An Industry Standard Benchmark Consortium

DENBench™ Version 1.0 — Benchmark Name: DES

Highlights

- **Benchmarks the Digital Encryption Standard (DES) algorithm**
- **Created in part from SSLEAY sources, the open source Netscape Secure Socket Layer source code base**
- **Roundtrip implementation and self-checking assures accuracy**
- **A component of the EEMBC Cryptography Sub-suite**
- **DES is a popular cryptographic algorithm (especially in Triple-DES configuration) used widely in eCommerce applications, including mobile phones m-commerce**

History, Applications and Restrictions

The Digital Encryption Standard (DES) benchmark is a cipher algorithm that provides an indication of the potential performance of a microprocessor or digital signal processor (DSP) subsystem doing DES cryptographic encryptions and decryptions. The DES cipher is used in numerous cryptographic protocols, including transport layer security (TLS), secure socket layer, (SSL), secure shell (SSH), and Internet protocol security (IPSEC). A history of the cipher's development is available at http://en.wikipedia.org/wiki/DES.

Although it is vulnerable to certain, extremely computationally intensive cracking attacks (on the order of a successful crack in 24 hours), DES remains popular in many eCommerce (internet) and m-commerce (mobile) applications but has been replaced for the most secure applications by the Advanced Encryption Standard (AES), which is also part of the EEMBC benchmark suite.

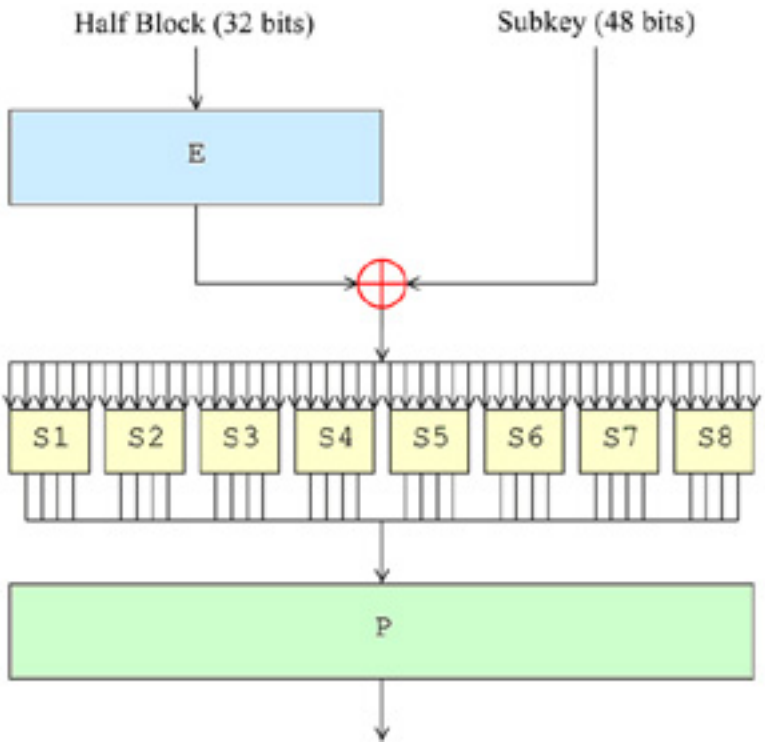
This benchmark, and the source code, is subject to the following restrictions:

This software is subject to export restrictions from the United States of America to non-USA countries. Export and re-export controls on commercial encryption products are administered by the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce. Rules governing exports and re-exports of encryption items are found in the Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774. Sections 740.13, 740.17 and 742.15 of the EAR are the principal references for the export and re-export of encryption items. Further information is available from http://www.bis.doc.gov/Encryption.

Benchmark Description

DES is an iterated block cipher with a fixed block length of 64 bits and a fixed key length of 64 bits. However, only the first 56 bits are used; the other 8 bits are for parity checking (hence DES is considered 56-bit encryption). EEMBC implements the correct key length. Like most cryptographic functions, there is an array (or "block") that is subjected to multiple transformations (in

the case of DES, 16). Unlike the AES benchmark implementation [correct?], EEMBC does not implement the FIPS tests on DES. Checking is by cyclical redundancy checksum (CRC).



The input data for the DES benchmark is proprietary to EEMBC but [what characteristics?].

Analysis of Computing Resources

The benchmark is computationally challenging: addition, multiplication, extensive use of division, bit shifting, matrix math, bitwise operators such as XOR, and other operators are used. It is implemented in integer math. This benchmark is almost exclusively CPU bound, and the quality of the math library as well as memory library has an effect on performance. Memory moves are repeatedly performed, so optimized C library mem* functions would improve performance without overwhelming the basic math computations. Superscalar and VLIW architectures scheduled by sophisticated compilers (or assembly language implementations) can take advantage of some parallelism. Many of the computationally challenging functions can be offloaded to hardware acceleration logic.