February 1999

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

# ENHANCEMENTS TO DATA ENCRYPTION AND DIGITAL SIGNATURE FEDERAL STANDARDS

To provide needed increased security protection of sensitive, unclassified information in federal computer systems, NIST's Information Technology Laboratory recently took steps to enhance two Federal Information Processing Standards (FIPS): FIPS 46-2, Data Encryption Standard, and FIPS 186, Digital Signature Standard. These two standards are discussed below.

## DATA ENCRYPTION STANDARD

On January 15, 1999, a *Federal Register* notice announced the Draft FIPS 46-3, Data Encryption Standard, and requested comments from industry, government agencies, and the public on the draft standard. The Data Encryption Standard (DES) provides specifications for the Data Encryption Algorithm and is used by federal agencies (and others outside the government) for the protection of sensitive information. The DES, currently specified in FIPS 46-2, was due for review in December 1998. NIST proposes replacing FIPS 46-2 with FIPS 46-3 to provide for the use of Triple DES as specified in the American National Standards Institute (ANSI) X9.52 standard.

### Background

FIPS 46, Data Encryption Standard, first issued in 1977, specifies the Data Encryption Algorithm for the cryptographic protection of computer data. The standard provided that it be reviewed within five (5) years to assess its adequacy. The first review was completed in 1983, and the standard was reaffirmed for federal government use (48 FR 41062). The second review was completed in 1987, and the standard was again reaffirmed for federal government use (52 FR 7006) and re-issued as FIPS 46-1 with minor editorial updating. The third review was completed in 1993, and the standard was reaffirmed as FIPS 46-2 for federal government use (58 FR 69347). In addition to hardware implementations, FIPS 46-2 provided for software implementations of the DES. NIST now proposes to replace FIPS 46-2 with FIPS 46-3 to also allow for the use of Triple DES as described in ANSI X9.52.

When DES was reaffirmed in 1993, NIST stated in the announcement that NIST would "consider alternatives which offer a higher level of security" at the next review in 1998. After the first exhaustion of a DES key, NIST advised federal organizations that DES, properly used, still provided adequate security for many applications. At that time, NIST also stated that organizations needing security beyond that provided by the DES could use Triple DES as specified in ANSI X9.52. NIST worked with the financial community to develop this standard. Triple DES is a

*Continued on page 2*

*ITL Bulletins* are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since April 1997:

method for using the DES algorithm in three operations. These operations have been documented and specified as an American National Standard (ANSI X9.52) by Accredited Standards Committee X9 for Financial Services, which develops cryptography and public key infrastructure standards. The American Bankers Association is the secretariat for X9. See below for ordering information for the X9.52 standard.

Additionally, knowing that the DES' security life was nearing an end, NIST has been working with industry and the cryptographic community to develop an Advanced Encryption Standard (AES) for the 21st century. On January 2, 1997, NIST announced the initiation of an effort to develop the AES (62 FR 93). It is intended that the AES will specify an unclassified, publicly disclosed encryption algorithm capable of protecting sensitive government information well into the next century. Unfortunately, since it takes a substantial amount of time to gain confidence in a new encryption algorithm, the AES is not expected to be a fully developed FIPS for some time to come. Information on NIST's multi-year effort to develop the AES can be obtained at http://www.nist.gov/aes.

### Use of Triple DES

Recently, claims have been made of a special-purpose hardware-based attack on the DES. In light of this most recent attack, NIST can no longer support the use of the DES for many applications. As with other security tools, encryption must balance cost against risk. The recent brute force exhaustion attack by a "cracking machine" costing $250,000 took 56 hours to crack a single message. With this special-purpose technology, the average time of cracking per message would be twice that, since only a quarter of all keys were tested. In some cases this kind of attack may not pose an immediate or significant threat -- for example where short-term protection of perishable information is desired. However, advances in technology are likely to further reduce the average cracking time. Therefore, NIST recommends the following:

- For existing systems, develop a prudent transition strategy to move to Triple DES. This strategy should match the strength of the protective measures against the associated risk. Critical systems should receive priority; and
- When building new systems, use Triple DES to protect sensitive, unclassified data.

These recommendations are reflected in the proposed draft FIPS 46-3 by recognizing Triple DES, as described in ANSI X9.52, as a FIPS-approved algorithm.

### Comments and Ordering Information

Comments on the proposed draft FIPS 46-3 must be received **on or before April 15, 1999**. Written comments concerning this standard should be sent to:

Information Technology Laboratory
ATTN: Review of Draft FIPS 46-3
National Institute of Standards and Technology
100 Bureau Drive, STOP 8970
Gaithersburg, MD 20899-8970

Comments may also be sent electronically to: desreview@nist.gov.

Interested parties may order a copy of FIPS 46-2 from the

National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161
Telephone (703) 487-1650

Copies of FIPS 46-2 and its proposed replacement (Draft FIPS 46-3) are available electronically at http://csrc.nist.gov/fips.

Ordering information for the ANSI X9.52 (Triple DES) standard is available from American Bankers Assoc./DC, X9 Customer Service Dept., P.O. Box 79064, Baltimore, MD 21279-0064, telephone 1-800-338-0626.

For more information, contact Miles Smid, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-8930; telephone (301) 975-2938 or fax (301) 926-2733.

### DIGITAL SIGNATURE STANDARD

A *Federal Register* notice of December 15, 1998, announced that the Secretary of Commerce had approved an interim final standard FIPS 186-1, Digital Signature Standard, and requested comments from the public, academic and research communities, manufacturers, voluntary standards organizations, and federal, state, and local government organizations. This interim final standard

**Who we are**

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today.

allows for both the use of the Digital Signature Algorithm (DSA) and the American National Standards Institute (ANSI) X9.31 standard by federal organizations. The X9.31 standard describes the Rivest-Shamir-Adleman (RSA) digital signature technique. The effective date of the interim final standard is December 15, 1998.

### Background

On May 10, 1994, the Secretary of Commerce approved FIPS 186, Digital Signature Standard, which specifies a single technique for the generation and verification of digital signatures. Recently, another technique, known as RSA, was approved as the X9.31 standard [X9.31-1998 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)] by ANSI. A second standard, based upon a technique known as elliptic curve, is expected to be completed and approved by ANSI in the near future. Agencies have expressed considerable interest to NIST in using these technologies.

On May 13, 1997, NIST published a *Federal Register* notice soliciting comments on amending FIPS 186 to allow for the use of other techniques, specifically mentioning RSA and elliptic curve (but not with detailed specifications as now exist for RSA in the ANSI X9.31 standard). The public comments overwhelmingly supported revising FIPS 186 to include these additional algorithms. RSA, which has withstood widespread scrutiny by the cryptographic research community, is available in many commercial products. NIST believes it to be robust and sufficiently strong for use by federal agencies.

**ITL Bulletins Via E-Mail**

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

### Interim Modification to FIPS 186

Following ANSI's recent approval of the ANSI X9.31 standard, the Secretary of Commerce approved an interim modification to FIPS 186 (FIPS 186-1) to approve the use of the digital signature technique specified in X9.31 in addition to the algorithm currently specified in FIPS 186. The Secretary's decision revises the old FIPS 186 by adding the following statements into the new FIPS 186-1:

- Add the following as the last sentence of the "Applications" paragraph: The technique specified in ANSI X9.31 may be used in addition to the Digital Signature Algorithm (DSA) specified herein.
- Add the following as the last two sentences of the "Implementations" paragraph: Agencies are advised that separate keys should be used for signature and confidentiality purposes when using the X9.31 standard. This is because the RSA algorithm can be used for both data encryption and digital signature purposes.
- To minimize any potential for spoofing digital signatures, keys used for signature purposes should not be recoverable. Using separate keys will allow agencies to recover confidentiality keys but not signature keys.

The standard has also been modified to reflect the availability of conformity testing for DSA implementations. (ANSI's conformity testing program for X9.31 implementations is not yet in place.) Minor language modifications (e.g., indicating that two algorithms are now approved) and other administrative updates have also been made to the standard.

Since ANSI's conformance testing program for the X9.31 standard is not yet in place, federal agencies are advised, in the interim, to acquire products that vendors hold out as in conformance with ANSI X9.31. Agencies will be advised by NIST when a conformance testing program is in effect.

### Comments and Ordering Information

Comments are due **on or before March 15, 1999**. These comments will assist NIST in making a recommendation to the Secretary of Commerce regarding a final decision.

Comments should be sent to:

Information Technology Laboratory
ATTN: DSS/X9.31 Comments
National Institute of Standards and Technology
100 Bureau Drive, STOP 8970
Gaithersburg, MD 20899-8970

Comments may also be sent electronically to fips186rsa@nist.gov.

Specifications of FIPS 186 (and FIPS 186-1) are available electronically at http://csrc.nist.gov/fips/.

Ordering information for the ANSI X9.31 standard is available from American Bankers Assoc./DC, X9 Customer Service Dept., P.O. Box 79064, Baltimore, MD 21279-0064, telephone 1-800-338-0626.

For more information, contact Edward Roback, National Institute of Standards and Technology, 100 Bureau Drive, STOP 8930, Gaithersburg, MD 20899-8930; telephone (301) 975-3696 or fax (301) 926-2733.

*U.S. DEPARTMENT OF COMMERCE*
*National Institute of Standards and Technology*
*100 Bureau Drive, Stop 8900*
*Gaithersburg, MD 20899-8900*

*Official Business*
*Penalty for Private Use $300*

*Address Service Requested*

*BULK RATE*
*POSTAGE & FEES*
*PAID*
*NIST*
*PERMIT NUMBER G195*