

NIST Special Publication 800-XX

NIST

National Institute of Standards
and Technology
Technology Administration
U.S. Department of Commerce

**Recommendations Regarding
Federal Information Processing
Standard (FIPS) 186-2,
Digital Signature Standard (DSS)**

Methods and Techniques

Elaine Barker

COMPUTER SECURITY



The National Institute of Standards and Technology was established in 1988 by Congress to “assist industry in the development of technology needed to improve product quality, to modernize manufacturing processes, to ensure product reliability . . . and to facilitate rapid commercialization . . . of products based on new scientific discoveries.”

NIST, originally founded as the National Bureau of Standards in 1901, works to strengthen U.S. industry’s competitiveness; advance science and engineering; and improve public health, safety, and the environment. One of the agency’s basic functions is to develop, maintain, and retain custody of the national standards of measurement, and provide the means and methods for comparing standards used in science, engineering, manufacturing, commerce, industry, and education with the standards adopted or recognized by the Federal Government.

As an agency of the U.S. Commerce Department’s Technology Administration, NIST conducts basic and applied research in the physical sciences and engineering, and develops measurement techniques, test methods, standards, and related services. The Institute does generic and precompetitive work on new and advanced technologies. NIST’s research facilities are located at Gaithersburg, MD 20899, and at Boulder, CO 80303. Major technical operating units and their principal activities are listed below. For more information contact the Publications and Program Inquiries Desk, 301-975-3058.

Office of the Director

- National Quality Program
- International and Academic Affairs

Technology Services

- Standards Services
- Technology Partnerships
- Measurement Services
- Information Services

Advanced Technology Program

- Economic Assessment
- Information Technology and Applications
- Chemistry and Life Sciences
- Materials and Manufacturing Technology
- Electronics and Photonics Technology

Manufacturing Extension Partnership Program

- Regional Programs
- National Programs
- Program Development

Electronics and Electrical Engineering Laboratory

- Microelectronics
- Law Enforcement Standards
- Electricity
- Semiconductor Electronics
- Radio-Frequency Technology¹
- Electromagnetic Technology¹
- Optoelectronics¹

Materials Science and Engineering Laboratory

- Intelligent Processing of Materials
- Ceramics
- Materials Reliability¹
- Polymers
- Metallurgy
- NIST Center for Neutron Research

Chemical Science and Technology Laboratory

- Biotechnology
- Physical and Chemical Properties²
- Analytical Chemistry
- Process Measurements
- Surface and Microanalysis Science

Physics Laboratory

- Electron and Optical Physics
- Atomic Physics
- Optical Technology
- Ionizing Radiation
- Time and Frequency¹
- Quantum Physics¹

Manufacturing Engineering Laboratory

- Precision Engineering
- Automated Production Technology
- Intelligent Systems
- Fabrication Technology
- Manufacturing Systems Integration

Building and Fire Research Laboratory

- Applied Economics
- Structures
- Building Materials
- Building Environment
- Fire Safety Engineering
- Fire Science

Information Technology Laboratory

- Mathematical and Computational Sciences²
- Advanced Network Technologies
- Computer Security
- Information Access and User Interfaces
- High Performance Systems and Services
- Distributed Computing and Information Services
- Software Diagnostics and Conformance Testing
- Statistical Engineering

¹At Boulder, CO 80303,

²Some elements at Boulder, CO.

NIST Special Publication 800-xx

Recommendations Regarding Federal Information Processing Standard (FIPS) 186-2, Digital Signature Standard (DSS)

Methods and Techniques

Elaine Barker

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

October 2001



U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Karen H. Brown, Acting Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Karen H. Brown, Acting Director

Reports on Information Security Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure for information technology. ITL develops tests, test methods, reference data, proof of concept implementations and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of Sensitive unclassified information in federal computer systems. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-xx
Natl. Inst. Stand. Technol. Spec. Publ. 800-xx, xx pages (Date)
CODEN: NSPUE2

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2001

For sale by the Superintendent of Documents. U.S. Government Printing Office. Washington. DC 20402-9325

Recommendations Regarding Federal Information Processing Standard (FIPS) 186-2, Digital Signature Standard (DSS)

Methods and Techniques

1 Purpose

This publication provides recommendations regarding the implementation and use of Federal Information Processing Standard (FIPS) 186-2, Digital Signature Standard (DSS).

2 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Computer Security Act of 1997 (Public Law 100-235) and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3(a)(5). This is not a guideline within the meaning of (15 U.S.C. 278 g-3 (a)(5).

This recommendation is neither a standard nor a guideline, and as such, is neither mandatory nor binding on Federal agencies. Federal agencies and non-government organizations may use this recommendation on a voluntary basis. It is not subject to copyright.

Nothing in this recommendation should be taken to contradict standards and guidelines that have been made mandatory and binding upon Federal agencies by the Secretary of Commerce under his statutory authority. Nor should this recommendation be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

3 Background

FIPS 186-2 specifies the Digital Signature Algorithm (DSA) that may be used in the generation and verification of digital signatures for sensitive, unclassified applications. This standard is used in conjunction with the hash function specified in FIPS 180-1 and includes specifications for the size of the prime modulus p , and algorithms for the generation of a user's private key, x , and a user's per message secret number, k . This publication is intended to provide recommendations for the continued use of FIPS 186-2.

4 Recommendations regarding FIPS 186-2

This special publication provides recommendations regarding the size of the prime modulus p , modifications for the random number generation techniques specified in Appendix 3 of FIPS 186-2, and recommendations for the use of these techniques when used in contexts other than the generation of DSA keys.

4.1 The Prime Modulus p

FIPS 186-2 specifies that the prime modulus p is defined for the range of prime integers $2^{L-1} < p < 2^L$, where $512 \leq L \leq 1024$ and L is a multiple of 64. This publication recommends that L should assume only the value 1024 for DSA as specified in this standard, i.e., the prime modulus p should be defined in the range $2^{1023} < p < 2^{1024}$.

4.2 Random Number Generation

FIPS 186-2 includes algorithms for the generation of a user's private key, x , and a user's per message secret number, k . These values must be generated randomly or pseudorandomly and must have values between 0 and the 160-bit prime q (as specified in the standard). Techniques for generating x and k are provided in Appendix 3 of the standard.

Recently, an unpublished attack on DSA¹ was found that relies on the non-uniformity of the pseudorandom number generators (PRNGs) specified in Appendix 3 of the standard. The attack is not considered to be feasible at this time, so existing implementations of DSA are not yet at risk. However, the following modifications of the PRNGs may be used in lieu of those PRNGs specified in FIPS 186-2 when users are concerned about the attack. These modifications reduce the non-uniformity of the PRNGs and do not affect interoperability.

The algorithms described in Sections 4.2.1 and 4.2.2 use a one-way function $G(t,c)$, where t is 160 bits, c is b bits and $G(t,c)$ is 160 bits. Two methods for constructing G are defined in FIPS 186-2: using SHA-1 as defined in FIPS 180-1, and using the Data Encryption Standard (DES) as defined in FIPS 46-3. If G is constructed using SHA-1, b is between 160 and 512 bits ($160 \leq b \leq 512$); if G is constructed using DES, b is equal to 160 bits.

4.2.1 Revised Algorithm for Computing m values of x (Appendix 3.1 of FIPS 186-2)

Let x be the signer's private key. The following may be used to generate m values of x :

Step 1. Choose a new, secret value for the seed-key, $XKEY$.

Step 2. In hexadecimal notation let

$$t = 67452301 \text{ EFCDAB89 } 98\text{BADCFE } 10325476 \text{ C3D2E1F0.}$$

¹ The attack was discovered by Dr. Daniel Blichebacher of Lucent Technologies, Bell Labs, Murray Hill, NJ. See a February 25, 2001 press article at <http://www.lucent.com/press/0201/010205.bla.html>.

This is the initial value for $H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4$ in the SHS [FIPS 180-1].

Step 3. For $j = 0$ to $m - 1$ do

3.1 $XSEED_j$ = optional user input

3.2 For $i = 0$ to 1 do

a. $XVAL = (XKEY + XSEED_j) \bmod 2^b$

b. $w_i = G(t, XVAL)$.

c. $XKEY = (1 + XKEY + w_i) \bmod 2^b$.

3.3 $x_j = (w_0 \parallel w_1) \bmod q$

4.2.2 Revised Algorithm for Precomputing one or More k and r Values (Appendix 3.2 of FIPS 186-2)

This algorithm can be used to precompute k , k^{-1} , and r for m messages at a time. Note that implementation of the DSA with precomputation may be covered by U.S. and foreign patents.

Step 1. Choose a secret initial value for the seed-key, $KKEY$.

Step 2. In hexadecimal notation let

$t = \text{EFCDAB89 98BADCFE 10325476 C3D2E1F0 67452301}$.

This is a cyclic shift of the initial value for $H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4$ in the SHS.

Step 3. For $j = 0$ to $m - 1$ do

3.1 For $i = 0$ to 1 do

a. $w_i = G(t, KKEY)$

b. $KKEY = (1 + KKEY + w_i) \bmod 2^b$

3.2 $k = (w_0 \parallel w_1) \bmod q$

3.3 Compute $k_j^{-1} = k^{-1} \bmod q$

3.4 Compute $r_j = (g^k \bmod p) \bmod q$

Step 4. Suppose M_0, \dots, M_{m-1} are the next m messages. For $j = 0$ to $m - 1$ do

- a. Let $h = \text{SHA-1}(M_j)$.
- b. Let $s_j = (k_j^{-1}(h + xr_j)) \bmod q$
- c. The signature for M_j is (r_j, s_j) .

Step 5. Let $t = h$

Step 6. Go to step 3.

Step 3 permits pre-computation of the quantities needed to sign the next m messages. Step 4 can begin whenever the first of these m messages is ready. The execution of step 4 can be suspended whenever the next of the m messages is not ready. As soon as steps 4 and 5 have completed, step 3 can be executed, and the results saved until the first member of the next group of m messages is ready.

In addition to space for $KKEY$, two arrays of length m are needed to store r_0, \dots, r_{m-1} and $k_0^{-1}, \dots, k_{m-1}^{-1}$ when they are computed in step 3. Storage for s_0, \dots, s_{m-1} is only needed if the signatures for a group of messages are stored; otherwise s_j in step 4 can be replaced by s , and a single space allocated.

4.3 General Purpose Random Number Generation

Several of the FIPS require the use of an Approved (i.e., FIPS-approved or NIST recommended) random number generator (RNG). The RNG in Appendix 3.1 of FIPS 186-2 or in Section 4.2.1 of this recommendation may be used in addition to any other Approved RNG. However, when the RNG is used for the generation of random numbers other than for DSA keys, it is recommended that the “mod q ” term be omitted. This will result in the following changes to the specification:

FIPS 186-2, Appendix 3.1, Step 3 c:

Change “ $x_j = G(t, XVAL) \bmod q$ ” to “ $x_j = G(t, XVAL)$ ”.

This recommendation, Section 4.2.1, Step 3, substep 3.2:

Change “ $x_j = (w_0 \parallel w_1) \bmod q$ ” to “ $x_j = (w_0 \parallel w_1)$ ”.