FAIRCHILD
A Schlumberger Company

F9414
4-Chip Data Encryption Set

Microprocessor Product

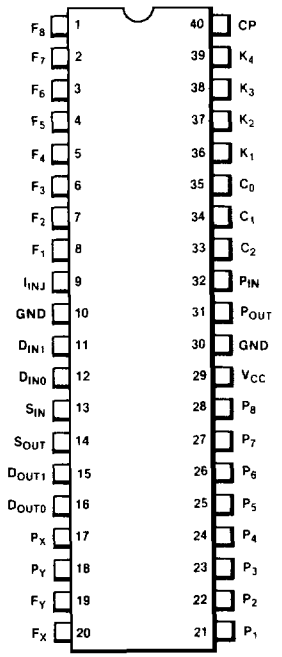
Description

The Fairchild F9414 4-Chip Data Encryption Set consists of four similar 40-pin $I^3L^{®}$ LSI devices (the 9414-1, 9414-2, 9414-3, and 9414-4), and is designed to implement the National Bureau of Standards data encryption standard (DES) algorithm (FIPS-46). The set uses a 56-bit key word to encipher or decipher a 64-bit word that is stored in 8 bytes; 2 bits of each byte are distributed to each of the four chips.

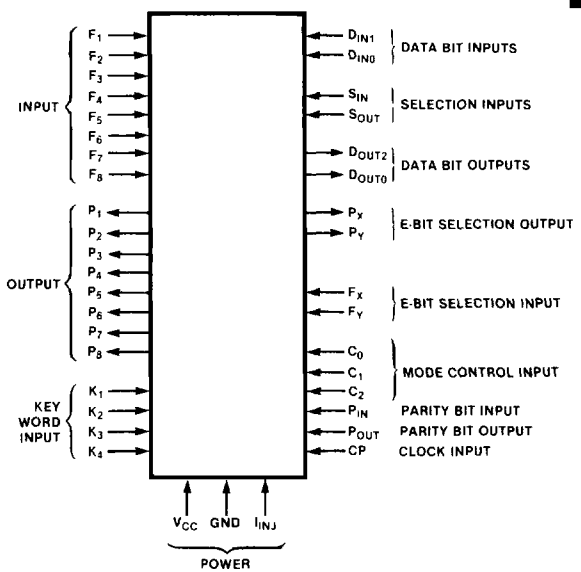
The major elements of each chip include a pair of data registers, four 8-bit shift (key) registers, control logic, and two 64-word by 4-bit read-only memories (ROMs). The F9414 encryption set has passed the NBS functional validation test.

- **High Throughput**
- **LSTTL Input/Output**
- **Single Clock**
- **Parity Testing**
- **Simultaneous Load and Output Data**
- **Cipher Feedback and Block Chaining**
- **3-State Data Buffers**
- **Single 5V Power Supply**
- **5 MHz Operation Typical**
- **Data Throughput — 4.8 μs Per 64-Bit Word**

Connection Diagram



Signal Functions



6

Signal Descriptions

The F9414 input and output signals are described in table 1.

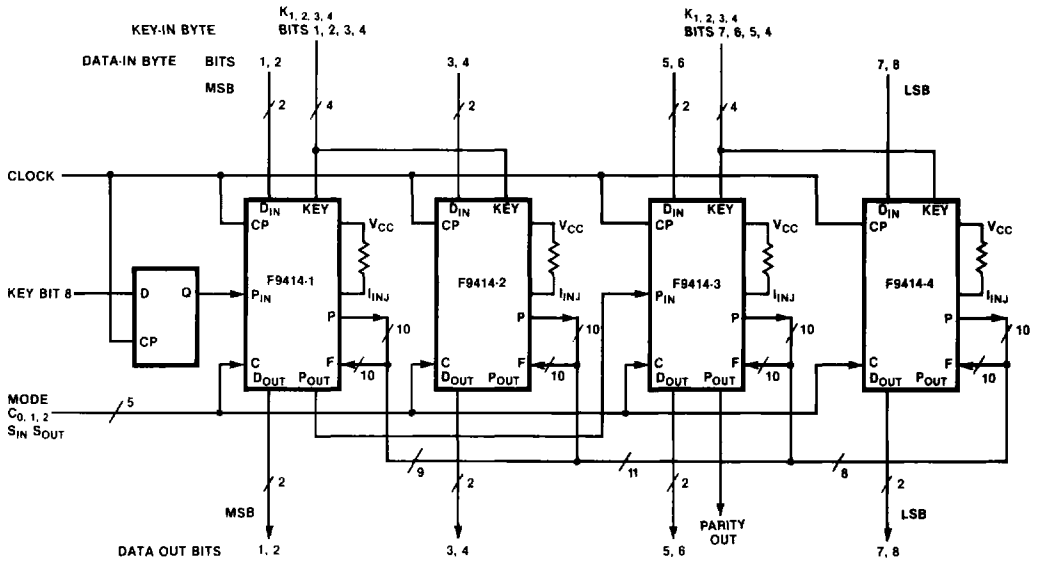
Functional Description

The set operates with a 56-bit key word to encipher or decipher a 64-bit data word that is stored in 8 bytes; 2 bits of each byte are distributed to each of the four chips (see figure 1). The key consists of 64 bits in 8 bytes; bit 8 of each byte is parity. Bits 1 through 4 go to both chip 1 and 2; bits 4 through 7 go to chips 3 and 4. The four chips together also store the 64-bit plaintext or ciphertext word. The chips have separate data inputs and outputs, so the block of data to be processed can be input as the previous block is being output. This overlap permits the processing of a 64-bit block in 24 clock pulses at a 5 MHz typical clock frequency. This results in data throughput of 13.3 MHz (75 ns) per bit, or 200 kHz (4.8 μs) per 64-bit word.

Table 1 F9414 Signal Descriptions

Mnemonic	Pin No.	Name	Description
F_1 - F_8	8, 7, 6, 5, 4, 3, 2, 1	Interconnect Lines	Input signals; interconnect with P_1-P_8 to implement the permutation function, P, of the algorithm.
P_1 - P_8	21 - 28	Interconnect Lines	Output signals; interconnect with F_1-F_8 to implement the permutation function, P, of the algorithm.
K_1 - K_4	36 - 39	Keyword	Input signal for 4 bits of the keyword.
D_{IN0}, D_{IN1}	12, 11	Data In	Data inputs for 2 bits of the data word.
S_{IN}	13	Select In	Input signal that selects the exclusive-OR function.
S_{OUT}	14	Select Out	Input signal that selects the output function.
D_{OUT0}, D_{OUT1}	16, 15	Data Out	Output lines for the data bits.
P_X, P_Y	17, 18	E-Bit Select	Output signal; E-bit selection for interconnection with F_X, F_Y.
F_X, F_Y	20, 19	E-Bit Select	Input signal; E-bit selection for interconnection with P_X, P_Y.
C_0, C_1, C_2	35, 34, 33	Control	Input signals used to control the F9414 in one of five modes.
P_{IN}	32	Parity In	Parity bit input signal
P_{OUT}	31	Parity Out	Parity bit output signal
CP	40	Clock	Input signal
V_{CC}	29	Power	+5 V ±5% power supply
I_{INJ}	9	Power	Injection current input
GND	10	Ground	0 V reference.

Figure 1 4-Chip Encryption Set



The key register is capable of hold, left shift (encipher), or right shift (decipher) operations, by one or two positions, as required by each of the 16 rounds of the algorithm (see figure 2). Each device also includes logic for the control of these registers during load and cipher operations. The 64-bit word by 4-bit ROMs in each device implement the S-boxes of the algorithm.

The major differences among the four devices are the masking of the ROM codes and the key bits that are selected as ROM addresses, according to the E-bit selection table of the algorithm.

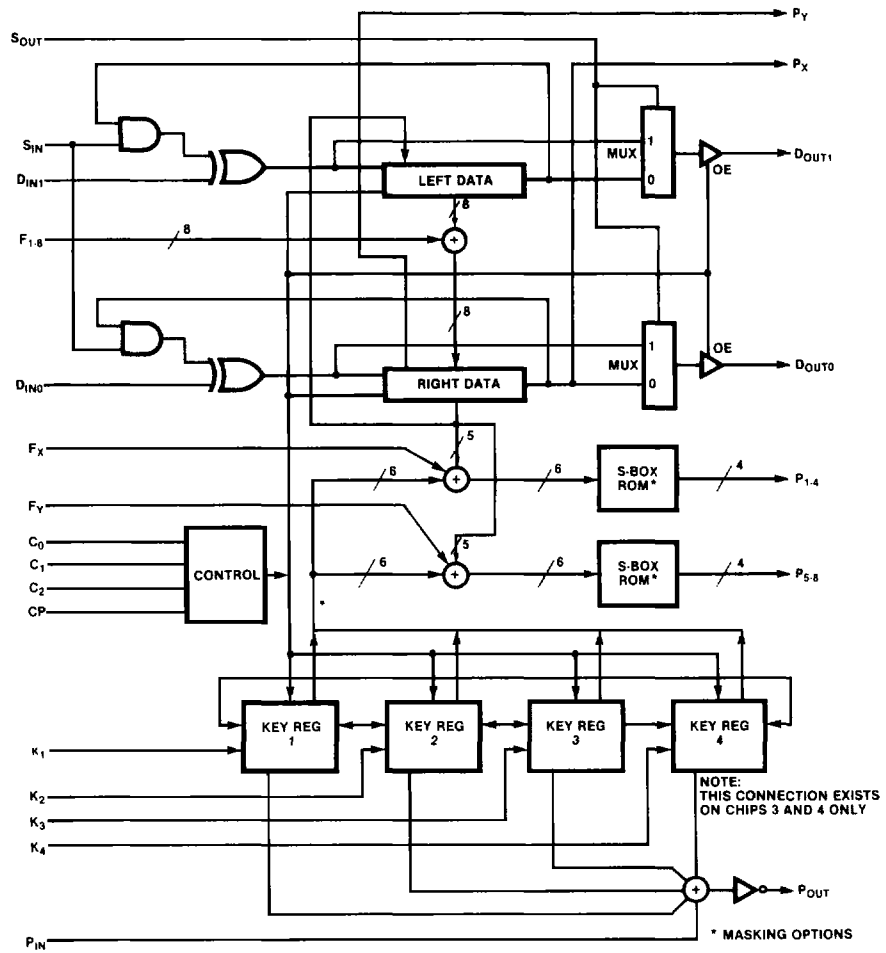
A set of eight output signals (P_{1-8}) and input signals (F_{1-8}) is interconnected between chips to implement the permutation function, P, of the algorithm. An additional set of outputs (P_X and P_Y) and inputs (F_X and F_Y) is used to interconnect the chips as required by columns 1 and 6 of the E bit-selection table.

Implementation of the Algorithm

Initial permutation is accomplished in the F9414 chip set by the manner in which the data is loaded. The D_{IN0} input of chip 1 loads bit 1 of each byte, D_{IN1} of chip 1 loads bit 2 of each byte, D_{IN0} of chip 2 loads bit 3 of each byte, etc. After eight clock cycles, the four registers receiving data bits 2, 4, 6, and 8 of each input byte comprise the L_0 block of 32 bits in permuted order within the four devices. The four registers receiving bits 1, 3, 5, and 7 of each byte hold the R_0 block. Therefore, each chip slice contains one byte each of the L_0 and R_0 blocks.

Further shifting of the bits and extracting outputs from the right end of each byte implements the inverse permutation, $1P^{-1}$. Each column of the inverse permutation may be found in a register byte, and the first 8 bits (40, 8, 48, etc.) required by row 1 of the inverse permutation table are at the output ends of the shift registers.

Figure 2 F9414 Block Diagram (One Unit)



The 28 key bits in the top half, C_0, of the key permutation function are duplicated in the key registers of F9414-1 and F9414-2, while key bits in the bottom half, D_0, occupy the registers of both the F9414-3 and F9414-4. In each device, key register 4 holds the last 4 bits of both halves of the key permutation function. Each of the 16 iterations involves a left rotation (encipher) or right rotation (decipher) of the key registers.

During the key shift schedule, chips 1 and 2 bypass the right half of key register 4, and chips 3 and 4 bypass the left. This results in the key alignment returning to its original position after a total of 28 shifts from the 16 alterations.

An internal 1-bit right realignment is required by a change from encipher to decipher, after the key has been entered. This, and the reverse (left realignment for decipher to encipher), are performed by the F9414 control logic, which must be stable prior to the loading of the last data byte. When clocked at the same time as a load-key code, the data registers all fill with logic ones.

The results of the exclusive-OR of the key bits and data words derived from R_0 in the calculation of f(R,K) are taken, 6 bits at a time, to address a set of eight 64 × 4 S ROMs (i.e., S boxes). Two S ROMs per chip, each with four output bits, provide the 32 bits that are then permuted per primitive function P, by chip-to-chip interconnection. The effective result of the interconnect is exclusive-ORed with the L_0 block and the entire algorithm is repeated 16 times.

The F9414 is structurally designed for high throughput. Since no I/O ports are used for both entering data and reading results, a potential bottleneck is avoided. The 64-bit data word is entered into the F9414 data registers 1 byte at a time at the D_0,D_1 inputs. The MSB of data goes to D_0 of the F9414-1. The result is output 1 byte at a time on the Q_0,Q_1 pins, MSB output first. Similarly, the keyword is entered 1 byte at a time at its own dedicated inputs (K_1-K_4). Table 2 shows the distribution of the keyword to the four F9414 devices.

Table 2 Keyword Distribution

Keyword	F9414-1 Key Reg.	F9414-2 Key Reg.	F9414-3 Key Reg.	F9414-4 Key Reg.
8 MSB	1	1		
7	2	2		
6	3	3		
5	4	4	4	4
4			3	3
3			2	2
2 LSB			1	1
1 Parity (Option)	P_{IN}			

The keyword is 56 bits long but, if desired, an optional parity bit can be included with each byte of key, making the keyword 64 bits long. Parity does not in any way affect the encryption or decryption, and is taken across the keyword register, not across the K_1-K_4 inputs. Parity across 1 byte of keyword is taken by passing the parity bit of the keyword through a delay flip-flop to P_{IN} of the F9414-1 or F9414-2, and through P_{OUT} of the F9414-1 or F9414-2 into P_{IN} of the F9414-3 or F9414-4. The final parity sum is available on P_{OUT} of the F9414-3 or F9414-4.

The functions of the F9414 (load key, load data, encryption/decryption, and wait) are controlled by the C_0-C_2 inputs. Data and key are clocked in and/or out on low-to-high clock transitions. Loading a key sets the data registers to all high.

The F9414 enables simultaneous input and output of data; i.e., the results of a DES cipher operation can be clocked out on the same low-to-high transition that loads the next word to be processed. Thus, a complete input and output cycle (LOAD/READ DATA) takes just eight clocks. Since the algorithm requires 16 clocks, an entire DES iteration can be accomplished in 24 clocks. At a typical clock frequency of 6 MHz, this translates into a 16 MHz bit rate, a very fast LSI implementation of the DES. This high throughput ensures that the F9414 set is capable of keeping pace with practically every application, and this speed is available over the full military temperature range.

Implementation of Cipher Feedback

In cipher feedback (see figure 3), the present 64-bit data input is exclusive-ORed with the output of the encryption unit, and the result of this operation is transmitted and also fed back into the encryption unit to perpetuate the feedback. At the receiver, the received 64-bit vector is first exclusive-ORed and then deciphered.

Figure 4 illustrates the cipher feedback (CFB) transmitter operation. A 64-bit buffer is necessary for storing the input word external to the F9414 and can be provided with two F9423 first-in first-out (FIFO) buffer memories. Both receiver and transmitter operate in the same mode and start with the same (arbitrary) initialization word in the buffer. If the initialization is not done, the first 64 bits of data at the receiver are erroneously deciphered.

To encrypt 1 byte of data, one iteration of the DES algorithm is performed on the contents of the buffer. Then the MSB output from the F9414 is exclusive-ORed with the data byte and the result is transmitted. Additionally, the result of the exclusive-ORing is shifted into the least significant position of the buffer, while all other bytes are shifted and the former MSB discarded. This causes all following encryptions to depend on the present transmission, providing greater security than when each encryption depends only on the present data byte.

At the receiver (see figure 5), the transmission is shifted into the least significant position of the buffer and one DES iteration is performed. Since the receiver has used the same data word as the transmitter, this generates the same exclusive-OR mask as was used at the transmitter. Therefore, exclusive-ORing the next received byte with the MSB of the F9414 output recovers the data byte.

The transmitter and receiver must be operating in synchronization in cipher feedback. If synchronization is lost or an erroneous bit received, 64 bits of data will be incorrectly deciphered.

Figure 3 Cipher Feedback Implementation

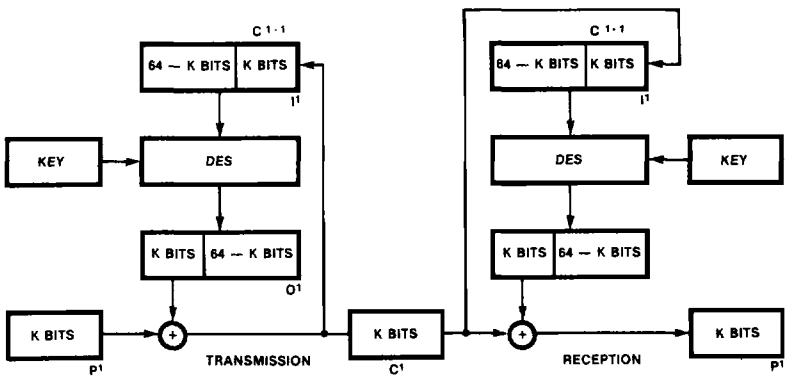
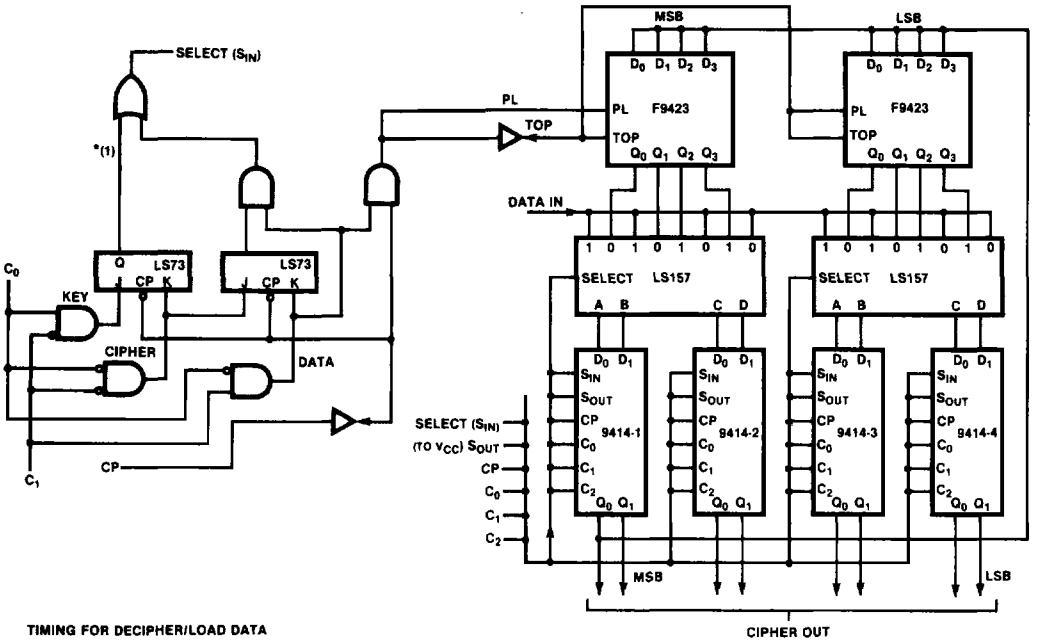
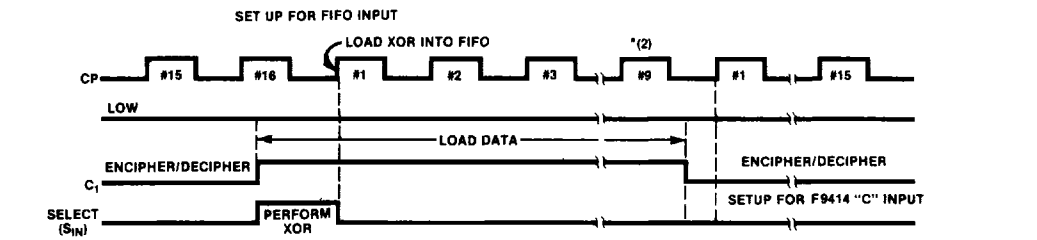


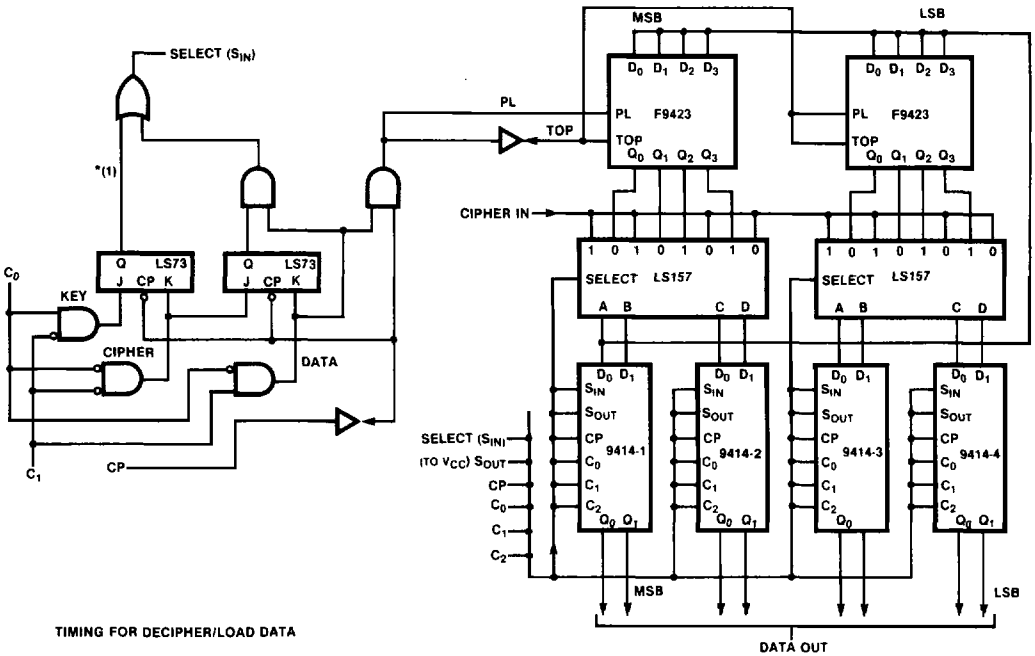
Figure 4 Cipher Feedback Transmitter



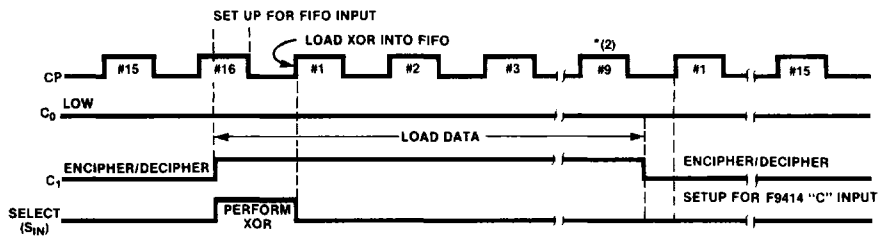


NOTES:
1. 8 byte initialization vector following LD KEY
2. 9 clock pulses required to complete load data operation

Figure 5 Cipher Feedback Receiver



TIMING FOR DECIPHER/LOAD DATA



NOTES:
1. 8 byte initialization vector following LD KEY
2. 9 clock pulses required to complete load data operation

Implementation of Cipher Block Chaining

Cipher block chaining (see figure 6) is similar to cipher feedback in that successive transmissions are made dependent on previous transmissions, thereby increasing the level of security. The cipher block chaining transmitter takes the present 64-bit input vector and exclusive-ORs it with the output of the encryption unit, then performs an encryption on the result. The result of the encryption is transmitted and also exclusive-ORed with the next 64-bit vector, continuing the chaining process. The receiver runs synchronously with the transmitter, and recovers the data by performing a decryption and then an exclusive-OR on the received 64 bits.

Receiver and transmitter must operate in different modes: encrypt and decrypt (see figures 7 and 8). No data buffering is necessary at the transmitter, but the receiver needs a 64-bit buffer to store the previous transmission. Both receiver and transmitter must start with the same initialization data or the first 64 bits of transmission will be incorrectly deciphered.

Internal exclusive-OR gates on the F9414 make implementation of the cipher block chaining transmitter especially simple. When S_{IN} is high, the exclusive-OR of the D inputs and Q outputs is input to the F9414 register. Since the F9414 can input and output simultaneously, the input data and the F9414 output are exclusive-ORed while the result of the DES iteration is being clocked out at the Q outputs. Therefore, no additional packages are required.

6

Figure 6 Cipher Block Chaining Mode with Terminal Block Padding

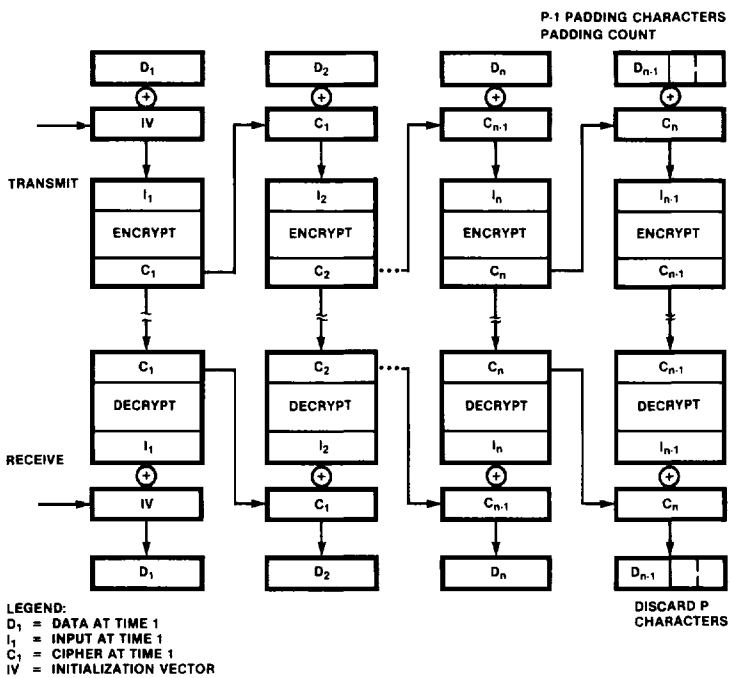
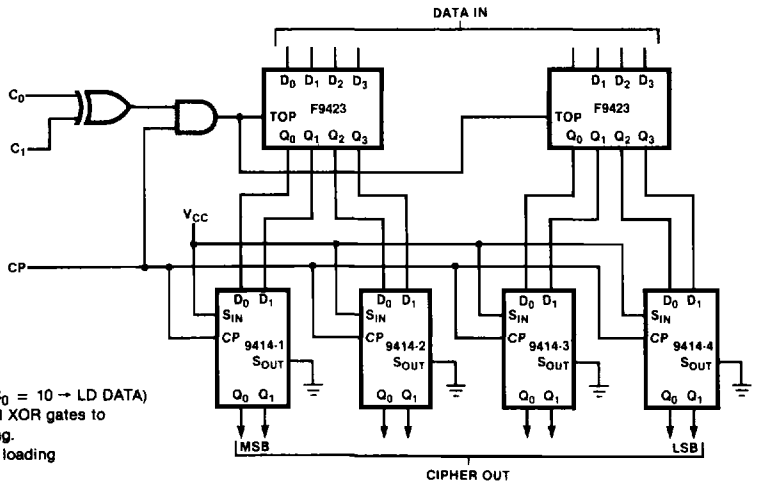
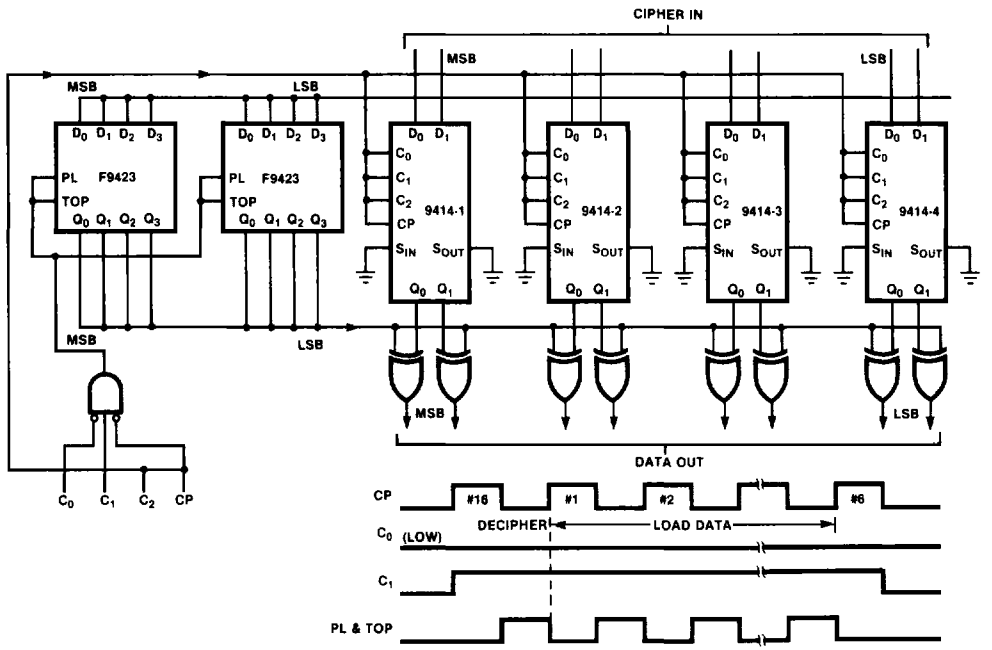


Figure 7 Cipher Block Chaining Transmitter



NOTES:
1. A high on S_{IN} (C_1 C_0 = 10 → LD DATA) enables the internal XOR gates to perform the chaining.
2. Hold S_{IN} low while loading initialization vector.

Figure 8 Cipher Block Chaining Receiver



Timing Characteristics

Signal timing diagrams for the data encryption set are shown in figures 9 through 11, and the timing characteristics are provided in table 3. The ac characteristics are: V_{CC} = 5V ±5%; T_A = 0°C to 70°C; C_L = 15 pF; and I_{INJ} = 85 to 125 mA.

Table 3 Timing Characteristics

Symbol	Parameter	Limits			Units	Comments
		Min	Typ	Max		
T_P	Prop. Delay, CP to P_{1-8}			155	ns	
T_P	Prop. Delay, CP to P_X, P_Y			110	ns	
T_P	Prop. Delay, CP to D_{OUT}			120	ns	S_{OUT} Low
T_P	Prop. Delay, CP to D_{OUT}		132	—	ns	S_{IN}, S_{OUT}, High
T_P	Prop. Delay, CP to P_{OUT} (9414-1, -2)			130	ns	C_{210} = XLH
T_P	Prop. Delay, CP to P_{OUT} (9414-3, -4)			145	ns	C_{210} = XLH
T_P	Prop. Delay, S_{IN} to D_{OUT}		75	—	ns	S_{OUT} High
T_P	Prop. Delay, S_{OUT} to D_{OUT}			85	ns	
T_P	Prop. Delay, D_{IN} to D_{OUT}		55	—	ns	S_{IN}, S_{OUT} High
T_P	Prop. Delay, C_{210} to D_{OUT}			105	ns	
T_P	Prop. Delay, P_{IN} to P_{OUT}			60	ns	
T_P	Prop. Delay, F_X, F_Y to P_{1-8}			100	ns	
T_S	Set-up Time, F_{1-8} to CP	50			ns	
T_S	Set-up Time, D_{IN} to CP	45			ns	C_{210} = XHL
T_S	Set-up Time, S_{IN} to CP	70			ns	C_{210} = XHL
T_S	Set-up Time, C_{210} to CP	110			ns	
T_S	Set-up Time, K_{1-4} to CP	50			ns	C_{210} = XLH
T_H	Hold Time, CP to F_{1-8}	5			ns	
T_H	Hold Time, CP to D_{IN}	0			ns	C_{210} = XHL
T_H	Hold Time, CP to S_{IN}	0			ns	C_{210} = XHL
T_H	Hold Time, CP to C_{210}	0			ns	
T_H	Hold Time, CP to K_{1-4}	10			ns	C_{210} = XLH
T_{PWH}	CP Pulse Width High	50			ns	

Figure 9 Load Key Timing Diagram

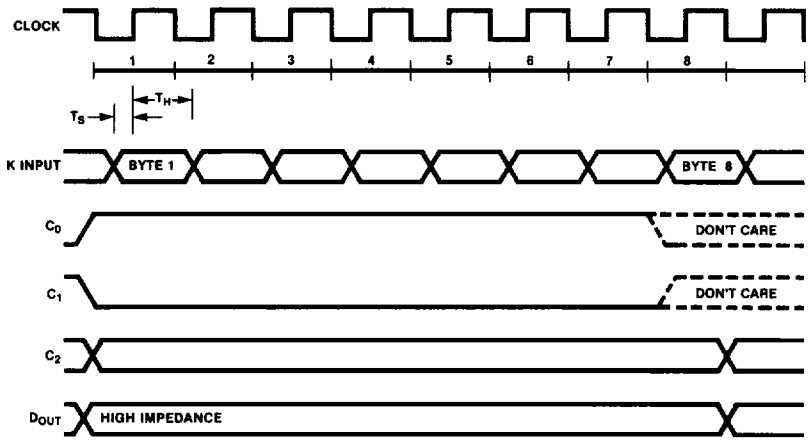


Figure 10 Load/Read Data Timing Diagram

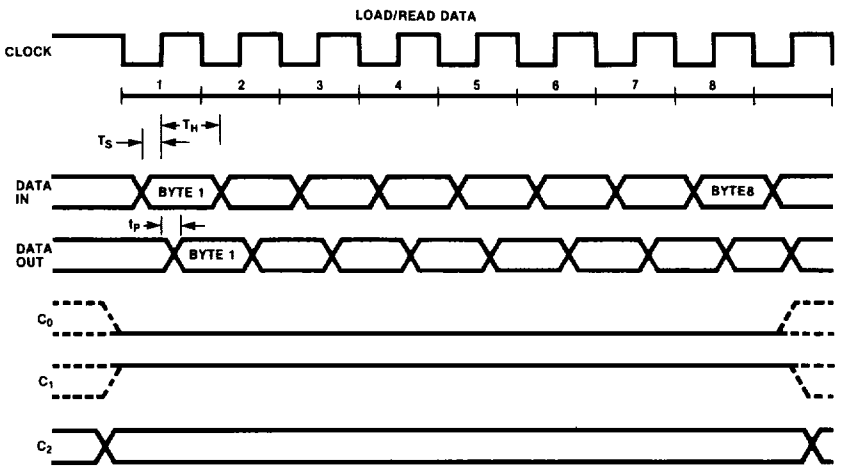
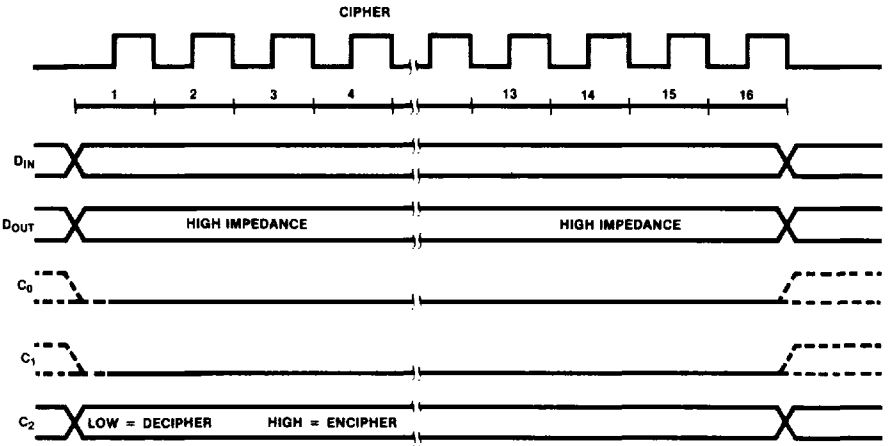


Figure 11 Cipher Timing Diagram



6

DC Characteristics

The dc characteristics of the data encryption set are provided in table 4. The dc characteristics are specified over operating temperature range, unless otherwise noted:

0 °C to 70 °C; $I_{INJ(min.)}$ = 85 mA; $I_{INJ(max.)}$ = 125 mA;
$V_{CC(min.)}$ = 4.75 V; $V_{CC(max.)}$ = 5.25 V.
Typical limits are at V_{CC} = 5.0 V, T_A = 25 °C.

Absolute Maximum Ratings

These are stress ratings only, and functional operation at these ratings, or under any conditions above those indicated in this data sheet, is not implied. Exposure to the absolute maximum rating conditions for extended periods of time may affect device reliability, and exposure to stresses greater than those listed may cause permanent damage to the device.

Storage Temperature	−65 °, +150 °C
Ambient Temperature under Bias	−55 °, +125 °C
V_{CC} Pin Potential to Ground Pin	−0.5, +6.0 V
Input Voltage (DC)	−0.5, +5.5 V
Input Current (DC)	−20, +5 mA
Output Voltage (Output High)	−0.5, +5.5 V
Output Current (DC) (Output Low)	+20 mA
Injector Current (I_{INJ})	+200 mA
Injector Voltage (V_{INJ})	−0.5, +1.8 V

Control Codes

Table 5 provides the control codes for the data encryption set.

Table 5 Control Codes

C_2 C_1 C_0		Clock Cycles
0 0 0	DECIPHER	16
1 0 0	ENCIPHER	16
X 0 1	LOAD KEY	8
X 1 0	LOAD DATA/OUTPUT DATA	8
X 1 1	WAIT	X

Table 4 DC Characteristics

Symbol	Parameter	Limits			Units	Test Conditions I_{INJ} = 100 mA
		Min	Typ	Max		
V_{IH}	Input High Voltage	2.0			V	Guaranteed Input High Voltage
V_{IL}	Input Low Voltage			0.8	V	Guaranteed Input Low Voltage
V_{CD}	Input Clamp Diode Voltage		−0.9	−1.5	V	V_{CC} = Min, I_{IN} = −18 mA
V_{OH}	Output High Voltage	2.4	3.4		V	V_{CC} = Min I_{OH} = −1.0 mA (D_{OUT}) I_{OH} = −400 μA (Other Outputs)
V_{OL}	Output Low Voltage		0.25	0.5	V	V_{CC} = Min, I_{OL} = 8.0 mA
	Input High Current, All Except CP		1.0	20	μA	V_{CC} = Max, V_{IN} = 2.7 V
I_{IH}	Input High Current, CP		1.0	40	μA	V_{CC} = Max, V_{IN} = 2.7 V
	Input High Current, All Inputs			1.0	mA	V_{CC} = Max, V_{IN} = 5.5 V
I_{IL}	Input Low Current, All Except CP Input Low Current, CP		−0.21 −0.42	−0.36 −0.72	mA	V_{CC} = Max, V_{IN} = 0.4 V
I_{OZH} I_{OZL}	Off State (High Impedance) Output Current, D_{OUT}			100 −100	μA μA	V_{CC} = Max, V_{OUT} = 2.4 V V_{CC} = Max, V_{OUT} = 0.5 V
I_{OS}	Output Short Circuit Current	−15		−100	mA	V_{CC} = Max, V_{OUT} = 0
I_{CC}	Supply Current		150	220	mA	V_{CC} = Max
V_{INJ}	Injector Voltage	1.0	1.3	1.5	V	I_{INJ} = 100 mA, V_{CC} = 5.0 V

Device Interconnection

Table 6 gives the interconnection information for the four-chip set.

Table 6 Device Interconnection

nF (f) to nP (p)*							
1F1 to 2P8		2F1 to 1P1		3F1 to 1P2		4F1 to 3P3	
1F2	1P7	2F2	2P7	3F2	1P8	4F2	2P5
1F3	3P4	2F3	3P7	3F3	3P8	4F3	4P6
1F4	3P5	2F4	4P2	3F4	2P6	4F4	1P6
1F5	4P5	2F5	1P5	3F5	4P8	4F5	3P6
1F6	2P4	2F6	3P2	3F6	4P3	4F6	2P3
1F7	4P4	2F7	4P7	3F7	1P3	4F7	1P4
1F8	3P1	2F8	2P2	3F8	2P1	4F8	4P1
1FX	4PX	2FX	1PX	3FX	2PX	4FX	3PX
1FY	2PY	2FY	3PY	3FY	4PY	4FY	1PY

*n indicates chip option
f and p indicate specific member

Ordering Information

Part Number	Package	Temperature Range
F9414 ST DC	Ceramic DIP	0°C to 70°C

Export Control

Cryptographic devices and technical data regarding them are subject to Federal Government export controls as specified in Title 22, Code Of Federal Regulations, Parts 121 through 128.