# DES
## IP Core
IPC-DES

### FEATURES

- FIPS 46-3 Standard Compliant
- Encryption/Decryption performed in 17 cycles
- ECB, CBC, OFB Modes
- 56 bits of security
- Small gate count
- For use in FPGA or ASIC designs

### LICENSED IP PACKAGE INCLUDES

- Verilog Source
- Complete Test Environment
- AHB Bus Functional Model
- C-Sample Code

### DESCRIPTION

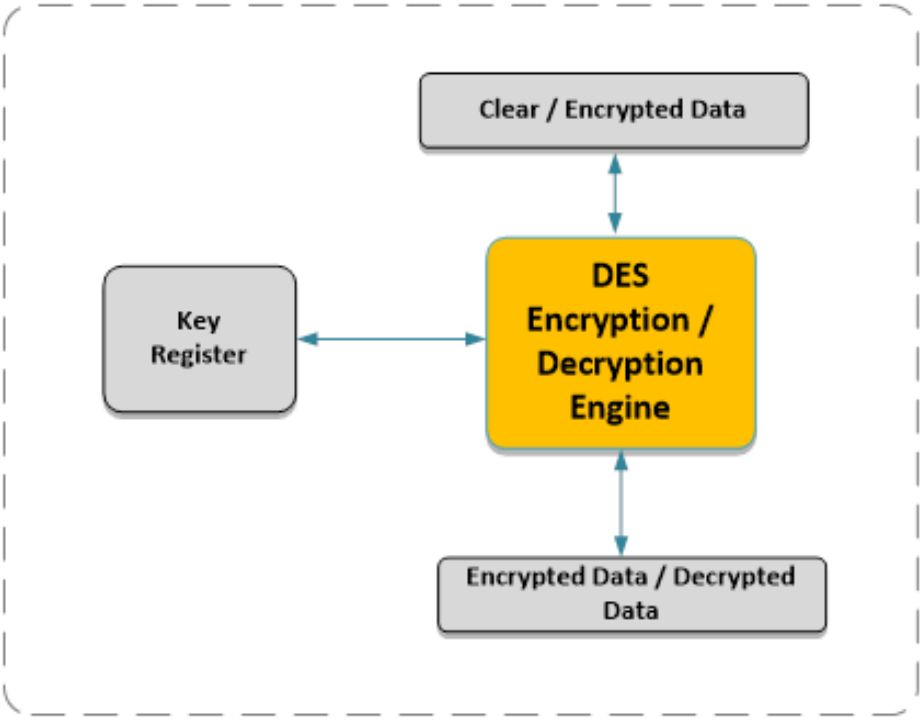
The Data Encryption Standard (DES) IP Core is a complete implementation of the Data Encryption Standard (DES) documented in the U.S. Government publication FIPS 46-3.

The DES core is a block cipher, working on 64 bits of data at a time. The DES core uses a single 64 bit key of which only 56 bits are used. Encoding and decoding operations are performed in 16 clocks per block, in Electronic Codebook (ECB), Cipher Block Chaining (CBC), and Output Feedback (OFB) mode.

The DES core is fully synchronous using only one clock signal and can be implemented in both FPGAs and ASICs. The DES IP Core is delivered as Verilog RTL Source code.

This DES IP Core version is implemented to minimize the gate count and FPGA resources. The design does not use any memories such as SRAM.

### GENERAL USE



**You may also be interested in:**

## AMBA® Subsystems

- Low Power Subsystem (simple AHB system)
- Low Power / Performance Subsystem (includes AHB Multi-matrix Fabric)
- Custom Performance Subsystem (includes AXI Multi-layer Fabric)

# IP Cores

### Infrastructure Cores

AHB Multi-Matrix Fabric
AHB/AHBLite Channel
AHB Arbiter
AXI Multi-Layer Fabric
AXI to AHBLite Bridge
AXI to APB Bridge
AHB to ABP Bridge
APB Channel

### AXI Cores

AXI Multi-Layer Fabric
AXI to AHBLite Bridge
AXI to APB Bridge
AXI External Bus Interface
(Memory/Flash Controller)
AXI Internal Memory Controller
AXI QSPI with Execute in Place (XIP)

### AHB Cores

AHB Channel
AHB Multi-Matrix Fabric
AHB to ABP Bridge
AHB Arbiter
AHB QSPI with Execute in Place (XIP)
AHB External Bus Interface
AHB Internal SRAM Controller
AHB Interrupt Controller
AHB DMA Controller
AHB DMA 4 Channel Controller
AHB TFT LCD Controller
AHB DES/TDES Encryption/Decryption

AHB Serial Flash Controller
Octal, Quad, Dual and Single Modes

Serial to AHB Bridge
SPI slave to AHB Master
Monitor/Control

### APB Cores

APB Channel
APB Quad SPI Controller
APB General Purpose IO
APB Timer
APB UART
APB I2C (Master and Slave)
APB SPI
APB Watchdog Timer
APB Pulse Width Modulator
APB Real Time Clock

### General

DES – Digital Encryption Standard
Triple DES (Low Gates)
Triple DES (pipelined)
ADC Interface (semi-custom)
Mixed-Signal Interfaces (semi-custom)
Power Management Unit (semi-custom)

AES Encryption Core

**For more information contact**

**sales@socsolutions.com**