NOLAM SERVICES & INDUSTRIES

www.nsindus.com

NES-IPCORE-TDES

IP CORE TRIPLE DES

HIGHLIGHTS

Certified 64 bits capable DES and triple-DES 64 bits Crypto Core

The core performs a classical modular exponentiation $x^y \ mod \ m$

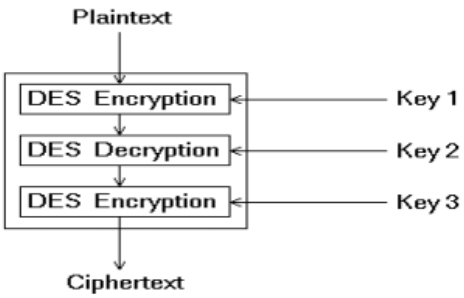
The core performs $E_{K3}\left(D_{K2}\left(E_{K1}(I)\right)\right) = O$ encryption and $D_{K1}\left(E_{K2}\left(D_{K3}(O)\right)\right) = I$ decryption

where $E_k(I)$ and $D_k(I)$ denote the DES encryption and decryption of I using DES key K, respectively

Direct addressing of all Registers

Can be customized

RELATED PRODUCT



The NES-IPCORE-TDES is a Triple-DES which is an extension of Data Encryption Standard (DES) that results in a more complex but more secure block cipher. Standard DES represents a component in Triple-DES architecture. If $E_K(I)$ and $D_K(I)$ denote the DES encryption and decryption of *I* using DES key *K*, respectively, then Triple-DES encryption and decryption is performed as follows:

Encryption: $E_{K3}(D_{K2}(E_{K1}(I))) = O$

Decryption: $D_{K1}(E_{K2}(D_{K3}(O))) = I$

Any other pre-designed functions can be integrated into the FPGA. FPGA density and I/O requirements can be defined according to customer specifications.

Designers should be familiar with cryptographic standard, VHDL or Verilog, synthesis tools, FPGA Place and Route data flow and VHDL simulation software. Experience with microprocessor is recommended. The macro can easily be integrated into hierarchical VHDL or Verilog designs.

Order Part Number:

- NES-IPCORE-TDES-VH IP CORE Triple DES VHDL version
- NES-IPCORE-TDES-VE IP CORE Triple DES VERILOG version