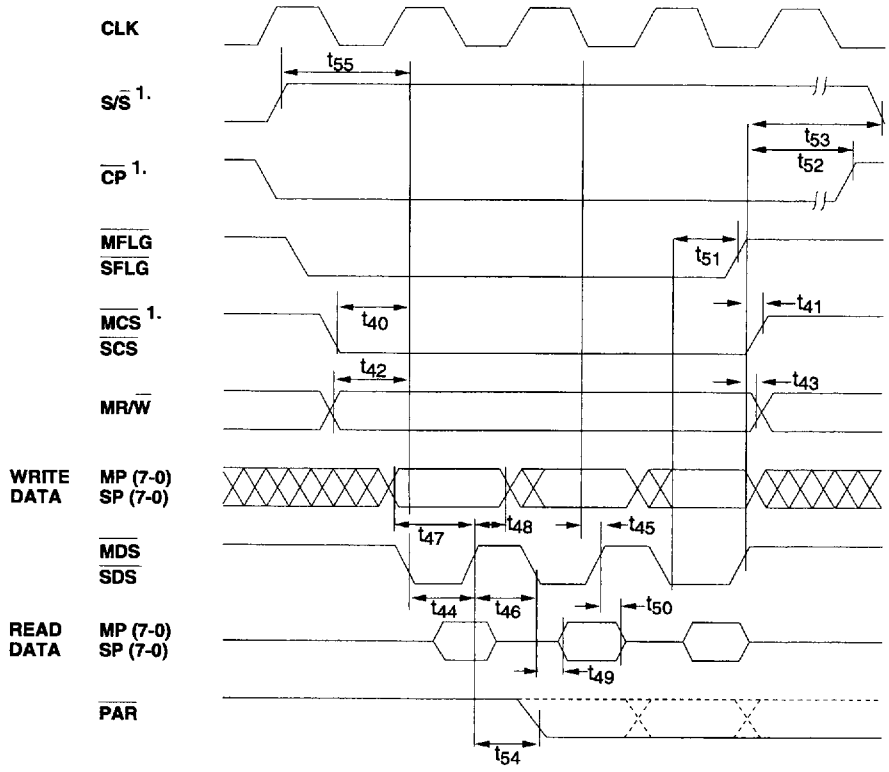


Figure 3-13 : CA95C18 Master Port, Multiplexed Control Mode, Read/Write Timing



1. These Signals are only used for Read/Write timing in Direct Control Mode of operation.

Figure 3-14 : CA95C18 Master (Slave) Port Read/Write Timing

Table 3-4 : DC Characteristics (T_A = 0 to 70°C, V_{DD} = +5.0V ± 5%, V_{SS} = 0V)

Symbol	Parameter	Test Conditions	Limits		Units
			Min	Max	
I_{IL}	Input leakage current	$0 V \le V_{IN} \le V_{DD}$	-1.0	+1.0	µA
I_{OZ}	Output leakage current	$0 V \le V_{IN} \le V_{DD}$	-10.0	+10.0	µA
I_{DDOP}	Operating supply current	–	–	3.0	mA/MHz
I_{DDSB}	Standby supply current	$V_{IN} = V_{DD}$ or V_{SS} V_{DD} = 5.50V, Outputs open	–	70.0	µA
V_{IL}	Input low voltage	Note 2	-0.5	0.8	V
V_{IH}	Input high voltage	Note 2	2.0	V_{DD}	V
V_{TL}	Schmitt trigger input low voltage	Note 1	-0.5	0.8	V
V_{TH}	Schmitt trigger input high voltage	Note 1	2.3	V_{DD}	V
V_{HY}	Schmitt trigger hysteresis	Note 1	0.4	–	V
V_{OL}	Output low voltage	I_{OL} = 4.0mA	–	0.4	V
V_{OH}	Output high voltage	I_{OH} = -4.0mA	2.4	–	V

Note:

1) Applies to the following inputs:
   For CA95C68: CLK, C/$\overline{K}$, $\overline{MCS}$, $\overline{MRD}$, $\overline{MWR}$, MALE, $\overline{SCS}$, $\overline{SDS}$, $\overline{ASTB}$.
   For CA95C18: CLK, C/$\overline{K}$, $\overline{MCS}$, $\overline{MAS}$, $\overline{MDS}$, MR/$\overline{W}$, $\overline{SCS}$, $\overline{SDS}$, $\overline{ASTB}$.
   For CA95C09: CLK, DCM, $\overline{MCS}$, $\overline{MRD}$ _ $\overline{MDS}$, MALE_$\overline{MAS}$, $\overline{MWR}$ _MR/$\overline{W}$, $\overline{SCS}$, $\overline{SDS}$, $\overline{ASTB}$, OPTION.
2) Applies to the following inputs: MP_{7-0}, SP_{7-0}, AUX_{7-0}.

Table 3-5 : Recommended Operating Conditions

DC Supply Voltage (V_{DD})	+4.5V to +5.5V
Power Dissipation (P_{DD}), (Note 1)	0.5 W
Ambient Operating Temperature (T_A Commercial)	0 to 70° C

Note:

1) The power dissipation figure is based on typical internal logic dissipation plus the worst case set of outputs simultaneously active with maximum rated loads.

Table 3-6 : Absolute Maximum Ratings

DC Supply Voltage (V_{DD})	-0.3 to +7.0V
Input Voltage (V_{IN})	-0.3 to +7.0V
DC Input Current (I_{IN})	-10 to +10 mA
Storage Temperature, plastic (T_{STG})	-65° to +150°C

Stresses beyond those listed above may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of this specification is not implied. Exposure to maximum rating conditions for extended periods may affect device reliability.

The design of the DCP, as shown in Figure 3-1 is optimized for high data throughput. The cryptography key bytes can be written through both the Auxiliary and Master Ports. 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 each incoming key byte. Two 64-bit registers are provided for the initialization Vectors (IVE and IVD) required for chained (feedback) ciphering modes. Clear and cipher data bytes can be transferred through both the Master and Slave Ports to the Input Register; conversely, data can be transferred from the Output Register to either port. Four 8-bit registers (Mode, Command, Status and Mask) are accessible through the Master Port for interfacing to a host microprocessor.

Algorithm Processing

The DCP's Algorithm Processing Unit (see Figure 3-1) is designed to encrypt and decrypt data according to the National Bureau of Standards Data Encryption Standard (DES), as specified in Federal Information Processing Standards Publication FIPS PUB 46 (1-15-1977).

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 four ciphering methods: Electronic Code Book (ECB), Cipher Block Chaining (CBC), one (CFB-1) and eight bit Cipher Feedback (CFB-8). Electronic Code Block (ECB) is a straightforward implementation of the DES algorithm; 64 bits of clear data in, 64 bits of cipher text out, with no cryptographic dependence between blocks. Cipher Block Chaining (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 identical cipher text. CBC also provides an error extension characteristic which protects against fraudulent data insertions and deletions. Cipher Feedback is an additive stream cipher method in which the DES generates a pseudo random binary stream which is then exclusive-ORed with the clear text 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 both 1-bit and 8-bit cipher feedback which is useful for low speed bit and byte oriented serial communications.

Multiple Key Registers

The DCP provides the necessary registers to implement a multiple-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 only be loaded with plain text through the Auxiliary Port, using the Load Clear M Key command.

In addition to the Master 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 through the Master Port (Multiplexed Control Mode) into the Command Register, and then writing the eight bytes of key data to the port when the Command Pending bit = "1" in the Status Register (see Command Description Section).

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 connected to allow a host CPU to directly address six internal (Mode, Command, Status, Mask, Input, Output) registers and thereby control the device by writing and reading these registers. In Multiplexed Control Mode, the Auxiliary Port is also enabled for entering keys.

If the logic level of C/$\overline{K}$ is brought HIGH, the DCP enters Direct Control Mode, and the Auxiliary Port pins are converted into direct hardware control or status 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 especially well suited for ciphering data for high-speed peripheral devices.

Initialization

The DCP can be reset in several ways:

1) By the "Software Reset" command,
2) By a hardware reset:

(CA95C68) Assertion of $\overline{MRD}$ and $\overline{MWR}$ LOW simultaneously for 1 clock cycle,

(CA95C18) Assertion of $\overline{MAS}$ and $\overline{MDS}$ LOW simultaneously for 1 clock cycle.

3) By writing to the Mode Register,
4) By aborting any command.

All these sequences are identical internally, except that loading the Mode Register doesn't subsequently reset the Mode Register. Once the reset process starts, the DCP is unable to respond to any further commands for approximately five clock cycles. If a power-up reset is used, the rising edge of the reset signal should not occur until approximately 1 ms after V_{DD} has reached the normal operating voltage. This delay time is required for internal nodes to stabilize.

Master Port Read/Write Timing

The DCP's Master Port is designed to operate with multiplexed address-data buses. The Master Port can be optimized to interface with either a Latched Address Enable (CA95C68) or a Strobed (CA95C18) microprocessor.

Several features of the CA95C68 interface should be stressed.

- The level on Master Port Chip Select ($\overline{MCS}$) is latched internally on the falling edge of Master Port Address Latch Enable (MALE) in Multiplexed Control Mode only. This relieves external address decode circuitry of the responsibility for latching chip select at address time.
- The levels on MP1, MP2 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, Mask, Input and Output). Again, this eliminates the need for external address latching and decoding. The Mask Register is only accessible when the DCP is programmed for one-bit CFB mode via the Mode Register's Cipher Type bits.
- Data transfers through the Master Port are controlled by the levels and transitions on the Master Port Read ($\overline{MRD}$) and Master Port Write ($\overline{MWR}$) pins. Master Port data transfers do not disturb either the chip-select or address latches, so that once the DCP and a particular register have been selected, unlimited writing and reading of that register can be done without intervening address cycles. Given the required transfer control external to the DCP, this feature could greatly speed up loading keys and data.

The CA95C18 interface is similar with the following exceptions:

- The level on $\overline{MCS}$ is latched internally on the rising edge of $\overline{MAS}$ in Multiplexed Control Mode only.
- The levels on MP1, MP2 are also latched internally on the rising edge of $\overline{MAS}$ and are then decoded to enable reading and writing of internal registers.
- Data transfers through the Master Port are controlled by Master Port Data Strobe ($\overline{MDS}$) and Master Port Read/Write (MR/$\overline{W}$). The chip-select and address latches aren't affected by data transfers. Any number of reads or writes to this selected register can be accomplished without intervening address cycles.

Loading Key and Initialization Vector (IV) Registers

The Key and Initialization Vector Registers are not directly addressable through any of the DCP's ports, therefore keys and vector data must be loaded through "command data sequences" (see Command Description Section). 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 bit in the Status Register; the user then either writes eight bytes of key or initial vector data through the Master or Auxiliary Port, as selected by the specific command, or reads eight bytes of initial 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 subsequently raising the AUX_7-K/$\overline{D}$ input, indicating that key loading is required. The command processor will assert the AUX_3-$\overline{CP}$ (Command Pending) signal, then the eight key bytes may be written through the Master Port to the appropriate register. In Multiplexed Control Mode, all Key and Initial Vector Registers, except the Master (M) Key, may be loaded with encrypted, as well as clear, data. Before loading an encrypted key or initial vector, the clear Master Key must first be loaded through the Auxiliary Port. If the operation is a Load Encrypted command, the subsequent data is written to either the Master or Auxiliary Port and is routed first to the Input Register and decrypted before being stored in the specified Key or Initial Vector Register. After loading the last byte of an encrypted key or initial vector, no reading or writing of internal registers is allowed for the subsequent 60 clock cycles.

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 the three key registers. The output of the parity detection circuit is connected to the $\overline{PAR}$ pin, as well as the state of this pin being reflected by the Status Register PAR (S3) bit. Status Register bit PAR goes to "1" whenever a byte with even parity (an even number of "1"s) is detected. The Status Register also has a Latched Parity bit (LPAR, S4) which is set to "1" whenever the Status Register PAR bit goes to "1". Once it is set to "1", the LPAR bit is not cleared until a reset occurs or a new Load Key command is issued.

When an encrypted key has been loaded, 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 appropriate key register. Therefore, 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 byte contained errors.

Data Flow

The Mode Register contains two bits, M2 and M3, which 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 Data Flow Control bits are set to Master Port only. Data to be encrypted/decrypted (depending on the value loaded into the Encrypt/Decrypt bit (M4) of the Mode Register) is written to the Input Register through the Master Port. To facilitate monitoring of the Input Register status, the $\overline{MFLG}$ signal goes LOW when the Input Register is not full. Clear or cipher data is ready to be read by the host CPU through the Master Port Output Register address when $\overline{SFLG}$ goes LOW. Therefore, $\overline{MFLG}$ is redefined as Master Input Flag and $\overline{SFLG}$ is redefined as Master Output Flag.

Dual Port, Master Port Clear Configuration

In the dual port configurations, entering and removing data is accomplished with both the Master and Slave Ports. In the Master Port Clear configuration, clear text for encryption or clear text resulting from decryption can pass only through the Master Port. Cipher text can be handled only through the Slave Port. The direction of data flow is controlled either by the Encrypt/Decrypt bit (M4) in the Mode Register, or by the Start Encryption or Start Decryption commands. For encryption, clear data is written through the Master Port to the Input Register, and cipher data can be read from the Output Register through the Slave Port at the appropriate time. If decryption is selected, the process is reversed, cipher data being written to the Input Register through the Slave Port, and the clear data being read from the Output Register through the Master Port.

Dual Port, Slave Port Clear Configuration

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

3

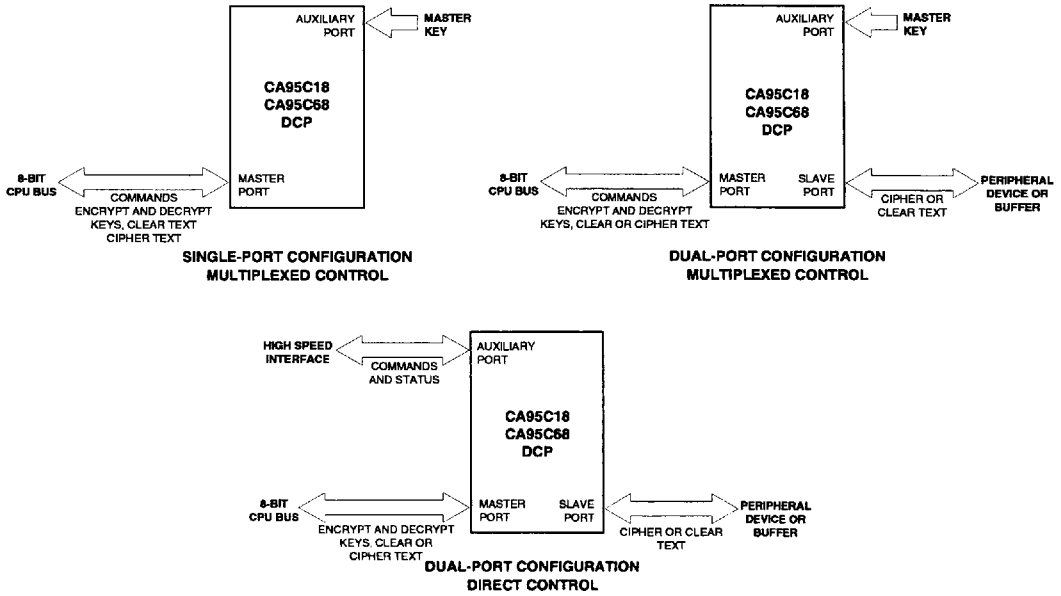


Figure 3-15 : CA95C68 and CA95C18 Data Flow Options

REGISTER DESCRIPTION

The registers in the DCP which can be directly addressed through the Master Port are shown with their addresses in Table 3-7. A brief description of these registers and others not directly accessible is given below.

Table 3-7 : Master Port Register Address

C/$\overline{K}$	Cipher Type	MP2	MP1	$\overline{MRD}$ 9568	$\overline{MWR}$ 9568	MR/$\overline{W}$ 9518	$\overline{MCS}$	Register Addressed
0	all	0	0	1	0	0	0	Input Register
0	all	0	0	0	1	1	0	Output Register
0	all	0	1	1	0	0	0	Command Register
0	all	0	1	0	1	1	0	Status Register
0	ECB/ CBC/ CFB-8	1	0	1	0	0	0	Input Register
0	ECB/ CBC/ CFB-8	1	0	0	1	1	0	Output Register
0	CFB-1	1	0	X	X	X	0	Mask Register
0	all	1	1	X	X	X	0	Mode Register
X	all	X	X	X	X	X	1	No Register Accessed
1	all	X	X	1	0	0	0	Input Register
1	all	X	X	0	1	1	0	Output Register

Mode Register

Figure 3-16 shows the bit assignments in this 7-bit read/write register. The Cipher Type bits (M1, M0) indicate to the DCP which ciphering algorithm is to be used. After a reset, the Cipher Type defaults to the Electronic Code Book.

Configuration bits (M3, M2) 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 (M3, M2=10), the Slave Port is disabled and no manipulation of Slave Port Chip Select ($\overline{SCS}$) or Slave Port Data Strobe ($\overline{SDS}$) can cause data movement through the Slave Port. All data transfers are accomplished through the Master Port, as described more fully in the Functional Description section. In this configuration, $\overline{MFLG}$ gives the status of the Input Register and $\overline{SFLG}$ the Output Register.

Both the Master and Slave Ports are available for input and output operations when the Configuration bits are set to one of the dual port configurations (M3,M2 = 00 or 01). When M3,M2 = 01 (the default configuration), the Master Port handles clear data while the Slave Port handles ciphered data. Configuration M3,M2 = 00 reverses this assignment. The data direction at any particular moment is controlled by the Encrypt/Decrypt bit (M4).

The Encrypt/Decrypt bit 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 the data flow direction within the DCP. For example, when the Encrypt/Decrypt bit is "1" (encrypt) and the Configuration bits are "01" (Dual Port, Master Clear, Slave Encrypted), clear data will enter the DCP through the Master Port and encrypted data will be removed from the Slave Port. When the Encrypt/Decrypt bit is set to "0" (decrypt), the direction of data flow reverses.

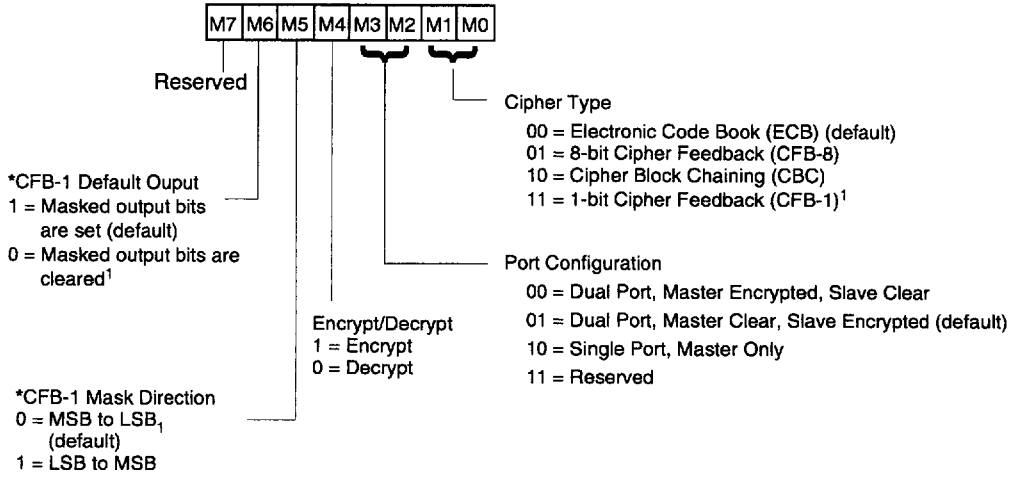
The CFB-1 Mask Direction bit (M5) determines the direction in which the Mask Register's bits and the input data are interpreted. When the CFB-1 Mask Direction bit is set to "0" the DCP will read the Mask Direction and data to be ciphered from most significant bit (MSB) to least significant bit (LSB). When the CFB-1 Mask Direction bit is set to "1" the DCP will read the Mask Register and data from LSB to MSB. The CFB-1 Mask Direction bit is only accessible when the DCP is set to 1-bit Cipher Feedback mode via the Mode Register.

The CFB-1 Default Output bit (M6) defines the sense of output bits which are masked off in the Mask Register. If the Default Output bit is set to "1" then output bits, which are masked (not used), will be set to "1". If the Default Output bit is cleared to "0" then output bits, which are masked (not used), will be cleared to "0".

Mask Register

The 8-bit read/write Mask Register determines which Input and Output Register bits are significant during One-bit Cipher Feedback mode (CFB-1). If any Mask Register bit is set to "1" then the corresponding bit of the Input Register will be used as an input to the one-bit cipher feedback encryption/decryption process and its one bit result will likewise be placed in the corresponding bit of the Output Register. If any Mask Register bit is cleared to "0" then the corresponding bit of the Input Register will be ignored.

In one-bit cipher feedback mode, if a single byte is written to the Input Register (when requested by the DCP via the Input Flag) then the ciphering algorithm unit will remain busy until all bits in the Input Register, corresponding to set bits in the Mask Register, are processed. For example, if the Mask Register is set to "01101001" and the Mode Register's CFB-1 Mask Direction bit is set for MSB to LSB Mask interpretation, then the DCP will perform Encryption/Decryption on bit 6 of the Input Register, followed by bits 5, 3, and 1. The corresponding results will be placed in bits 6, 5, 3 and 1 of the Output Register. All other bits in the Input Register will be ignored and all other bits in the Output Register will be set to the state indicated by the Default Output bit (M6) of the Mode Register. The ciphering algorithm unit will remain busy until all four bits are ciphered. Zero to eight bits of the Mask Register may be set to "1". If zero bits are set to "1" then any subsequent writes to the Input Register will be ignored.



* The CFB-1 Mask Direction and Default Output bits are only accessible when the DCP is in CFB-1 mode, otherwise these bits are high.
1.) This mode is Newbridge Microsystems specific.

Figure 3-16 : Mode Register Bit Assignments

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 in the Command Description section, and the commands and their binary representations are summarized in Table 3-8 and Table 3-9.

Table 3-8 : Command Codes in Multiplexed Control Mode

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

Status Register

The bit assignments for the read-only Status Register are shown in Figure 3-17. The PAR, AFLG, SFLG and MFLG bits indicate the status of the similarly named output pins, as do the Busy and Command Pending bits when the DCP is the 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.

Table 3-9 : Implicit Command Sequences in Direct Control Mode

C/$\overline{K}$	AUX_7 - K/$\overline{D}$	AUX_6 - E/$\overline{D}$	AUX_5 - S/$\overline{S}$	Command Initiated
H	L	L	↑	Start Decryption
H	L	H	↑	Start Encryption
H	L	X	↓	Stop
H	↑	L	L	Load Clear D Key through Master Port
H	↑	H	L	Load Clear E Key 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

The Busy bit will be a "1" whenever the ciphering algorithm unit is actively encrypting or decrypting data. For example, the Busy bit is set in response to a Load Encrypted Key command (the Command Pending bit will go HIGH as well) or in the ciphering of regular text (indicated by the Start/Stop bit being a "1"). If the ciphered data cannot be transferred to the Output Register (due to the presence of data from a previous ciphering cycle), then the Busy bit will remain a "1". The Busy bit will be "0" at all other times, including if no ciphering is possible because no data has been loaded into the Input Register.

The Command Pending bit is set to "1" by any instruction which 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. Therefore, the Command Pending bit will be set following all commands except the three Start Commands, the Stop command and the software Reset command. The Command Pending bit will return to an inactive state ("0") after all eight bytes have been transferred following Load Clear, Read Clear or Read Encrypted commands. In addition the inactive state ("0") only returns after data has been entered, decrypted and placed 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.

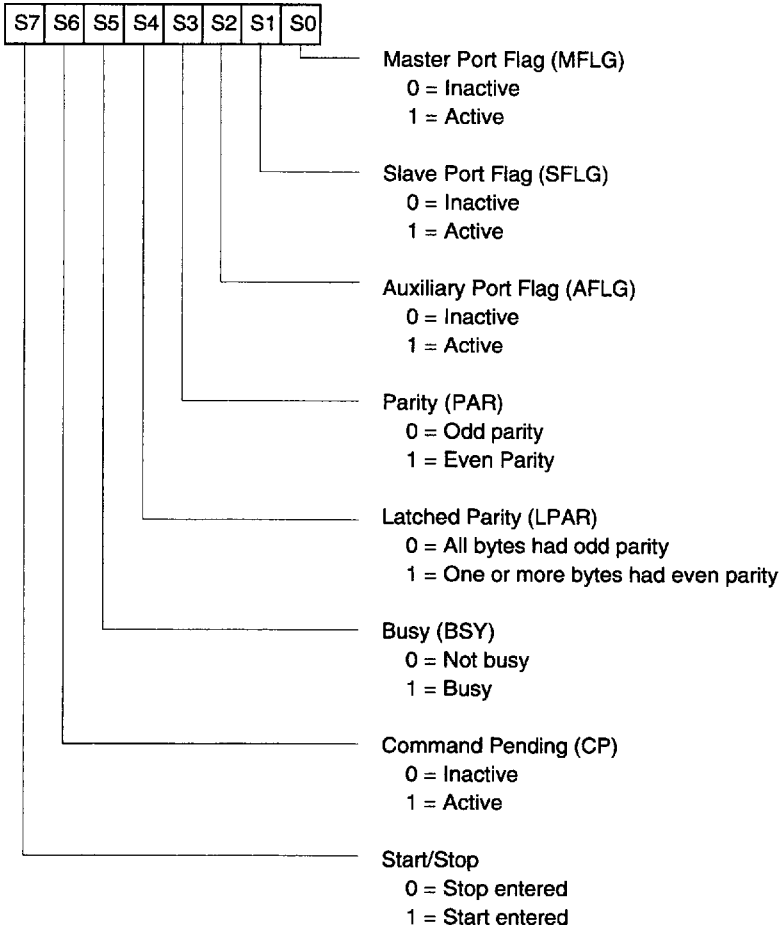


Figure 3-17 : Status Register Bit Assignments

3

Input Register

The 64-bit, write-only Input Register is organized to appear to the user as eight bytes of push-down storage. The number of bytes stored in the register is monitored by a status circuit. The register is considered full when eight bytes of data have been loaded with the ECB or CBC ciphering algorithm in use, or when one byte of data has been entered in either CFB mode. It is considered empty when the data stored in it has been or is being processed. The data in the register won't be destroyed if the user attempts to write data into the Input Register when it is full. Table 3-10 gives a summary of the port flag associated with this register depending on the mode of operation.

Output Register

The 64-bit, read-only Output Register is setup 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 an attempt is made to read data from the Output Register when it is empty, the output buffers will remain in a tri-state condition.

Table 3-10 : Association of Master Port Flag ($\overline{MFLG}$) and Slave Port Flag ($\overline{SFLG}$) with Input and Output Registers

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

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. These registers are not directly addressable, but can be loaded or read in response to a command (See Command Descriptions). The Master key can be loaded only with clear data through the Auxiliary Port. The Encrypt and Decrypt Keys can be loaded as either clear or cipher text through the Master or Auxiliary Port. If the key data is encrypted, it is first routed to the Input Register where it is decrypted using the M Key, and then written to the target key register from the Output Register.

Initialization Vector Registers

Two 64-bit registers are provided to store feedback from Cipher Feedback and Cipher Block Chaining modes of operation. One Initialization 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. If encrypted data is loaded, it is first decrypted before being written into the corresponding IV Register. Both registers may be read out through the Master Port as either clear or encrypted text (see Command Description Section).

PROGRAMMING INSTRUCTIONS FOR MULTIPLEXED CONTROL MODE

This section describes the registers that need programming prior to using the DCP in ECB, CBC, or CFB ciphering modes in Multiplexed Control Mode (MCM) of operation. The programming flow charts for each mode are implemented for a single 8 bit port interface (see the pipelining section for the dual port programming flow chart).

ECB Operation

Figure 3-18 illustrates the programming sequence for ECB.

1) A hardware or software reset must be implemented to bring the device to a known state. A reset clears all bits in the Status Register and programs the Mode Register to it's default setting.
2) Program the Mode Register (see Figure 3-16) with the cipher type and the port configuration. For further explanation see the Mode Register description.
3) The clear Encryption or Decryption Keys can be loaded through either the Master or Auxiliary Ports. The Command Pending bit in the Status Register will go active once a command has been entered in the Command Register. This bit will be active until all eight bytes of the key have been loaded into the Input Register of the DCP.

   An alternative method to Step 3 is to load a Master Key into the DCP through the Auxiliary Port. When this command is entered the AFLG bit in the Status Register will go active ($\overline{AFLG}$ output pin will be active low) until all 8 bytes have been entered. One key byte is loaded on each rising edge of the Auxiliary Strobe ($\overline{ASTB}$).

   A Load Encrypted Session Key command is then entered into the DCP. The Session Key is then decrypted by the Master Key before being stored in the corresponding register. This use of the Master Key allows you to enhance security by frequently changing the session keys over a communication link.
4) One of the three Start commands is then written to the Command Register to begin the ciphering session.
5) Once a Start command is entered, the DCP will indicate that it is ready for data input by activating the corresponding flag bit in the Status Register, as well as the associated input flag pin. Data can now be input through the assigned Input Port. The two flags, $\overline{MFLG}$ and $\overline{SFLG}$, which are associated with the Data Registers can be sensed by hardware or software to know when data is to be entered or removed from the DCP.
6) As soon as the Input flag is active, the DCP is ready to accept data (MSB first). This bit is deactivated once eight bytes of data have been entered.
7) The Output flag goes active whenever the DES algorithm is completed and data is ready to be removed from the Output Register.
8) Data is removed from the Output Port one byte at a time with the most significant byte first. The Output flag becomes inactive upon the removal of the eighth byte.
9) Loop through steps 5 through 9 until the ciphering session should be terminated.
10) The session can now be terminated by issuing the Stop command to the Command Register.

Upon termination, all remaining processed data is available in the Output Register until the DCP is reset. This allows you to enter the Stop command immediately upon entering the last input block. When all the data has been removed from the Output Register, all the flags will be inactive. If the DCP is restarted, any data that was not read out from the previous ciphering session will be lost.

3

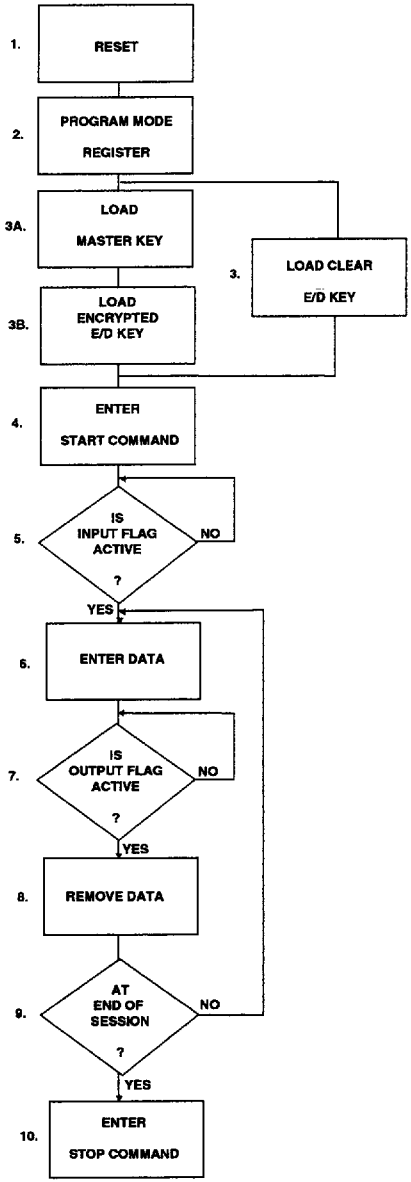


Figure 3-18 : Multiplexed Control Mode ECB Programming Flow Chart

CBC Operation

Figure 3-19 illustrates the DCP programming sequence for implementing the CBC method of ciphering. The programming sequence is identical to the ECB programming sequence except for an extra step included between steps 3 and 4. The Initialization Vectors (IVs) must be loaded before beginning to cipher data. These IVs can be loaded in either clear (step 3.1) or ciphered form (steps 3.1.A and 3.1.B).

3.1 Load in eight bytes (MSB first) of the Initialization Vector through the Master Port.

3.1.A(B) If the Initialization Vector is entered in encrypted form, it is decrypted using the Decrypt Session Key in ECB mode before being stored in the appropriate register. Load the D Key (if not already done) prior to executing an encrypted IV command. The eight IV bytes are then loaded into the Input Register and decrypted. The bits (Cipher Type and Encrypt/Decrypt bit) in the Mode Register are not affected by the decrypting of the IVs.

CFB Operation

The flow chart for the instruction sequence in CFB mode is very similar to CBC mode. The DCP can be programmed to execute in either 1-bit or 8-bit CFB mode. The Input and Output Registers hold between one and 8 bits depending on the cipher type and the setting of bits in the Mask Register. In both modes, the IV is first ciphered by the algorithm unit and the result is then XORed with the input byte or bit (see explanation of Mask Register for CFB-1 mode). The XOR result is then loaded into the Output Register to be read out by the CPU. This result is also shifted into the current IV Register to be used in the next cipher session. When operating in CFB mode, the Output Register must first be emptied before issuing a Stop command to the DCP. If you must stop in the middle of inputting a block of data while using ECB or CBC ciphering in Multiplexed Control Mode, follow this instruction sequence to avoid erroneous data:

1) Issue a Stop command.
2) Read all available data from the Output Register.
3) Reload the Mode Register.
4) Issue a Start command.
5) Wait for the input flag to go active and resume data input.

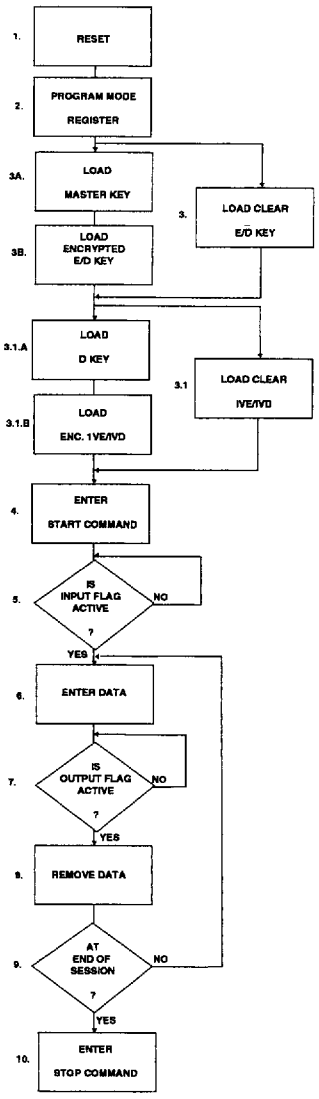


Figure 3-19 : Multiplexed Control Mode CBC Programming Flow Chart

PROGRAMMING INSTRUCTIONS FOR DIRECT CONTROL MODE

This section describes how the DCP functions in Direct Control Mode (DCM), (C/$\overline{K}$ pin is high). Only a subset of the commands that are available in Multiplexed Control Mode can be executed by controlling and monitoring the status of the Auxiliary Port pins. While in DCM, you are unable to access the Mode or Mask Register. The state of the E/$\overline{D}$ and K/$\overline{D}$ pins should be held constant throughout the entire key or data loading process. The state of the S/$\overline{S}$ pin must also be held constant during the entire data ciphering process.

ECB Operation

A flow chart of ECB operation in Direct Control Mode is illustrated in Figure 3-20. A detailed explanation of each step is described below:

In most DCM applications it is desirable to switch back and forth between MCM and DCM; therefore, C/$\overline{K}$ must be programmable. Before using the device, either a hardware or software reset should be performed to set the device to it's default state. If the default mode of operation and the Direct Control Mode instruction set is sufficient for your requirements, then C/$\overline{K}$ may be permanently tied high. If your application does not work in the default mode of operation, the Mode Register must be programmed while in Multiplexed Control Mode (which requires C/$\overline{K}$ to be low).

1) While in Multiplexed Control Mode, any key load commands can be executed before switching back to Direct Control Mode (DCM). Alternatively, the session keys may be loaded while in DCM. When operating in DCM, the DCP does not automatically latch the Input/Output Register's address. Before beginning to load any data into the Input Register, you must latch this address using the address latch enable strobe. Driving the K/$\overline{D}$ pin of the Auxiliary Port high sets up the DCP for key entry (the S/$\overline{S}$ pin must stay low for the entire key loading process). The level of the E/$\overline{D}$ pin determines whether the Encryption or Decryption Session Key will be loaded. As soon as the $\overline{CP}$ output pin goes low you may begin to strobe in the eight key bytes using the Master Port Write Strobe ($\overline{MCS}$ must be held low throughout the entire byte loading process).
2) Once the key loading process is complete, you may now enter a Start command by driving the S/$\overline{S}$ line high. The level on the E/$\overline{D}$ pin at this time will determine whether the data is encrypted or decrypted. The levels on the K/$\overline{D}$ and S/$\overline{S}$) pins must be low throughout the data ciphering process. The DCP responds to this command by lowering the Input Port flag (see Table 3-10).
3) Whenever the Input flag is active, data can be entered through the Master or the Slave Port, depending on the selected mode of operation. To achieve the highest throughput, the DCP must be configured to work in the pipeline mode of operation. When the DCP has processed the data, the Output flag will become active and the data may be removed from the Output Port.
4) Once all the data has been ciphered and read from the output port, the DCP should be returned to the inactive state by driving the S/$\overline{S}$ pin low.

Note: You must remove all the data from the output port before stopping the DCP or the data will be lost. Similarly, the key reloading process can not begin until all the data from the previous ciphering session has been removed from the output port.

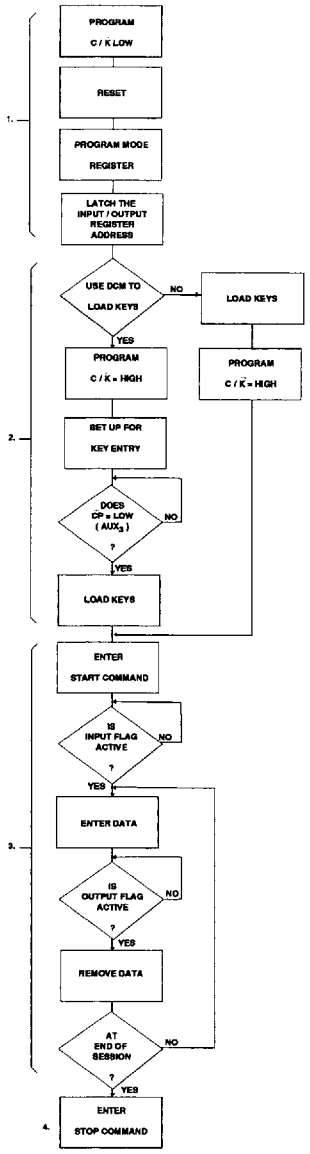


Figure 3-20 : Direct Control Mode ECB Programming Flow Chart

CBC and CFB Operation

The instruction sequence to perform CBC or CFB operation in Direct Control Mode (DCM) is similar to ECB mode of operation. When operating in these modes, the C/$\overline{K}$ pin must be programmable because the IV needed for CBC and CFB can only be loaded while in Multiplexed Control Mode. If you are using CFB-1 ciphering, the Mask Register must also be loaded before entering DCM. When operating in this mode you must ensure that a Stop command is not issued while the Command Pending or Busy pins are active, or when there is data still remaining in the Output Register. (see Figure 3-21 for a programming flow chart).

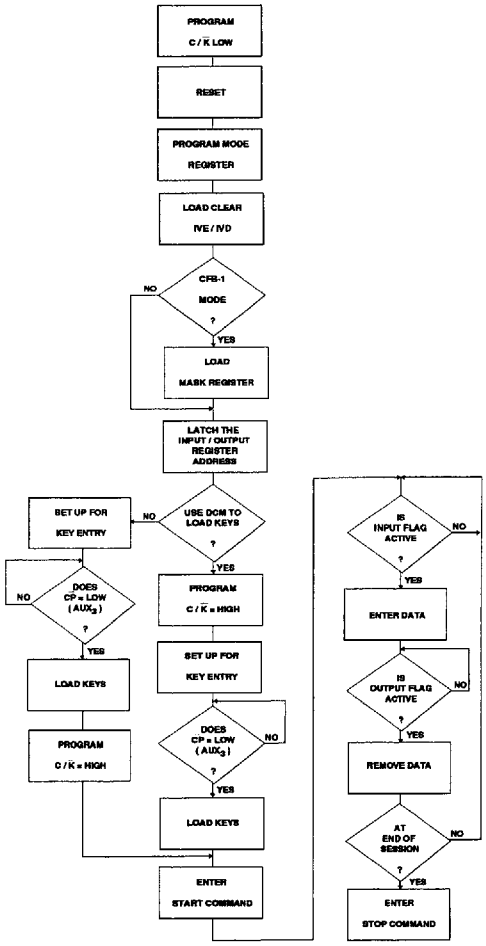
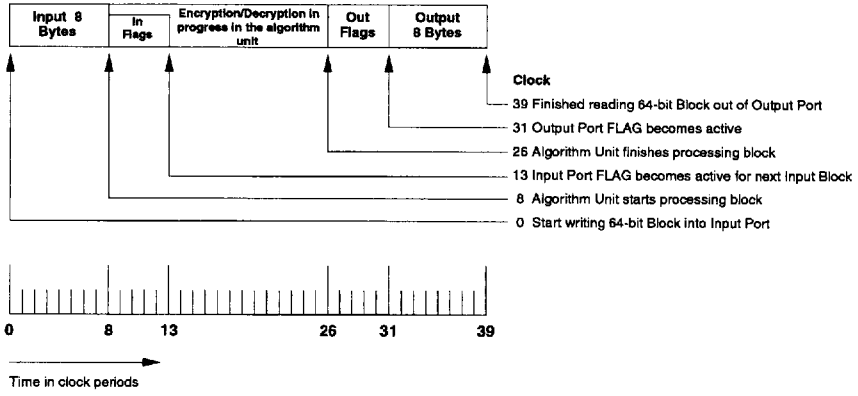


Figure 3-21 : Direct Control Mode CBC/CFB Programming Flow Chart

Maximum Throughput

The pipelined architecture of the DES DCPs allows simultaneous input, ciphering, and output operations. Maximum throughput is obtained when the device is configured for one of the dual port configurations. Figure 3-22 shows the timing for ciphering one block of 64 bits in either ECB or CBC modes of encryption. The inputting of the 64 bits of data takes 8 clock cycles to complete with one data strobe being issued per clock cycle. This data must then be transferred from the Input Register to the algorithm processing unit and the flags updated, which requires 5 additional clock cycles. The algorithm unit begins ciphering concurrently with the transfer and once the flags have been updated another 64 bit block may be entered. The ciphering of the first block is completed after 18 clock cycles have elapsed from the last byte having been written to the Input Register. Another 5 clock cycles are required to transfer the ciphered data to the Output Register and update flags. Transferring of data from the algorithm processing unit to the Output Register can be performed concurrently with loading new data into the DES algorithm unit. Removing the data from the Output Register involves 8 clock cycles with one data strobe per clock cycle. The whole procedure of ciphering one block takes 39 cycles but because the different operations can be overlapped, the DCP can process one block every 18 clock cycles once fully loaded.



Note: CA95C68 minimum clock period = 40 nanoseconds

Figure 3-22 : Detailed Timing of One Block

Pipelining

Once the device has been initialized for dual port configuration, two data blocks are loaded into the device to fill the Output Register and the DES algorithm processing unit. Now blocks of data can be strobed in and out concurrently. When the ciphering session is completed the DCP must be emptied by reading out the last two bytes.

Figure 3-23 illustrates a programming flow chart for programming the DCP for pipelined mode of operation.

Figure 3-24 shows the minimum timing configuration for maximum throughput for this device. The total time to transfer "n" blocks is (n+1)x18+3 clock cycles. The DCP can also be operated in pipelined mode when configured for signal port operation. Once initialized, one block of data is loaded into the device. Then, in a loop, one block of data is strobed in and one block is read out. The first block of data loaded before entering the loop is ciphered while the input of the second block is occurring.

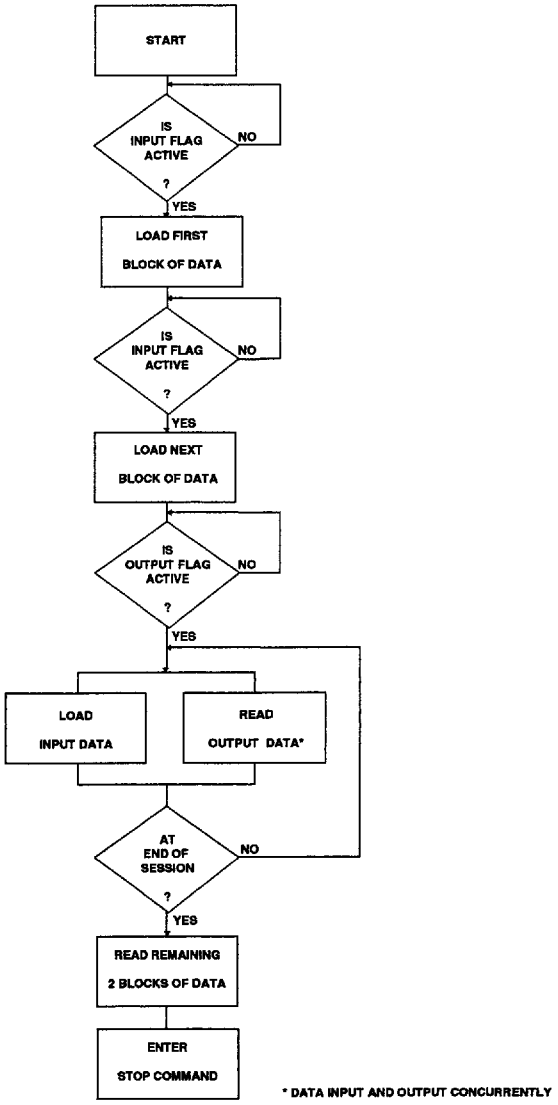
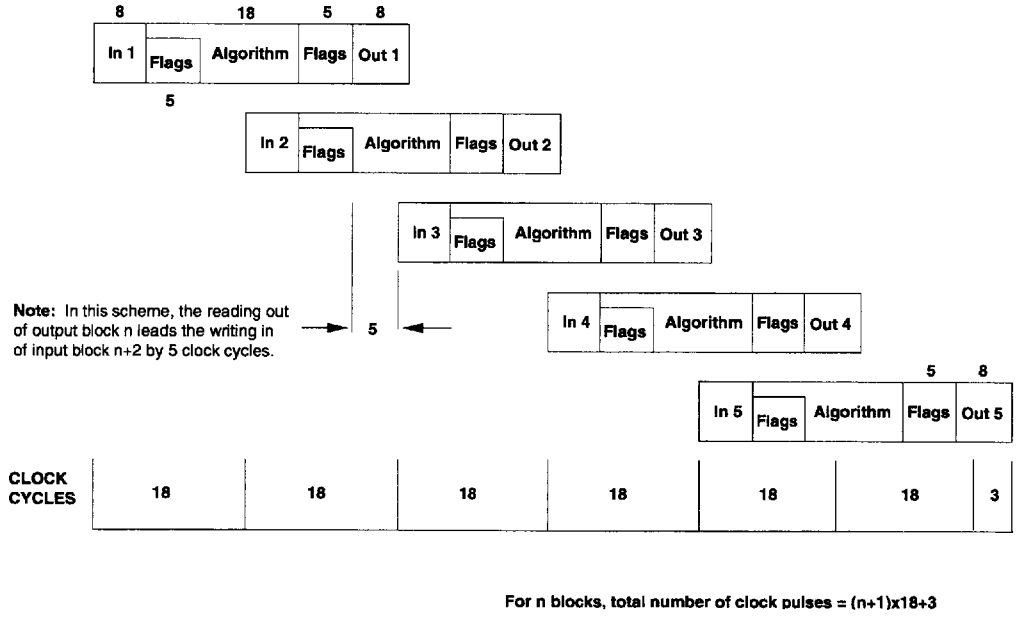


Figure 3-23 : Pipelining Operational Flow Chart



For n blocks, total number of clock pulses = (n+1)x18+3

Figure 3-24 : Pipelined Minimum Timing Operation

3

COMMAND DESCRIPTION

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. Table 3-8 shows all commands that may be given in Multiplexed Control Mode and Table 3-9 shows the 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 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. Once the load command is written to the Command Register, the Auxiliary Port flag ($\overline{AFLG}$) pin will go active (LOW), as well as the Auxiliary Port Flag bit (S2) in the Status Register being set to "1", indicating that the device is able to accept key bytes at the Auxiliary Port bus. In addition, the Command Pending bit (S6) will go to "1" during the entire loading process.

When data has been setup on the Auxiliary Port pins, each byte is written by placing an active LOW signal on the Auxiliary Port Strobe ($\overline{ASTB}$). The actual write occurs on the rising edge of $\overline{ASTB}$. The Auxiliary Port Flag ($\overline{AFLG}$) will go inactive immediately after the eighth strobe goes active (LOW). However, the Command Pending bit (S6) 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.

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 allow eight bytes of data to be written to the appropriate key register through the Master Port. In Multiplexed Control Mode, the command is initiated by writing the instruction 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 and the level on AUX_6-E/$\overline{D}$ determines which key register is loaded.

When the command has been recognized, the Command Pending bit (S6 in the Status Register) will go to "1" and in Direct Control Mode AUX_3-$\overline{CP}$ will go active (LOW), indicating that key loading may proceed. The host system then writes exactly eight bytes to the Input Register through the Master Port. When the Key Register has been loaded, the Command Pending bit 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 ($B2_H$)

These commands are only available in Multiplexed Control Mode. They are similar to the Load Clear E (or D) Key through Auxiliary Port commands, except that key bytes are initially decrypted using the Electronic Code Book algorithm and the Master (M) Key. The key bytes then pass through the parity checking logic and into the appropriate key register.

The Command Pending bit (S6) will be "1" during the entire decrypt-and-load operation. The Busy bit (S5) will be "1" during the actual decrypting of the key.

Load Encrypted E Key Through Master Port (31_H)

Load Encrypted D Key Through Master Port (32_H)

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

The Command Pending bit (S6) will be "1" during the entire decrypt-and-load operation. As well, the Busy bit (S5) 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 (available 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 transferred to either the Initialization Vector for Encryption (IVE) or Decryption (IVD) Register instead of a Key Register and no parity checking takes place. The Command Pending bit (S6) 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 similar to the Load Encrypted E (or D) Key Through Master Port commands. The data flow specification set in the Mode Register is overridden and the eight initial vector bytes are decrypted using the Decryption (D) Key and the Electronic Code Book algorithm. The resulting clear initial vector bytes are routed into the appropriate Initialization Vector Register, and no parity checking occurs. The Busy bit (S5) does not go to "1" during the decryption process, but Command Pending bit (S6) 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 (available in Multiplexed Control Mode only) is to override the data flow specifications set in the Mode Register and to allow the appropriate Initialization Vector Register to be read from the Output Register through the Master Port. When executing this instruction, each IV Register appears as eight bytes of FIFO storage. The first byte of data will be available six 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 Initialization Vector Register using the Electronic Code Book algorithm and the Encrypt (E) Key. The resulting eight bytes of cipher text can be read from the Output Register through the Master Port. The Busy bit (S5) will be "1" during the encryption process, when it goes to "0, "the encrypted initial vector bytes are ready to be read out. The Command Pending bit (S6) 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 (available in Multiplexed Control Mode only) overrides the data flow specifications set in the Mode Register and causes the DCP to write eight bytes of data to the Input Register via the Master Port. After the eighth byte has been received, the data is encrypted using the Master (M) Key and then routed to the Output Register, where it may be read out through the Master Port. The Command Pending (S6) and Busy (S5) 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 got 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.

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 (S7) in the Status Register to "1." The Start Encryption and Start Decryption commands specify the ciphering direction by forcing the Encrypt/Decrypt bit (M4) in the Mode Register to "1" or "0", respectively. Whereas Start uses the current state of the Mode Register Encrypt/Decrypt bit, as specified in a previous Mode Register load. When any Start command has been entered, the port status flag (MFLG or 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 of the AUX_5-S/$\overline{S}$ input. 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 sets the Start/Stop bit (S7) 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 data. Any ciphering in progress (Busy bit (S5) is "1" or AUX_2-$\overline{BSY}$ is active) will be completed and any data in the Output Register will remain accessible (except in CFB Mode). In either 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.

Software Reset (00_H)

This command is similar to a hardware reset (CA95C68: $\overline{MRD}$ and $\overline{MWR}$ low, CA95C18: $\overline{MAS}$ and $\overline{MDS}$ low) in that it forces the DCP back to its default configuration, and all the processing flags go inactive. The default configuration for the Mode Register is: Electronic Code Book cipher type and dual port configuration with Master Port clear, Slave Port encrypted.

CA95C68/18/09 NOTES

This listing describes known operating variants between the CA95C68/18/09 devices and both the AMD AM9568/18 and VLSI VM009 devices. Also contained here are some CA95C68/18/09 operating idiosyncrasies.

1) **CA95C68/18/09 Reset**: The CA95C68/18/09 device does not operate in the default mode of operation until one of the reset operations are performed on it. Either a hardware reset, a software reset, or a write to the Mode Register must be performed before beginning to program the CA95C68/18/09 to ensure that the device is operating in the default mode.
2) **CA95C68/18/09 Direct Control Mode**: When the CA95C68/18/09 is programmed for Direct Control Mode (DCM) operation, the Input and Output Register address and $\overline{MCS}$ must be manually latched immediately before or immediately after DCM is entered. The device does not automatically address the Input and Output Registers (Address 0) when DCM is entered. This should be done before any operations are performed.
3) **CA95C68/18/09 Busy Bit in CFB-8 Cipher Mode**: When the CA95C68/18/09 is programmed for eight bit cipher feedback (CFB-8), ciphering in either Multiplexed Control or Direct Control Mode of operation, the Busy bit (bit 5 in the Status Register) and the $\overline{BSY}$ pin (AUX_2-$\overline{BSY}$ in DCM) go active before the Input Register is addressed. The Busy bit and the $\overline{BSY}$ pin go active immediately after the Mode Register is programmed for the CFB-8 cipher type. This bit (and pin in DCM) is not of great importance and should be ignored in this mode of operation.
4) **Synchronization for CA95C68/18/09 and VM009 Read/Write**: Compared to the VLSI VM009 device, the CA95C68/18/09 has a narrower window in which the read and write strobes must synchronize to the clock input. The CA95C68/18/09 AC parameter in question is t_{45} which is specified as a minimum of 2ns and a maximum of t_c-25ns. Therefore, the CA95C68/18/09 read and write strobes must be driven HIGH between 2 and 15ns after the falling edge of the clock if you are using the DCP at 25MHz. With the VLSI device, the read and write synchronization occurs on the rising edge of the clock and there is only a 4ns region in which the strobes can not go HIGH for any clock frequency.
5) **Clock Frequency**: The clock input frequency for the various devices are:

AM9568	1.0 MHz to 4.0 MHz
AM9518	1.0 MHz to 3.1 MHz
CA95C68/18/09	0 MHz to 25MHz
VM009	0 MHz to 33 MHz

6) **One-Bit Cipher Feedback Mode**: This is a mode of encryption supported by the CA95C68/18/09 that the AMD and VLSI devices do not provide.

3

7) **Flag Output Assertion Timing Variant**: The AM9568/18 devices set and clear the flag output lines immediately after the corresponding event has occurred. The CA95C68/18/09 devices synchronize all internal events with respect to the falling edge of the clock input. Therefore, the flag output lines are set or cleared on the next falling clock edge after the corresponding event has occurred.

8) **IVE in Pipelined CBC Mode of Encryption**: The AM9568/18 presents the previous IVE instead of the current IVE during a read IVE operation after a series of CBC encryptions in which more than one round of data was in the encryption pipeline. In the CA95C68/18/09 devices, the correct IVE is presented for the pipelined CBC mode encryption scheme.

9) **Direct Control Mode, Mode Register Encrypt/Decrypt Bit Variant**: In Direct Control Mode (DCM), the AM9568/18 adjusts the sense of the Mode Register's Encrypt/Decrypt bit (M4) inconsistently; based on whether encryption or decryption is performed. The CA95C68/18/09 always sets the Encrypt/Decrypt bit to be the same sense as the AUX_6-E/$\overline{D}$ input line in this case.

10) **Key Parity in Direct Control Mode**: The AM9568/18 erroneously indicates a parity error during the loading of keys of correct parity in Direct Control Mode. The CA95C68/18/09 devices do not indicate a parity error in this scenario.

11) **Encrypted Key Load Parity Variant**: The AM9568/18 will clear a parity error regardless of whether the last byte of an encrypted key load has a parity error. The CA95C68/18/09 devices will indicate the parity of the last byte of an encrypted key load correctly, and if required, the parity error must be cleared by one of the specified methods.

12) **Mode Register's Encrypt/Decrypt Bit Status on a Command Abort Reset**: The AM9568/18 will not set the Encrypt/Decrypt bit high if that bit is low and a command is aborted. The CA95C68/18/09 devices will reset this bit high when the Mode Register is reset during a command abort sequence.

NEWBRIDGE MICROSYSTEMS

RBG 1210

RANDOM BIT GENERATOR

- **Operational speeds up to 20,000 bits/second**
- **Each value is independent of all other values**
- **No seed value required**
- **No hardware/software algorithms required**
- **Based on Johnson Noise phenomenon**
- **Single 12 Volt supply**
- **TTL compatible I/O**
- **Shielded package**

APPLICATIONS

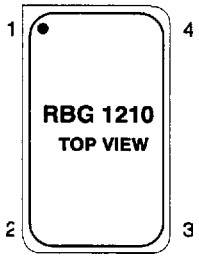
- **Encryption Systems**
- **Statistical Analysis**
- **Password Generation**
- **Seed Generator**
- **Fair Selection**
- **Monte Carlo Analysis**
- **Natural Phenomenon Simulation**

The RBG 1210 Random Bit Generator produces truly random bits. Based on the naturally occurring random phenomenon, Johnson noise, the RBG 1210 requires no initial starting value or seed. Furthermore, each new value is completely independent of all previous values. Unlike digital logic circuits or software based algorithms, the RBG 1210 is not pseudo-random; there is no repeating pattern, giving an infinite cycle size. This makes the RBG 1210 ideal for applications where purely random bits are required.

TTL compatible STROBE and OUTPUT signal pins are provided to allow the RBG 1210 to be easily connected into any digital system.

Table 3-1 : Pin Descriptions

Pin	Function
1	Gnd
2	STROBE
3	OUTPUT
4	+12V



3

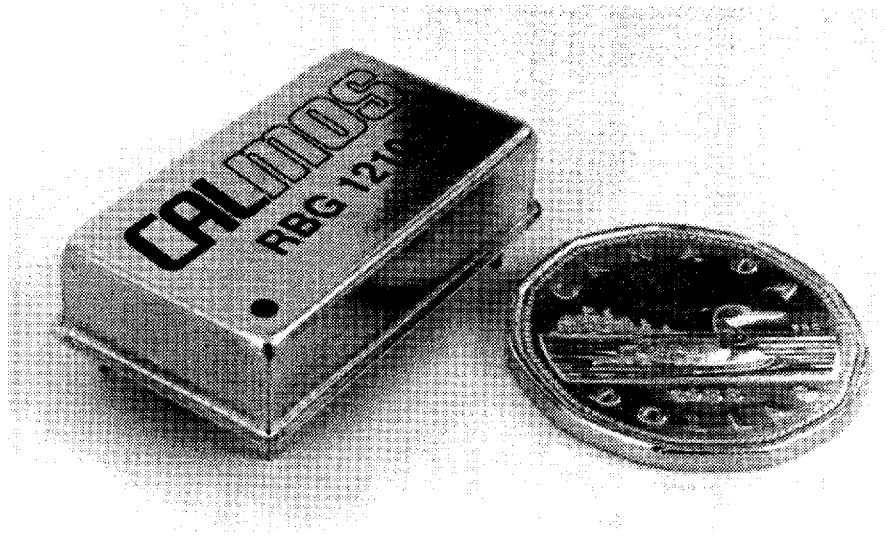


Figure 3-1 : RBG 1210 Random Bit Generator

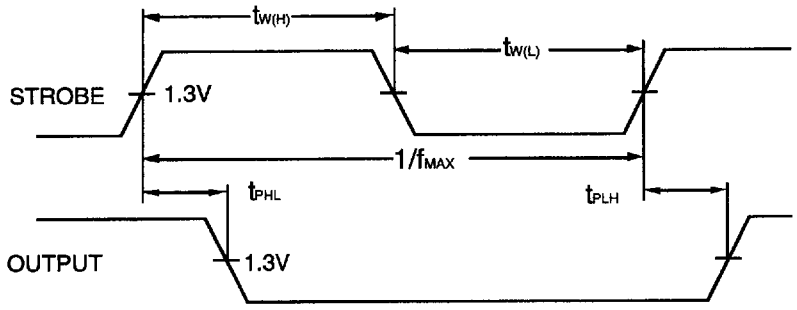


Figure 3-2 : Timing Diagram

Table 3-2 : AC Characteristics (V_{CC} = 0° to 70°C)

Symbol	Parameter	Test Conditions	Limits			Units
			Min	Typ	Max	
f_{MAX}	Maximum strobe frequency	C_L = 15pF	1	-	20	kHz
t_{PLH}	Strobe to output delay		-	13	25	nS
t_{PHL}			-	25	40	nS
$t_{W(H)}$	Strobe width		25	-	-	nS
$t_{W(L)}$	Supply voltage		25	-	-	nS

Table 3-3 : DC Characteristics (V_{CC} = 0° to 70°C)

Symbol	Parameter	Test Conditions	Limits			Units
			Min	Typ	Max	
I_{CC}	Supply current	V_{CC} = 12V	-	-	30	mA
I_{IH}	Input current @ max input voltage	V_{IH} = 7V	-	-	0.2	mA
	High level input current	V_{IH} = 2.7V	-	-	40	µA
I_{IL}	Low level input current	V_{IL} = 0.4V	-	-	-0.8	mA
I_{OS}	Output short circuit current	V_{CC} = 12V	-	-	-100	mA
V_{CC}	Supply voltage		10.5	12.0	16	V
V_{OH}	High level output voltage	I_{OH} = -400µA	2.7	3.5	-	V
V_{OL}	Low level output voltage	V_{IH} = 2V, I_{OL} = 8mA	-	0.4	0.5	V

FUNCTIONAL DESCRIPTION

The RBG 1210 uses a new and different approach to produce random bits which are neither predictable, nor repeatable, unlike computer generated pseudo random numbers, which are both. True randomness occurs naturally in electronic circuits, as evidenced by the background hissing sound heard from radio and audio equipment. Normally, amplifier circuits are carefully designed to minimize this problem. However, in the CA1210 RBG, such amplifier noise has been captured and purposely designed in.

Mathematically, this can be represented as follows. With reference to the noise equivalent circuit of an amplifier shown in Figure 3-3, the total input referred noise density is given by:

$$e_t = \sqrt{e^2 + r^2 + \langle iR \rangle^2} \qquad \left(\frac{V}{\sqrt{Hz}}\right)$$

where: R is the equivalent source resistance (Ohms),

r is the thermal noise of the input resistor $\left(\frac{V}{\sqrt{Hz}}\right)$,

e is the input noise voltage density $\left(\frac{V}{\sqrt{Hz}}\right)$ and

i is the input noise current density $\left(\frac{A}{\sqrt{Hz}}\right)$.

Also $r = \sqrt{4kTR}$

where: k is the Boltzmann constant ($1.38X10^{-23}$ joules/°K) and T is the temperature of the resistor (°K).

The input resistor value is chosen to maximize the contribution of the resistor thermal noise relative to the voltage and current sources. This ensures a wideband noise source with equal noise densities at all frequencies. Thermal noise is due to the random motion of free electrons in the resistor

Figure 3-4 shows a block diagram of the RBG 1210, which consists of a noisy amplifier and an analog to digital converter (A/D). The noise from an input resistor is amplified to about $50mV_{RMS}$. This white noise signal is then converted to a stream of binary levels by an A/D converter. This A/D is designed to equalize the probability of 1s and 0s, and negate the effects of component parametric tolerances and power supply voltage variations. The output is a standard TTL (transistor-transistor logic) level signal that is latched on the rising edge of the strobe signal.

To produce longer random numbers, one RBG 1210 may be read several times and the resulting bit stream saved until the desired number length has been obtained. A second approach is to connect several RBG 1210s in parallel to produce wider numbers. The serial approach is more cost effective (since only one RBG 1210 is required), while the parallel approach offers a substantial speed advantage, as no delay is incurred after reading each bit.

The NM 810 RNG Random Number Generator is an implementation of the latter approach, with eight RBG 1210s in parallel and a PC XT/AT bus interface. Random bytes are input to the computer through an I/O (Input/Output) port. Any data type (integer, floating point etc.) can then be easily constructed in software by using successive random bytes and arranging them according to the desired internal data format.

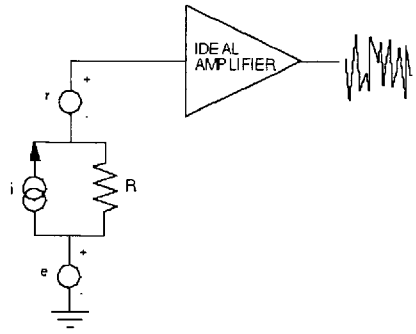


Figure 3-3 : Equivalent Circuit of an Amplifier

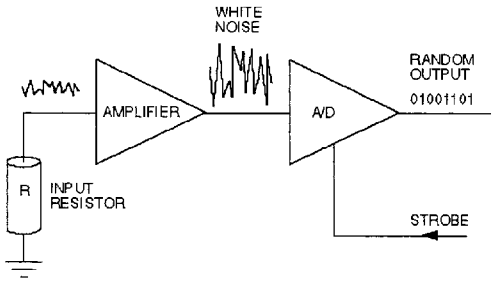


Figure 3-4 : RBG 1210 Block Diagram

TESTING FOR RANDOMNESS

The RBG 1210 Random Bit Generator has been successfully tested for true randomness against an extensive set of recognized tests which include; Chi squared, KS test, frequency test, serial test, poker test, coupon collector test, run test, collision test and picturing randomness. These tests results are available from Newbridge Microsystems.

NEWBRIDGE MICROSYSTEMS

NM 810 RNG

RANDOM NUMBER GENERATOR

- **Easy to install PC XT/AT board**
- **Eight independent random bit generators**
- **No seed required**
- **Up to 20,000 bytes/second operation**
- **No hardware/software algorithms**
- **Based on Johnson Noise**
- **Terne coated steel shield**

APPLICATIONS

- **Encryption systems**
- **Password generation**
- **Seed generation**
- **Audit accounting**
- **Statistical analysis**
- **Fair selection**
- **Monte Carlo analysis**
- **Simulating natural phenomenon**

The NM 810 RNG Random Number Generator uses a proprietary technology to create truly random numbers. Since the NM 810 RNG is based on a naturally occurring random phenomenon (Johnson Noise) rather than a digital logic circuit or computer program, it requires no initial starting value and each new value is independent of all previous values. Unlike software based algorithms, the NM 810 RNG is not pseudo-random; there is no repeating pattern and the cycle size is infinite. Thus the NM 810 RNG is ideal for those applications where pure random numbers are required.

Many built in random functions of computer languages, spreadsheets and simulation packages are statistically flawed. These functions require seeding, which can lead to unreliable results if not done carefully, though often the user has no control over this process. The NM 810 RNG avoids these limitations by providing pure random numbers which are neither predictable, nor repeating.

Designed for PC XT/AT or compatible systems, the NM 810 RNG board is supplied with documentation and sample programs which demonstrate its use.

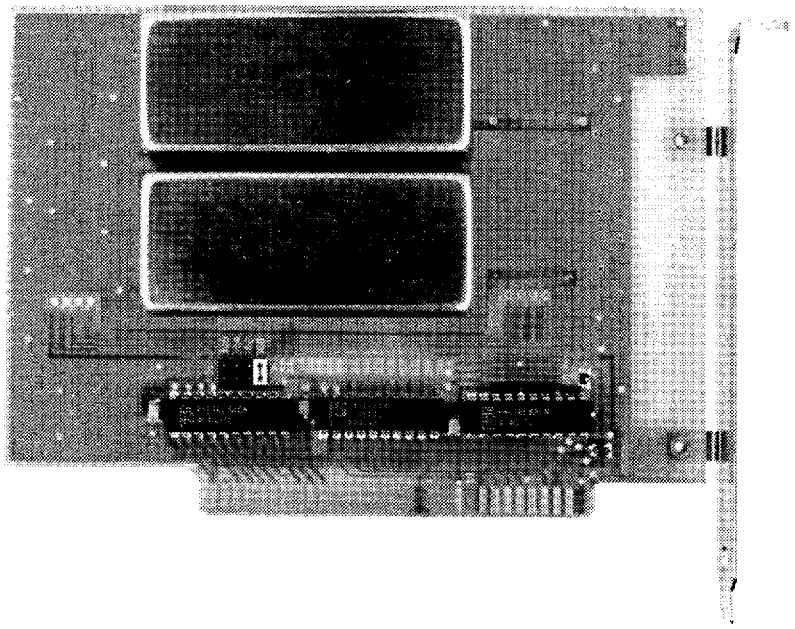


Figure 3-1 : NM 810 RNG Board

INTRODUCTION

The NM 810 RNG

The Newbridge Microsystems NM 810 RNG Random Number Generator card is a PC XT/AT or compatible accessory which provides the user with true random-number generation capability, unlike the pseudo-random numbers generally produced by standard PC randomizing functions. Such pseudo-random numbers are based on algorithms which repeat after a certain number of cycles or iterations, and are sufficient only for trivial applications. However, for sophisticated applications where truly random characteristics are necessary, the NM 810 RNG card is the ideal source for genuine random numbers.

The Source of the Numbers

The numbers from the RNG card originate from eight completely independent, RBG 1210 Random Bit Generator noise sources located on the card (shown in the Block Diagram of Figure 2). Each RBG 1210 noise source is based on the phenomenon of Johnson noise (resistor thermal noise). The random noise produced by these sources is converted into digital random noise signals (Digital random noise is a stream of unpatterned, unpredictable ones and zeros). These digital signals are sampled each time the NM 810 RNG is accessed by the user's software, to produce a random eight bit (one byte) number which appears at the active port address.

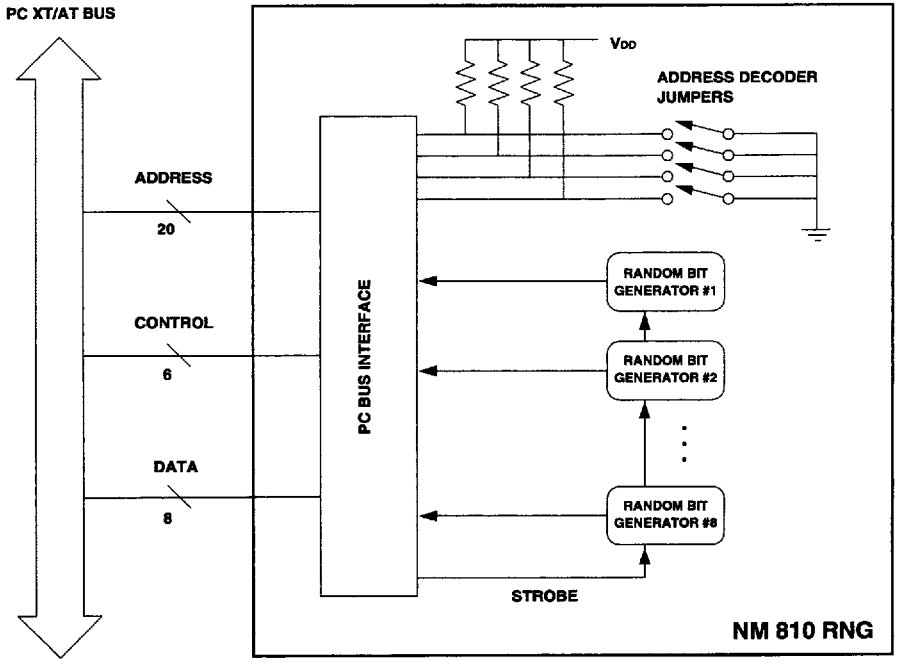


Figure 3-2 : Block Diagram of the NM 810 RNG Random Number Generator

INSTALLATION

The random bytes produced by the card are addressed at I/O port 300_{16}, 302_{16}, 304_{16} or 306_{16} (in hexadecimal, or base sixteen). These are the addresses reserved by the PC for accessing prototype cards. The active port address is selected by configuring a jumper (J1) located near one of the programmable array logic (PAL) units (Figure 3). The cards are factory configured for port 300_{16}. One of the alternate port addresses will be necessary if more than one NM 810 RNG card is present in the computer or another card is already using port 300_{16}. If this is the case, simply move the jumper to select the preferred address before installation. For most applications, port 300_{16} is the only location which you will have to access. Note that any program accessing the NM 810 RNG must use the correct port address, otherwise no random numbers will be transferred.

The NM 810 RNG card can be plugged into any PC XT or PC AT, or any true compatible. To install, follow these steps:

1) Turn the power off, and unplug the computer.
2) Remove cover.
3) Select a suitable (free) slot.
4) Remove the blank bracket associated with the slot.
5) Plug in the NM 810 RNG card. Be sure the correct port address is set.
6) Fasten mounting bracket with screw.
7) Replace cover.
8) Turn power on and reboot computer.

3

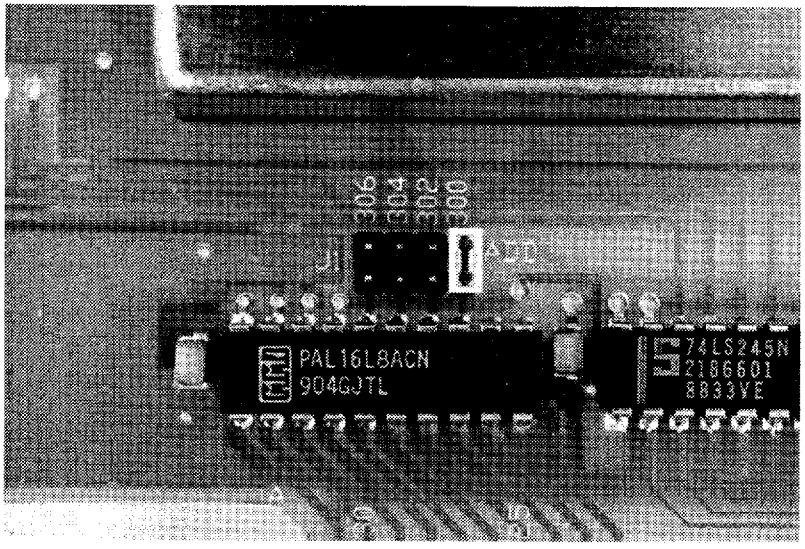


Figure 3-3 : Address Jumper Selection

ACCESSING THE RANDOM BITS

Programming languages have commands which allow the user to access ports (for example, the Pascal command called, logically enough, PORT). In Pascal, to access a port one merely assigns its value to a variable with the statement:

Variable: = Port[$300];

In Pascal, the use of a dollar ($) sign before a number indicates that the number is in hexadecimal (base sixteen). In Pascal there is also a PORTW command which accesses a word, which is two bytes long, beginning at the specified location. This command will not generally be used with the RNG card, as the random numbers from the card are only one byte long.

Though Pascal may not be the language used to create code for the RNG card, the language selected will have some means of accessing ports. As long as port 30016 can be read, or selected, the RNG card can be used for any applications requiring random numbers.

It is important to note here that the random characteristics of the bytes can be adversely affected by accessing them too quickly. Sampling bytes from the card too quickly increases the correlation between successive bytes. Thus the bytes will not be independent of each other and will not be random. It is recommended that the data access frequency from the card be no greater than 20,000 bytes per second. This is equivalent to waiting 50 µs between each successive port access.

Scaling Output Data from the NM 810 RNG

Since bytes have a range of values only from zero to 255, using this format alone will somewhat restrict the use of the RNG card. The full numeric potential of the card is realized when the bytes from the card are combined to form numbers with larger ranges. For example, it is relatively simple to read two bytes (waiting at least 50 µs before reading the second byte) and then concatenate them to form an integer-type number. This number will have possible whole-number values ranging from zero to ±32,767.

A note of caution... It may be tempting to simply multiply the integer numbers by a scaling factor to bring them into a desired range. However, this is not a good idea, as the numbers so created will have 'gaps' that can't be filled. For example, suppose the random integers are multiplied by two to yield new 'random' numbers between zero and 65,534. Note that for this new set of numbers it is impossible for odd numbers to occur (as all are multiples of two). This creates what is called a limited resolution of the set of numbers produced.

A numerical format which solves this problem is that of a real number. This type of number has a range of at least $\pm 8.43 \times 10^{-37}$ to $\pm 1.65 \times 10^{38}$. This yields a 'resolution' which usually exceeds that of the programming language. Thus, using this real numbers, random numbers in any range can be created, with the 'randomness' of all the numbers maintained.

It is important to consult the system reference manuals and documentation for the computer and language being used to determine the exact real number representation, as a thorough lesson in how computers view real numbers is beyond the scope of this document. Note that the representation of real numbers varies substantially among different computers and languages. It may be helpful to create a program which displays the byte-by-byte breakdown of a real number; arguably the fastest way to learn how to manipulate the random bytes to form a random number.

Real Number Representations

However, some discussion of the representation of real numbers in the computer is needed. This representation, as previously stated, varies between computer languages, but usually involves four to eight bytes. The number of bytes needed to represent a real number determines the maximum and minimum sizes of the numbers, as well as the resolution. The more bytes that are used, the better the resolution and the larger the possible range of the numbers. For example, Pascal uses six bytes to represent its real numbers, and will be used as the example.

The computer uses a binary scientific notation to represent real numbers, instead of having a different bit configuration for every possible number. This reduces the memory space that each number occupies. A real number is represented as one plus a fraction, multiplied by two raised to an exponent. Only the fraction, the exponent and the sign of the number are stored; the one (1) is assumed, as is the base of two.

For example, the real number 197.625 is represented in binary scientific notation as 1.1000101101 x 27. This number is stored in memory by Pascal as 10001000 00000000 00000000 00000000 10100000 01000101. Pascal arrives at this number by first adding 129 to the exponent of two; in this case, the exponent is 7. This biasing of the exponent is common to all languages – it is used as a means of adjusting the 2s complement form of the exponent so that positive and negative exponents can be directly compared in magnitude. The result of this biasing can be seen in the first byte, which represents 7 + 129 = 136. The sign of the number is represented in the most significant bit of the last

byte, the sign bit. Thus, if this number were the same value but negative, the last byte would be 11000101. The rest of the bits represent the fraction which is added to one. The last five bytes of the number are laid end-to-end in reverse order (ignoring the sign bit) to form the fraction 1000101101 plus the trailing zeros. Again, the computer documentation will contain a more detailed explanation of the binary representation of real numbers in the computer and language being used.

Once the programming language's representation of real numbers is known, it is easy to convert the random bytes to real numbers of any size. Change the exponent part of the real variable being used to zero (e.g.: 129 for Pascal). Place random bytes into the rest of the real variable. You now have a number equal to ±1 plus some fraction. Now take the absolute value of this number and subtract one. This leaves some fraction in the range zero to slightly less than one. This fraction can then be scaled up to the magnitude that is most useful.

The resolution of the numbers created depends on the number of bits used in the original fraction. For a real number of four bytes (the minimum), 23 bits are used for the fraction, yielding a resolution of approximately 0.00000012. Thus, given a four-byte real number, the maximum multiplying factor to create random whole numbers is about one million. To create random numbers with fractional parts, the maximum factor size must be scaled down according to the smallest fractional part desired. There are many ways of manipulating the random bytes to create numbers of any size and resolution.

Sample Programs

Several programs are provided on the distribution disk which demonstrate the capabilities of the NM 810 RNG. Source code is provided in Turbo Pascal® v5 to show the techniques that can used to address the card. Using the NM 810 RNG with any other computer language (such as C, Fortran, BASIC ...) will be very similar.

3