# OL_DES
# DES Cryptoprocessor
**Rev 1.4**

## General Description

This core is a fully compliant implementation of the DES encryption algorithm. Both encryption and decryption are supported. ECB, CBC and triple DES versions are available. Simple, fully synchronous design with low gate count.

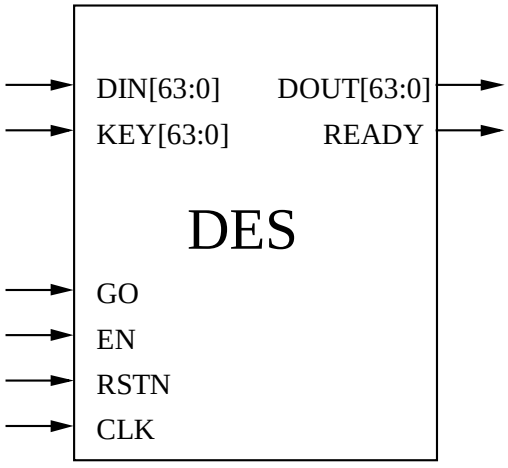
## Applications

- Electronic financial transactions.
- Secure communications.
- Secure video surveillance systems.
- Encrypted data storage.

## Features

- NIST certified 56 bit DES implementation.
- Both encryption and decryption supported.
- Encryption and decryption performed in sixteen clock cycles.
- No dead cycles for Key loading or mode switching.
- Suitable for Electronic Codebook (ECB), Cipher Block Chaining (CBC), CFB and OFB implementations.
- Triple DES version available.
- High clock speed and low gate count achieved.
- Sustained bit rate is 4x clock speed.
- Suitable for data security applications.
- Fully synchronous design.
- Available as fully functional and synthesizable VHDL or Verilog soft-core.

## Symbol



# Pin Description

| Name | Type | Description |
|---|---|---|
| RSTN | Input | Core reset, active low. |
| CLK | Input | Core clock signal. |
| EN | Input | Synchronous enable signal. When LOW the core ignores all its inputs and all its outputs must be ignored |
| GO | Input | Activates encryption or decryption. |
| E_D | Input | Selects encryption or decryption. |
| KEY[63:0] | Input | Input key. |
| DIN[63:0] | Output | Input data. |
| DOUT[63:0] | Output | Output data. |
| READY | Output | Output data valid. |

## General Description

The X_DES core is a fully compliant hardware implementation of the DES algorithm, suitable for a variety of applications.

The DES algorithm is the result of a joint effort of IBM and the NSA and was adopted as a federal standard in November 1974. It is a block cipher that encrypts and decrypts data in 64 bit blocks using a 56 bit key. The block diagram is shown in Figure 1.

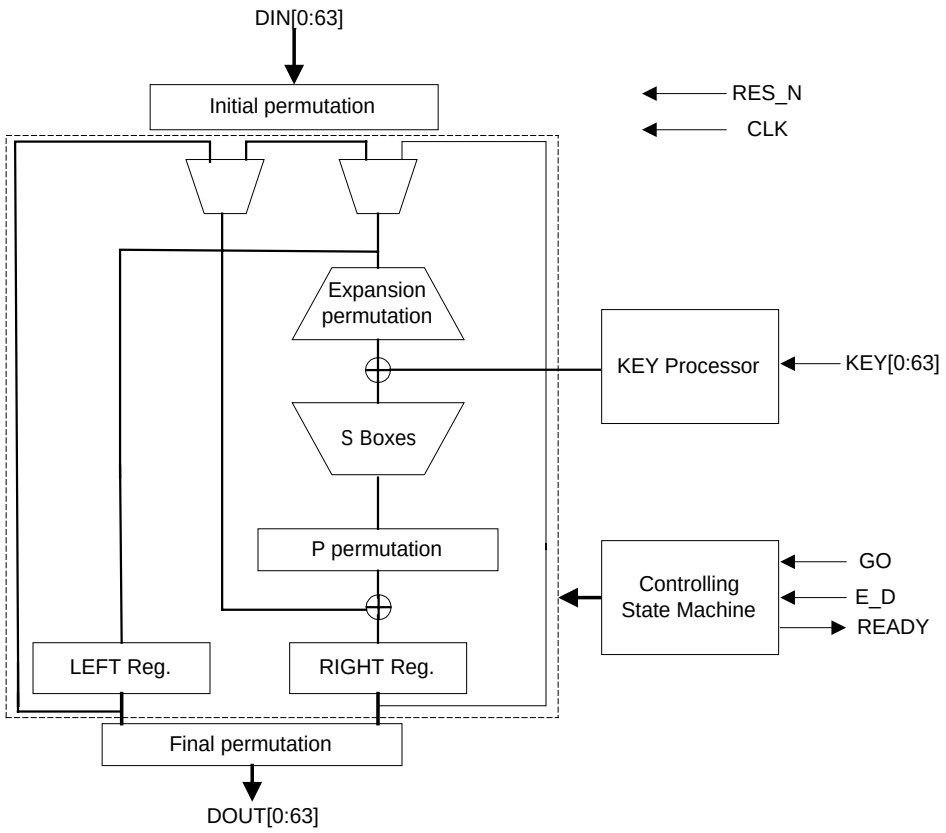



**Figure 1** Block Diagram for the DES Engine

After an initial permutation, the input data is split into two 32 bit words, left and right. This is followed by 16 rounds of identical operations.

The right word is processed with an expansion permutation and XORed with the processed key, followed by the S boxes substitution. The output of the S boxes is permuted and then XORed with the left word.

The result is used to update the right word register at the end of each round. Also, the previous right word is stored in the left word register. The processed key changes at each round as well, thanks to shifts and permutation operations.

At the end of the 16 rounds the left and right words are reassembled together and passed through the inverse of the initial permutation.

## Functional Description

Encryption or decryption is selected by the E_D signal. If this signal is high, the core performs encryption, otherwise decryption is performed.

Rising input on the GO port triggers the beginning of a cryptographic operation on the data DIN using the KEY as key.

Only 56 of the 64 bits of the KEY input port are considered by the core, according to the DES algorithm. Every eighth bit is ignored from the KEY input.

After 16 clock cycles, the READY output indicates that the output value DOUT is valid. The core is immediately ready for another operation so that a throughput of 64 bits every 16 cycles can be sustained. The timing is shown in Figure 2.

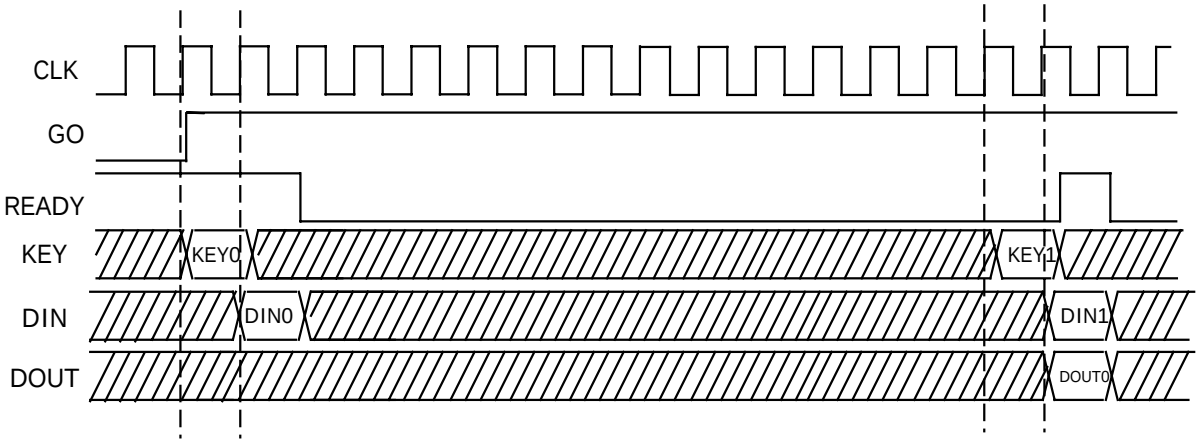



**Figure 2 Timing diagram for READY output.**

The core ignores the DIN and KEY inputs, except when highlighted in the timing diagram. This diagram shows that the core has no dead cycles and that it is possible to change the key as well as the input data, every 16-clock cycles as shown in Figure 3.

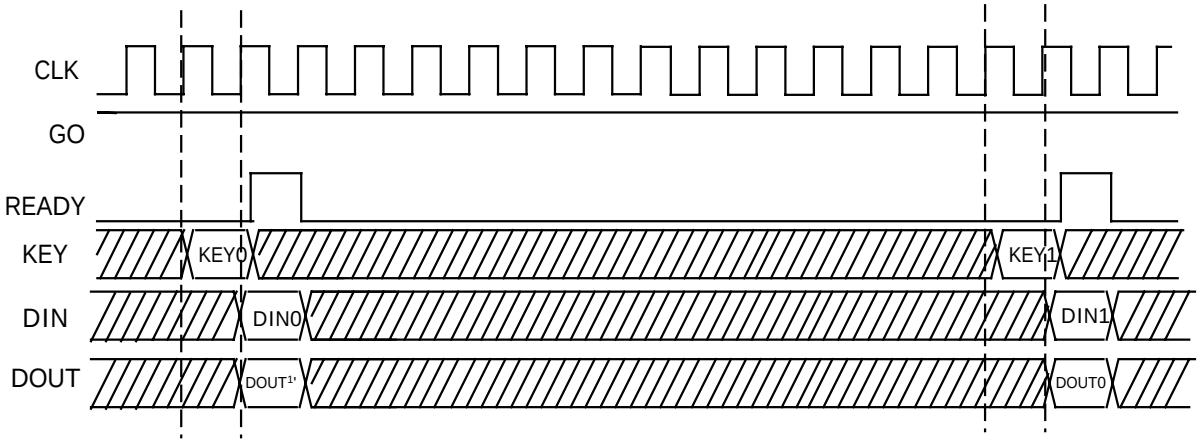



**Figure 3. Timing diagram for no dead cycles. DOUT[1] is the previous DOUT.**

Switching mode from encryption to decryption or vice-versa can be done with no dead cycles when providing a new key as shown in Figure 4.

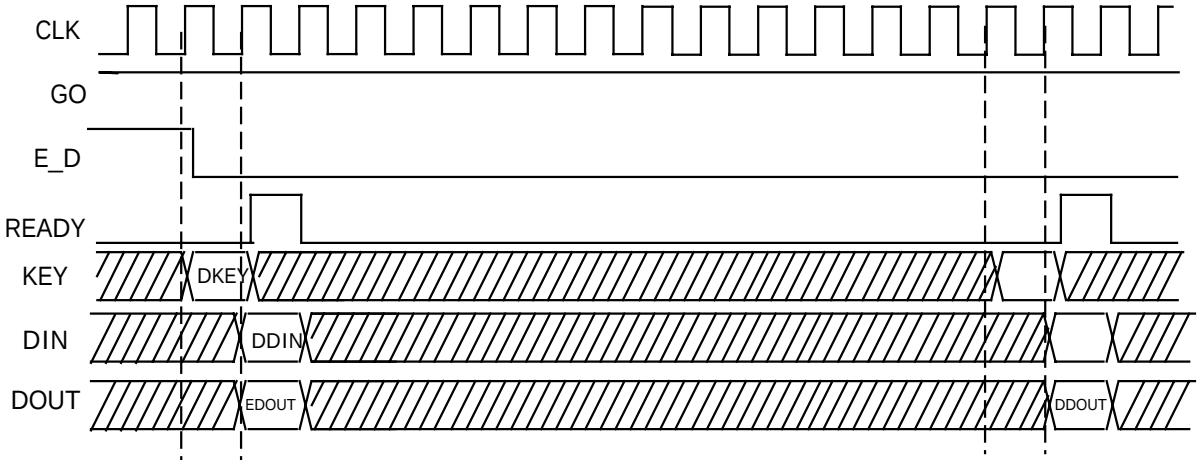



**Figure 4 Switching mode from encryption to decryption and vice-versa**

As can be seen from the timing diagram above, the decryption key DKEY is inputted one cycle before the result, EDOUT from a previous encryption operation.

The lack of dead cycles allows the core to sustain the theoretical bit rate of 4 x clock rate, regardless of the cryptographic operation being performed.

A cryptographic operation can be aborted at any time by lowering the GO signal.

The core can be asynchronously resetted by lowering the RSTN input port.

## Performance

Performance figures of the core in ECB mode, implemented with some particular technologies, are shown in the table below

| Technology | Area | Speed | Throughput |
|---|---|---|---|
| ASIC 0.18 u | 3.9 Kgates | 333 MHz | 1.332 Gbit/s |
| Virtex E | 238 slices | 143 MHz | 572 Mbit/s |
| Virtex II | 238 slices | 204 MHz | 816 Mbit/s |

## Export Permits

The core is available for export to all the countries of the world with the exception of the following:

Iran North Korea Libya Cuba Sudan
Syria Iraq

It is the customer's responsibility to check with relevant authorities regarding the re-export of equipment containing this technology.

## Deliverables

Netlist available for most Altera and Xilinx devices.
Synthesizable VHDL or Verilog RTL.
Complete HDL testbench.
Complete data sheet.

**Ocean Logic Pty Ltd**
PO BOX 768 - Manly NSW 1655 - Australia
Tel: +61-2-99054152 Fax: +61-2-99050921
E-Mail: info@ocean-logic.com URL : http://www.ocean-logic.com/