Features

- **Bus-compatible with the ARM7TDMI™ Core**
- **16-clock Cycle Encryption/Decryption Process**
- **On Request: 8, 4, 2, 1 Clock Cycle Encryption/Decryption Process**
- **One Key Register**
- **Triple Data Encryption Capability**
- **Fully Scan Testable up to 100%**

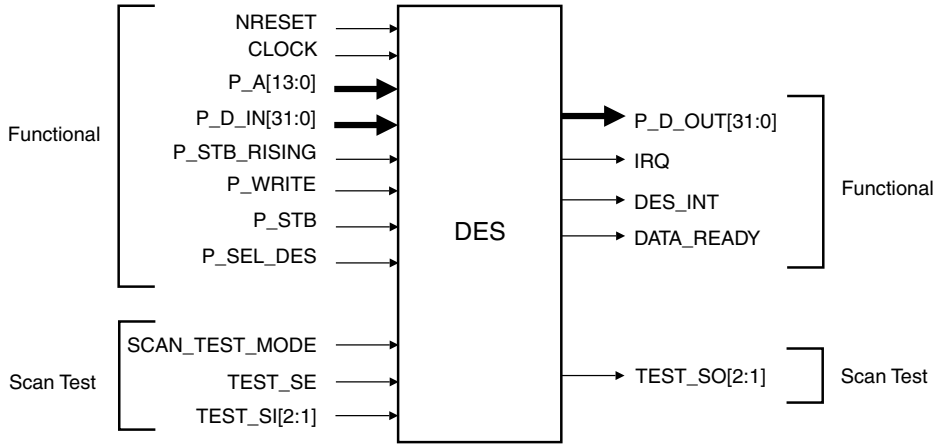
Description

The Data Encryption Standard (DES) is compliant with the American FIPS (Federal Information Processing Standard) PUB 46-2 specification. The data and key are stored in 2 x 32-bit registers. The key register is write-only. An external application is required to generate the key. Suitable precautions should be taken to protect the security of the key.

As soon as data and key are configured, the encryption/decryption process may be started. 16 clock cycles later, the interrupt is set (if enabled) and the encrypted/decrypted data is ready to be read out on 2 x 32-bit registers. The DATA_READY signal indicates that the process is finished and is cleared when the user reads out the data.

The DES peripheral is compatible with the APB bus of the ARM7TDMI core. It may also be used with any 32-bit microcontroller.

Figure 1. DES Pin Configuration



32-bit Embedded Core Peripheral

Data Encryption Standard (DES)

Rev. 1351D–10/01

Table 1. DES Pin Description

Name	Function	Direction	Comments
Functional			
NRESET	System reset	Input	Asynchronous, active low
CLOCK	System clock	Input	Everything is clocked on this signal except the configuration registers
P_A[13:0]	Software user interface address bus	Input	The address includes the 2 LSBs [1:0], but the macrocell does not take into account these bits (left unconnected)
P_D_IN[31:0]	Software user interface data bus	Input	Data from host (bridge)
P_D_OUT[31:0]	Software user interface data bus.	Output	Data to host (bridge)
P_WRITE	Transfer enable (from host to peripheral)	Input	When high, indicates that the host processor is writing to a register or executing a command
P_SEL_DES	Peripheral selection	Input	Active high
P_STB_RISING	Peripheral strobe	Input	Clock for all DFFs controlling configuration registers
P_STB	Peripheral strobe	Input	When high, indicates that data and address buses are stable
DES_INT	Interrupt	Output	Active high
DATA_READY	Flag	Output	Set when encryption/decryption process is finished Cleared when data is read out
Scan Test			
SCAN_TEST_MODE	Scan test mode	Input	Must be tied high during scan test, must be tied low in functional mode
TEST_SE	Test scan shift enable	Input	Scan shift enabled when tied high
TEST_SI[2:1]	Test scan input	Input	Entry of scan chain
TEST_SO[2:1]	Test scan output	Output	Output of scan chain

Note: One scan chain uses the clock P_STB_RISING while the other uses CLOCK.

Scan Test Configuration

The coverage is maximum if all non-scan inputs can be controlled and all non-scan outputs can be observed. In order to acheive this, the ATPG vectors must be generated on the entire circuit (top level) which includes the DES or all DES I/Os must have a top level access and ATPG vectors must be applied to these pins.

Figure 2. DES Timer Block Diagram

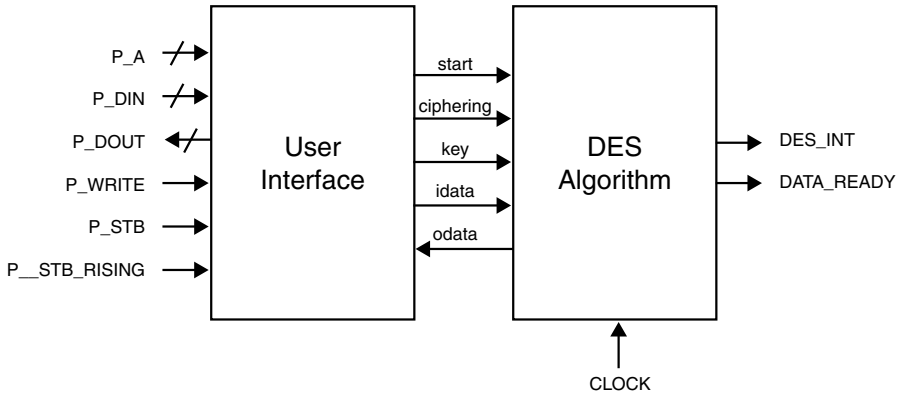
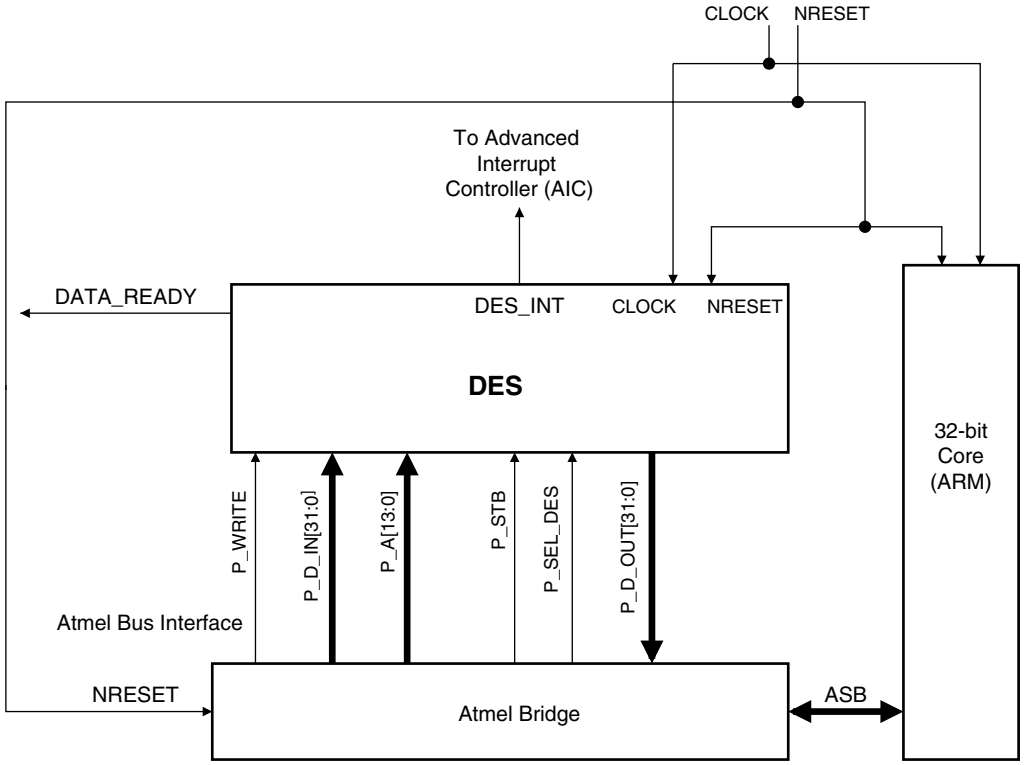
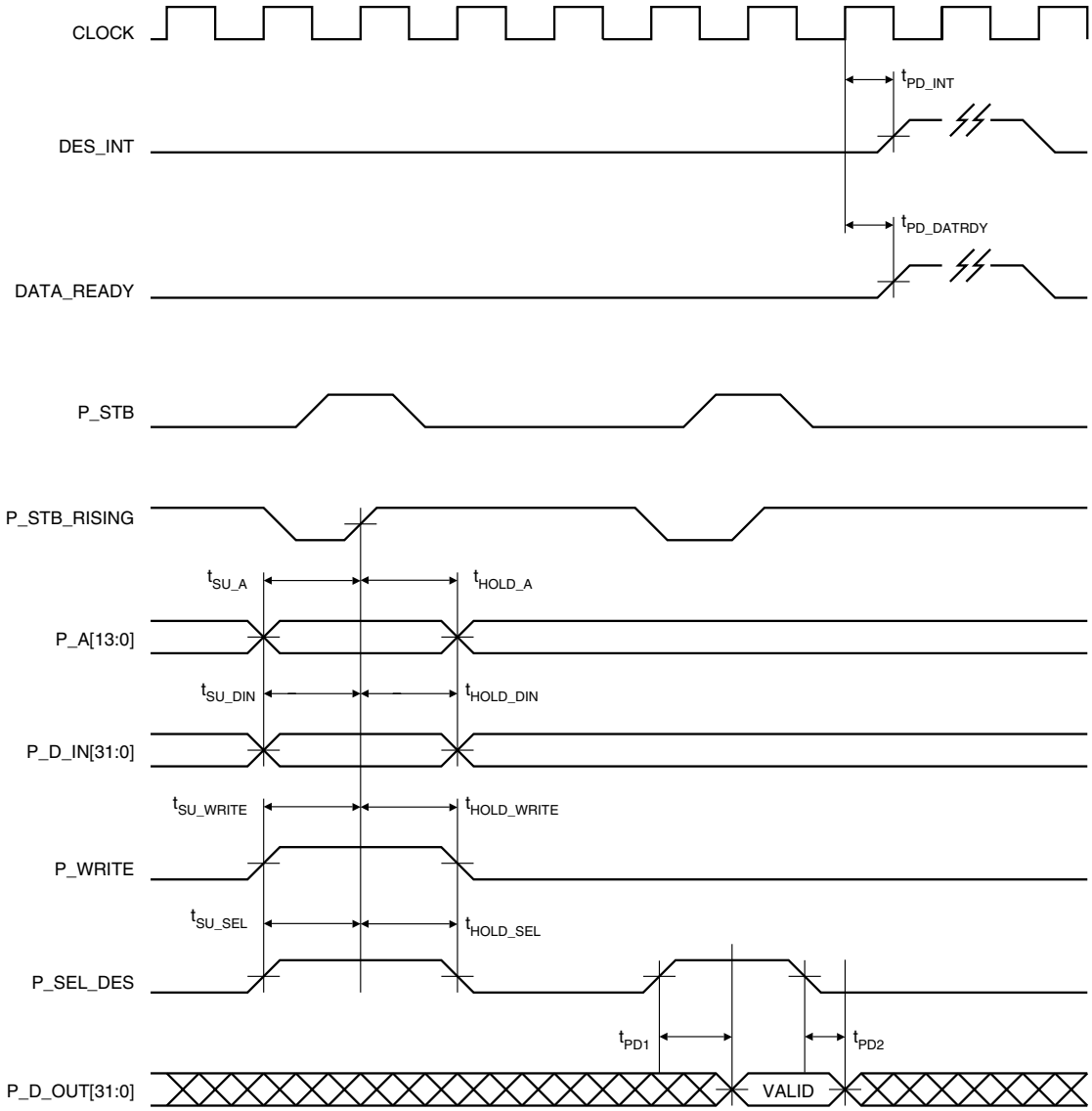


Figure 3. Connecting the DES to an ARM®-based Microcontroller



Timing Diagram

Figure 4. DES Timing Diagram



DES Software User Interface

Table 2. DES Memory Map[1, 2]

Offset	Register	Name	Access	Reset State
0x0000	Control Register	DES_CR	Write-only	–
0x0004	Mode Register	DES_MR	Read/Write	0
0x0008	Reserved	–	–	–
0x000C	Reserved	–	–	–
0x0010	Interrupt Enable Register	DES_IER	Write-only	–
0x0014	Interrupt Disable Register	DES_IDR	Write-only	–
0x0018	Interrupt Mask Register	DES_IMR	Read-only	0
0x001C	Interrupt Status Register	DES_ISR	Read-only	0
0x0020	MSB Key	DES_MKEY	Write-only	0
0x0024	LSB Key	DES_LKEY	Write-only	0
0x0028	Reserved	–	–	–
0x002C	Reserved	–	–	–
0x0030	MSB Input Data	DES_MIDATA	Read/Write	0
0x0034	LSB Input Data	DES_LIDATA	Read/Write	0
0x0038	MSB Output Data	DES_MODATA	Read-only	0
0x003C	LSB Output Data	DES_LODATA	Read-only	0

Notes: 1. The address includes the 2 LSBs [1:0], but the macrocell does not take these bits into account (left unconnected). Therefore, loading 0x0001, 0x0002 or 0x0003 on P_A[13:0] addresses the Control Register.
2. If the user selects an address which is not defined in the above table, the value of P_D_OUT[31:0] is 0x00000000.

DES Registers

In the following register descriptions, all undefined bits (“–”) read “0”.

DES Control Register

Name: DES_CR

Access Type: Write-only

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	–
7	6	5	4	3	2	1	0
–	–	–	–	–	–	–	START

- **START: Starts processing**

0 = No effect

1 = Starts encryption/decryption process

DES Mode Register

Name: DES_MR

Access Type: Read/Write

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	–
7	6	5	4	3	2	1	0
–	–	–	–	–	–	–	CIPHER

- **CIPHER: Processing mode**

0 = Decrypts data

1 = Encrypts data

DES Interrupt Enable Register

Name: DES_IER

Access Type: Write-only

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	–
7	6	5	4	3	2	1	0
–	–	–	–	–	–	–	DATRDY

- **DATRDY: Enable DATRDY Interrupt**

0 = No effect

1 = Enables DATRDY interrupt

DES Interrupt Disable Register

Name: DES_IDR

Access Type: Write-only

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	–
7	6	5	4	3	2	1	0
–	–	–	–	–	–	–	DATRDY

- **DATRDY: Disable DATRDY Interrupt**

0 = No effect

1 = Disables DATRDY interrupt

DES Interrupt Mask Register

Name: DES_IMR

Access Type: Read-only

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	–
7	6	5	4	3	2	1	0
–	–	–	–	–	–	–	DATRDY

- **DATRDY: Enable/disable status of DATRDY Interrupt**

0 = DATRDY interrupt is disabled

1 = DATRDY interrupt is enabled

DES Interrupt Status Register

Name: DES_ISR

Access Type: Read-only

31	30	29	28	27	26	25	24
–	–	–	–	–	–	–	–
23	22	21	20	19	18	17	16
–	–	–	–	–	–	–	–
15	14	13	12	11	10	9	8
–	–	–	–	–	–	–	–
7	6	5	4	3	2	1	0
–	–	–	–	–	–	–	DATRDY

- **DATRDY: Data Ready**

0 = Output data is not valid

1 = Encryption or decryption process is completed

DES MSB KEY

Register Name: DES_MKEY

Access Type: Write-only

31	30	29	28	27	26	25	24
MKEY							
23	22	21	20	19	18	17	16
MKEY							
15	14	13	12	11	10	9	8
MKEY							
7	6	5	4	3	2	1	0
MKEY							

MKEY contains the MSB of the KEY. It is write-only to prevent the KEY from being read by another application.

DES LSB KEY

Register Name: DES_LKEY

Access Type: Write-only

31	30	29	28	27	26	25	24
LKEY							
23	22	21	20	19	18	17	16
LKEY							
15	14	13	12	11	10	9	8
LKEY							
7	6	5	4	3	2	1	0
LKEY							

LKEY contains the LSB of the KEY. It is write-only to prevent the KEY from being read by another application.

DES MSB Input Data

Register Name: DES_MIDATA

Access Type: Read/Write

31	30	29	28	27	26	25	24
MIDATA							
23	22	21	20	19	18	17	16
MIDATA							
15	14	13	12	11	10	9	8
MIDATA							
7	6	5	4	3	2	1	0
MIDATA							

MIDATA contains the MSB of the data to be encrypted/decrypted.

DES LSB Input Data

Register Name: DES_LIDATA

Access Type: Read/Write

31	30	29	28	27	26	25	24
LIDATA							
23	22	21	20	19	18	17	16
LIDATA							
15	14	13	12	11	10	9	8
LIDATA							
7	6	5	4	3	2	1	0
LIDATA							

LIDATA contains the LSB of the data to be encrypted/decrypted.

DES MSB Output Data

Register Name: DES_MODATA

Access Type: Read-only

31	30	29	28	27	26	25	24
MODATA							
23	22	21	20	19	18	17	16
MODATA							
15	14	13	12	11	10	9	8
MODATA							
7	6	5	4	3	2	1	0
MODATA							

MODATA contains the MSB of the data which has been encrypted/decrypted

DES LSB Output Data

Register Name: DES_LODATA

Access Type: Read-only

31	30	29	28	27	26	25	24
LODATA							
23	22	21	20	19	18	17	16
LODATA							
15	14	13	12	11	10	9	8
LODATA							
7	6	5	4	3	2	1	0
LODATA							

LODATA contains the LSB of the data which has been encrypted/decrypted

Atmel Headquarters

Corporate Headquarters
2325 Orchard Parkway
San Jose, CA 95131
TEL (408) 441-0311
FAX (408) 487-2600

Europe
Atmel SarL
Route des Arsenaux 41
Casa Postale 80
CH-1705 Fribourg
Switzerland
TEL (41) 26-426-5555
FAX (41) 26-426-5500

Asia
Atmel Asia, Ltd.
Room 1219
Chinachem Golden Plaza
77 Mody Road Tsimhatsui
East Kowloon
Hong Kong
TEL (852) 2721-9778
FAX (852) 2722-1369

Japan
Atmel Japan K.K.
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
Japan
TEL (81) 3-3523-3551
FAX (81) 3-3523-7581

Atmel Product Operations

Atmel Colorado Springs
1150 E. Cheyenne Mtn. Blvd.
Colorado Springs, CO 80906
TEL (719) 576-3300
FAX (719) 540-1759

Atmel Grenoble
Avenue de Rochepleine
BP 123
38521 Saint-Egreve Cedex, France
TEL (33) 4-7658-3000
FAX (33) 4-7658-3480

Atmel Heilbronn
Theresienstrasse 2
POB 3535
D-74025 Heilbronn, Germany
TEL (49) 71 31 67 25 94
FAX (49) 71 31 67 24 23

Atmel Nantes
La Chantrerie
BP 70602
44306 Nantes Cedex 3, France
TEL (33) 0 2 40 18 18 18
FAX (33) 0 2 40 18 19 60

Atmel Rousset
Zone Industrielle
13106 Rousset Cedex, France
TEL (33) 4-4253-6000
FAX (33) 4-4253-6001

Atmel Smart Card ICs
Scottish Enterprise Technology Park
East Kilbride, Scotland G75 0QR
TEL (44) 1355-357-000
FAX (44) 1355-242-743

e-mail
literature@atmel.com

Web Site
http://www.atmel.com

1351D–10/01/0M