

CAST DES

Data Encryption Standard Core

The DES core implements 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) 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 Core non-pipelined version is implemented to minimize the gate count and FPGA resources. After an initial latency of 16 cycles, it can output encryption/decryption at every cycle. The design does not use any memories such as SRAM.

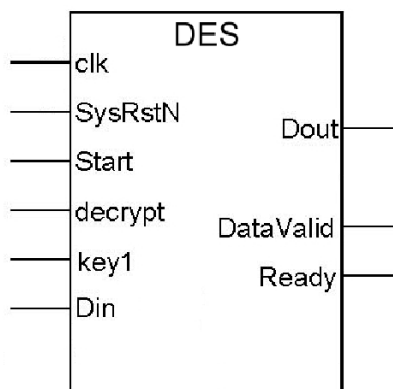
The DES core pipelined version is implemented to maximize performance by pipelining the DES transformation algorithm. The design does not use any memories such as SRAM.

Applications

The DES core can be utilized for a variety of encryption applications including:

- Secure File/Data transfer
- Electronic Funds Transfer
- Encrypted Storage Data
- Secure communications

Block Diagram



Features

- FIPS 46-3 Standard Compliant
- Encryption/Decryption performed in 16 cycles (ECB mode)
- 56 bits of security
- For use in FPGA or ASIC designs
- Verilog IP Core

Non Pipelined version

- Small gate count

Pipelined version

- Pipelined for maximum performance
- Encryption/Decryption performed in 1 cycle (ECB mode) after an initial latency of 16 cycles

Functional Description

DES Description

The Data Encryption Standard (DES) is a cryptographic algorithm specified in the United States Federal Information Processing Standards Publications (FIPS) 46-3 publication. This publication provides a complete description of a mathematical algorithm for encrypting and decrypting binary coded information.

Encrypting converts the data to an unintelligible form called ciphertext. Decrypting the ciphertext converts the data back to its original form and is called plaintext. The algorithm described in the FIPS 46-3 publication specifies both encrypting and decrypting operations based on a binary number called a key.

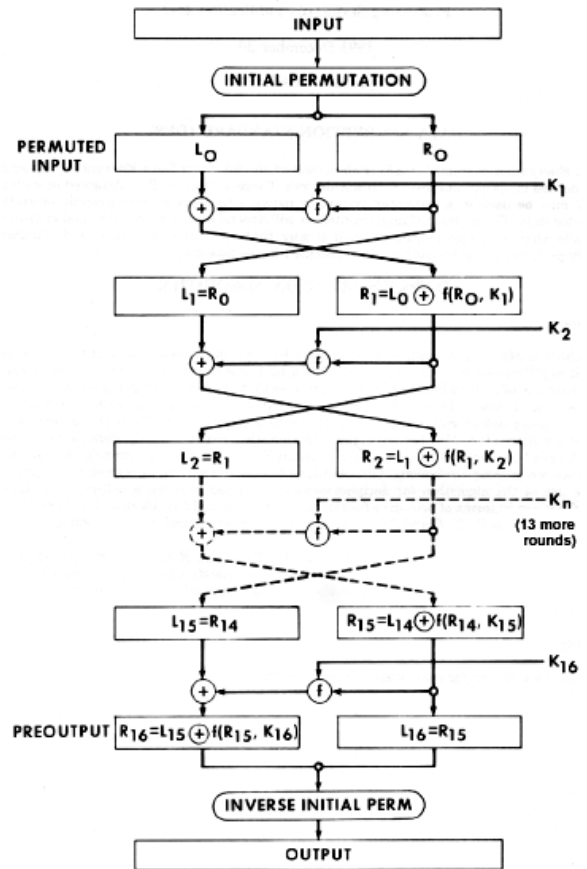
A key consists of 64 binary bits of which 56 bits are usually randomly generated and used directly by the algorithm. The other 8 bits are not used.

Authorized users of the data must have the key that was used to encrypt the data in order to decrypt it. The unique key chosen for use in a particular application makes the results of encrypting data using the algorithm unique. Selection of a different key causes the ciphertext that is produced for any given set of inputs to be different. Therefore, the cryptographic security of the data depends on the security provided for the key used to encrypt and decrypt the data.

DES Block Cipher Encryption Operation

During each pass of the DES engine (module), a 64 bit block is subjected to an initial permutation, then to a complex key-dependent computation and finally to a permutation that is the inverse permutation.

The key-dependent computation is implemented as a function called the key schedule and uses the subkeys generated in the key_sel module. The DES engine can be run in two directions - as a forward transformation and as an inverse transformation. The two directions differ only by the order in which the bits of the key are used. The forward transformation is shown in following figure.



DES Electronic Code Book (ECB) Mode

The Electronic Codebook (ECB) mode is a block, encryption/decryption method which transforms 64 bits of input to 64 bits of output. The ECB output block is a complex function of all 64 bits of the input block and all 56 independent bits of the key.

Since the ECB mode is a 64-bit block cipher, the DES engine encrypts data in multiples of sixty-four bits. Therefore a block input is 64 bits wide (Din [63:0]). See signal definitions.

If a user has less than sixty-four bits to encrypt, then the least significant bits of the unused portion of the input data block must be padded. These bits are often filled with random or pseudo-random bits, prior to ECB encryption. The corresponding DES decryption discards these padding bits after decryption of the ciphertext block.

The same input block always produces the same output block under a fixed key in ECB mode.

Implementation Results

DES core reference designs have been evaluated in a variety of technologies. The following are sample ASIC results.

Non Pipelined Optimized for Area					
ASIC Technology	Cell Area	NAND2 Area Used	Approx. Area (gate equiv.)	Frequency (MHz)	Throughput (Mbps)
TSMC .09 μm	7,297	2.82	2,588	334	1336
TSMC .13 μm	14,793	5.0922	2,905	232	928
TSMC .18 μm	29,958	9.9792	3,002	151	604
Non Pipelined Optimized for Speed					
ASIC Technology	Cell Area	NAND2 Area Used	Approx. Area (gate equiv.)	Frequency (MHz)	Throughput (Gbps)
TSMC .09 μm	8,411	2.82	2,983	625	2.50
TSMC .13 μm	20,525	5.0922	4,031	555	2.22
TSMC .18 μm	41,626	9.9792	4,171	416	1.66
Pipelined Optimized for Speed					
ASIC Technology	Cell Area	NAND2 Area Used	Approx. Area (gate equiv.)	Frequency (MHz)	Throughput (Gbps)
TSMC .09 μm	106,596	2.82	37,800	1,190	76.16
TSMC .13 μm	256,088	5.0922	50,290	813	52.03
TSMC .18 μm	502,010	9.9792	50,305	633	40.51

Example of DES Encrypted AND Decrypted Data

The following example data may be used when testing the DES encryption and decryption operations.

Key = 0x0123456789abcdef

PLAINTEXT0 = 0x4e6f772069732074

PLAINTEXT1 = 0x68652074696d6520

PLAINTEXT2 = 0x666f7220616c6c20

CIPHERTEXT0 = 0x3fa40e8a984d4815

CIPHERTEXT1 = 0x6a271787ab8883f9

CIPHERTEXT2 = 0x893d51ec4b563b53

Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

Verification

The core has been verified through extensive simulation and rigorous code coverage measurements.

Deliverables

The core includes everything required for successful implementation. The ASIC version includes:

- HDL RTL source code
- Sophisticated self-checking Testbench
- Simulation script, vectors, and expected results
- Synthesis script
- Comprehensive user documentation