

PACKAGE ID - 001186SPARC00 SSEL1.0

KWIC TITLE - Sandia Scalable Encryption Software

AUTHORS - Tarman, T.D.
Sandia National Labs., Albuquerque, NM (United States)

LIMITATION CODE -COPY **AUDIENCE CODE** - LIM

COMPLETION DATE - 08/29/1996 **PUBLICATION DATE** - 08/29/1996

DESCRIPTION - Sandia Scalable Encryption Library (SSEL) Version 1.0 is a library of functions that implement Sandia's scalable encryption algorithm. This algorithm is used to encrypt Asynchronous Transfer Mode (ATM) data traffic, and is capable of operating on an arbitrary number of bits at a time (which permits scaling via parallel implementations), while being interoperable with differently scaled versions of this algorithm. The routines in this library implement 8 bit and 32 bit versions of a non-linear mixer which is compatible with Sandia's hardware-based ATM encryptor.

PACKAGE CONTENTS - Media Directory; Software Abstract; Media Includes Source Code, Object Library, Executable Module, Compilation Instructions, Linking Instructions, Object Module, Programmer Documentation, Makefile and Sample Code Which Use the Library;

SOURCE CODE INCLUDED? - Yes

MEDIA QUANTITY - 1 3.5 Diskette

METHOD OF SOLUTION - The routines in this library implement functions that manipulate a linear feedback shift register (LFSR), and XOR the plaintext data with the output of the LFSR. In order to mask the linearity of this encryption approach, an invertible non-linear function (INLF) is provided as well. This provides protection against the well-known Berlekamp-Massey attack, and yet, provides the requisite scalability and interoperability required by ATM networks.

COMPUTER - SUN SPARC

OPERATING SYSTEMS - SunOS 4.1.3, Solaris 2.x (Sun Workstations), HP-UX 9.x (HP workstations)

PROGRAMMING LANGUAGES - C using the gcc compiler

SOFTWARE LIMITATIONS - Currently, the software can only encrypt/decrypt data 8 bits or 32 bits at a time (although the algorithm is scalable to an arbitrary number of bits).

SOURCE CODE AVAILABLE (Y/N) - Y

UNIQUE FEATURES - No other software package implements this algorithm.

PACKAGE ID - 001186SPARC00 SSEL1.0

OTHER PROG/OPER SYS INFO - This library is restricted to host platforms that are big endian, and operating systems that implement 32 bit integers.

HARDWARE REQS - Systems that meet the restrictions described above. Very little disk space and memory is required by these libraries.

TIME REQUIREMENTS - (Note: all timing measurements performed on a Sun SPARCstation 10, 40 MHz CPU, Solaris 2.4 multiuser) encrypt8 (8 bit encryption/LFSR operation): 35 microseconds/call, encrypt32 (32 bit encryption/LFSR operations): 36 microseconds/call, permute8 (8 bit INLF): 8 microseconds/call, permute32 (32 bit INLF): 18 microseconds/call.

ABSTRACT STATUS - Submitted 8/8/97. Released AS-IS 10/30/97

SUBJECT CLASS CODE - M

KEYWORDS -

COMPUTER PROGRAM DOCUMENTATION
S CODES
DATA ANALYSIS

EDB SUBJECT CATEGORIES -
990200

SPONSOR - DOE/DP

PACKAGE TYPE - AS - IS