

Serial Data Encryption / Decryption Standard

Features

- High speed DES Encryption and Decryption core
- Compliant with FIPS PUB 46-3
- Available for all vendors
- Easy to use interface signals
- On the fly encryption decryption changes

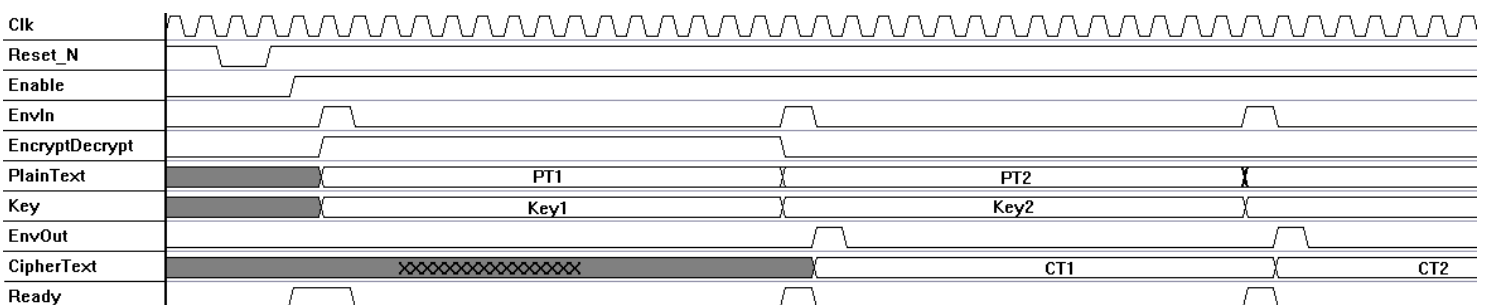
Application

The serial DES core can be used to secure all communication systems, data storage, financial transactions, video, etc...

I/O

Signal	Direction	Width	Function
Clk	IN	1 bit	Input clock
Reset_n	IN	1 bit	Reset (active Low)
Enable	IN	1 bit	Enable
EnvIn	IN	1 bit	Input envelop
EncryptDecrypt	IN	1 bit	Encryption ('1') or Decryption ('0') selection
PlainText	IN	64 bits	Data to encrypt or decrypt
Key	IN	64 bits	Encryption or decryption key
CypherText	OUT	64 bits	Encrypted or decrypted data
Ready	OUT	1 bit	Module ready
EnvOut	OUT	1 bit	Output envelop

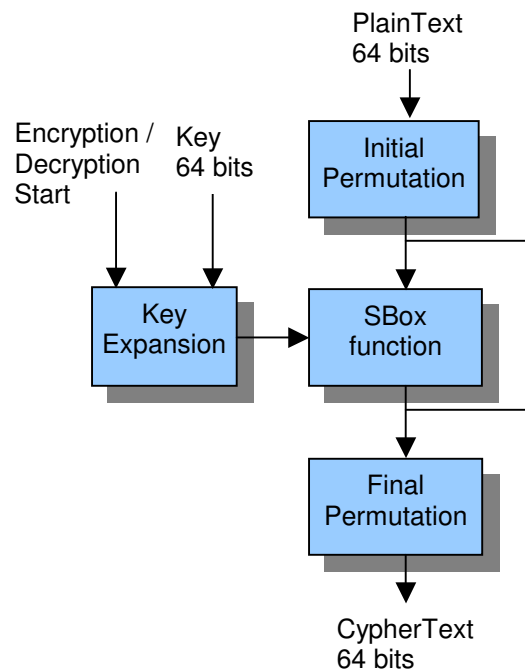
Timing



Functional description

The serial DES core encrypts and decrypts block words of 64 bits with the ECB (Electronic Codebook) method.

The architecture is shown below :



One word is encrypted or decrypted every 16 clocks.

Performance characteristics

The serial DES occupies 281 slices on Xilinx Virtex 2 Pro, and the synthesis frequency is 243MHz.

The overall throughput is 972 Mbits/s.