American National Standard
for Financial Services

X9.80–2005

Prime Number Generation, Primality Testing, and Primality Certificates

Accredited Standards Committee X9, Incorporated
Financial Industry Standards

Date Approved: August 15, 2005
American National Standards Institute

American National Standards, Technical Reports and Guides developed through the Accredited Standards Committee X9, Inc., are copyrighted. Copying these documents for personal or commercial use outside X9 membership agreements is prohibited without express written permission of the Accredited Standards Committee X9, Inc. For additional information please contact ASC X9, Inc., P.O. Box 4035, Annapolis, Maryland 21403.
Foreword

Approval of an American National Standard requires verification by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made toward their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken to reaffirm, revise, or withdraw this standard no later than five years from the date of approval.

Published by

Accredited Standards Committee X9, Incorporated
Financial Industry Standards
P.O. Box 4035
Annapolis, MD 21403 USA
X9 Online http://www.x9.org

Copyright © 2005 ASC X9, Inc.
All rights reserved.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of the publisher. Printed in the United States of America.
# Contents

Foreword .................................................................................................................................................. ii  
Tables ....................................................................................................................................................... v  
Introduction ............................................................................................................................................... vi  
1 Scope ....................................................................................................................................................... 1  
2 Normative references ............................................................................................................................... 2  
3 Terms and definitions .............................................................................................................................. 2  
4 Symbols and abbreviated terms ............................................................................................................. 4  
5 Prime Generation Methods .................................................................................................................... 5  
5.1 General Discussion ............................................................................................................................... 5  
5.2 Generation of Primes Using Random Integers ................................................................................... 7  
5.2.1 Generation of Random Primes with Sequential Search ............................................................... 7  
5.2.2 Generation of Random Primes with Uniform Distribution .......................................................... 8  
5.2.3 Testing Using Probabilistic Methods ............................................................................................ 8  
5.2.4 Testing Using Deterministic Methods ......................................................................................... 11  
5.3 Constructive Methods ......................................................................................................................... 16  
5.3.1 Shawe-Taylor's Algorithm ............................................................................................................ 16  
5.3.2 Maurer's Algorithm ....................................................................................................................... 17  
5.4 Side Conditions for Generating Primes using Random Integers ....................................................... 19  
6 Candidate Prime Testing Methods .......................................................................................................... 20  
7 Tables of Parameters ............................................................................................................................... 21  
7.1 Rounds Required for Miller-Rabin if Followed by Lucas .................................................................. 21  
7.2 Rounds Required for Frobenius-Granatham ....................................................................................... 21  
Annex A (normative) ................................................................................................................................. 23  
A.1 Modular Exponentiation ...................................................................................................................... 23  
A.2 Jacobi Symbol ......................................................................................................................................... 23  
A.3 Sieve Procedure ...................................................................................................................................... 25  
A.4 Algorithms for Polynomial Arithmetic .............................................................................................. 26  
A.5 Lucas Sequence ...................................................................................................................................... 28  
Annex B (informative) ................................................................................................................................. 30  
B.1 Discussion of General Prime Proving Methods .................................................................................. 30  
B.2 Discussion of the Distribution of Randomly Chosen Primes .......................................................... 30  
Annex C Summary of Changes from ANS X9.80–2001 (informative) ...................................................... 31  
C.1 Introduction ........................................................................................................................................... 31  
C.2 Technical changes ................................................................................................................................. 31  
C.2.1 Search Range for primes ................................................................................................................... 31  
C.2.2 Errors in Jacobi symbol algorithm ................................................................................................. 31  
C.2.3 Range of bases in Miller-Rabin test ............................................................................................... 32  
C.2.4 Perfect squares in Lucas test ........................................................................................................ 32  
C.2.5 Discriminants with Jacobi symbol 0 in Lucas test ........................................................................ 32  
C.2.6 Boundary conditions in Shawe-Taylor’s algorithm ................................................................... 32  
C.3 Editorial issues ....................................................................................................................................... 33  
C.3.1 Random bit generators .................................................................................................................... 33
C.3.2 Failure probability ....................................................................................................................................... 33
C.3.3 Lucas-Lehmer vs. Lucas............................................................................................................................. 33
C.3.4 Reference for combining Miller-Rabin and Lucas tests ........................................................................... 33
C.3.5 Versions of Shawe-Taylor.......................................................................................................................... 33
C.3.6 Binary expansions....................................................................................................................................... 33
C.3.7 Modulo $p$ division in Lucas sequence algorithm ...................................................................................... 33
C.3.8 Negative numbers in Lucas sequence example ............................................................................................ 33
C.3.9 Added Interval.............................................................................................................................................. 34
Bibliography.............................................................................................................................................................. 35
Tables

Table 1: An ECPP certificate for $p = 377681287$................................................................................................................. 16
Table 2: Rounds Required for Miller-Rabin ......................................................................................................................... 21
Table 3: Rounds Required for Frobenius-Grantham ........................................................................................................... 21
Introduction

NOTE The user’s attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights.

By publication of this standard, no position is taken with respect to the validity of this claim or of any patent rights in connection therewith. The patent holder has, however, filed a statement of willingness to grant a license under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. Details may be obtained from the standards developer.

Suggestions for the improvement or revision of this Standard are welcome. They should be sent to the X9 Committee Secretariat, Accredited Standards Committee X9, Inc., Financial Industry Standards, P.O. Box 4035, Annapolis, MD 21403 USA.

This Standard was processed and approved for submittal to ANSI by the Accredited Standards Committee on Financial Services, X9. Committee approval of the Standard does not necessarily imply that all the committee members voted for its approval.

The X9 committee had the following members:
Gene Kathol, X9 Chairman
Vincent DeSantis, X9 Vice-Chairman
Cynthia Fuller, Executive Director
Isabel Bailey, Managing Director

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACI Worldwide</td>
<td>Jim Shaffer</td>
</tr>
<tr>
<td>American Bankers Association</td>
<td>C. Diane Poole</td>
</tr>
<tr>
<td>American Express Company</td>
<td>Mike Jones</td>
</tr>
<tr>
<td>American Financial Services Association</td>
<td>Mark Zalewski</td>
</tr>
<tr>
<td>Bank of America</td>
<td>Daniel Welch</td>
</tr>
<tr>
<td>Capital One</td>
<td>Scott Sykes</td>
</tr>
<tr>
<td>Certicom Corporation</td>
<td>Daniel Brown</td>
</tr>
<tr>
<td>Citigroup, Inc.</td>
<td>Daniel Schutzer</td>
</tr>
<tr>
<td>Deluxe Corporation</td>
<td>John Fitzpatrick</td>
</tr>
<tr>
<td>Diebold, Inc.</td>
<td>Bruce Chapa</td>
</tr>
<tr>
<td>Discover Financial Services</td>
<td>Jennifer Schroeder</td>
</tr>
<tr>
<td>Federal Reserve Bank</td>
<td>Dexter Holt</td>
</tr>
<tr>
<td>First Data Corporation</td>
<td>Gene Kathol</td>
</tr>
<tr>
<td>Fiserv</td>
<td>Bud Beattie</td>
</tr>
<tr>
<td>Hewlett Packard</td>
<td>Larry Hines</td>
</tr>
<tr>
<td>Hypercom</td>
<td>Scott Spiker</td>
</tr>
<tr>
<td>IBM Corporation</td>
<td>Todd Arnold</td>
</tr>
<tr>
<td>Ingenico</td>
<td>John Sheets</td>
</tr>
<tr>
<td>Intuit, Inc.</td>
<td>Jana Hocker</td>
</tr>
<tr>
<td>J.P. Morgan Chase &amp; Co</td>
<td>Jacqueline Pagan</td>
</tr>
<tr>
<td>KPMG LLP</td>
<td>Alfred F. Van Ranst</td>
</tr>
</tbody>
</table>
The X9F subcommittee on Data and Information Security had the following members:

Richard J. Sweeney, Chairman

**Organization Represented**
- 3PEA Technologies, Inc.
- ACI Worldwide
- American Bankers Association
- American Express Company
- American Financial Services Association
- Bank of America
- Capital One
- Certicom Corporation
- Citigroup, Inc.
- Deluxe Corporation
- DeLap, White, Caldwell and Croy, LLP
- Diebold, Inc.
- Entrust, Inc.
- Federal Reserve Bank
- Ferris and Associates, Inc.
- Fidelity Investments
- First Data Corporation
- First National Bank of Nebraska, Inc.
- Fiserv
- Futurex
- Hewlett Packard
- Hypercom
- IBM Corporation
- Identrus
- InfoGard Laboratories
- Ingenico
- J.P. Morgan Chase & Co
- KPMG LLP

**Representative**
- Mark Newcomer
- Jim Shaffer
- C. Diane Poole
- Mike Jones
- Mark Zalewski
- Mack Hicks
- Scott Sykes
- Daniel Brown
- Paul Gubiotti
- John Fitzpatrick
- Darlene Kargel
- Bruce Chapa
- Robert Zucherato
- Neil Hersch
- J. Martin Ferris
- Michael Versace
- Gene Kathol
- Lisa Curry
- Bud Beattie
- Jason Anderson
- Larry Hines
- Scott Spiker
- Todd Arnold
- Brandon Brown
- Tom Caddy
- John Sheets
- Edward Koslow
- Alfred F. Van Ranst
Under ASC X9 procedures, a working group may be established to address specific segments of work under the ASC X9 Committee or one of its subcommittees. A working group exists only to develop standard(s) or guideline(s) in a specific area and is then disbanded. The individual experts are listed with their affiliated organizations. However, this does not imply that the organization has approved the content of the standard or guideline. (Note: Per X9 policy, company names of non-member participants are listed only if, at time of publication, the X9 Secretariat received an original signed release permitting such company names to appear in print.)

The X9F1 Cryptographic Tool Standards and Guidelines group that developed this standard had the following members:

Miles Smid, Chairman  
James Randall, Project Editor

**Organization Represented**

<table>
<thead>
<tr>
<th>Organization Represented</th>
<th>Representative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certicom Corporation</td>
<td>Dan Brown</td>
</tr>
<tr>
<td>Communications Security Establishment of Canada</td>
<td>Scott Vanstone</td>
</tr>
<tr>
<td>Entrust</td>
<td>Simon Blake-Wilson</td>
</tr>
<tr>
<td>HP</td>
<td>Mike Chawrun</td>
</tr>
<tr>
<td>IBM Corporation</td>
<td>Don Johnson</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Robert Zuccherato</td>
</tr>
<tr>
<td>Pitney Bowes, Inc.</td>
<td>Susan Langford</td>
</tr>
<tr>
<td>Proofspace</td>
<td>Alan Roginsky</td>
</tr>
<tr>
<td>RSA Security, Inc.</td>
<td>Richard Sweeney</td>
</tr>
<tr>
<td>Surety, Inc.</td>
<td>Stephen Ranzini</td>
</tr>
<tr>
<td>TECSEC Incorporated</td>
<td>Dave Faoro</td>
</tr>
<tr>
<td>Thales e-Security, Inc.</td>
<td>Ron Schultz</td>
</tr>
<tr>
<td>Triton Systems of Delaware, Inc.</td>
<td></td>
</tr>
<tr>
<td>University Bank</td>
<td></td>
</tr>
<tr>
<td>VeriFone, Inc.</td>
<td></td>
</tr>
<tr>
<td>VECTORSgi</td>
<td></td>
</tr>
<tr>
<td>VISA</td>
<td></td>
</tr>
<tr>
<td>Wachovia Bank</td>
<td></td>
</tr>
<tr>
<td>Wells Fargo Bank</td>
<td></td>
</tr>
</tbody>
</table>

This is a preview of "ANSI X9.80:2005". Click here to purchase the full version from the ANSI store.
Business practice has changed with the introduction of computer-based technologies. The substitution of electronic transactions for their paper-based predecessors has reduced costs and improved efficiency. Trillions of dollars in funds and securities are transferred daily by telephone, wire services, and other electronic communication mechanisms. The high value or sheer volume of such transactions within an open environment exposes the financial community and its customers to potentially severe risks from accidental or deliberate alteration, substitution, or destruction of data. This risk is compounded by interconnected networks, and the increased number and sophistication of malicious adversaries.

Some of the conventional “due care” controls used with paper-based transactions are unavailable in electronic transactions. Examples of such controls are safety paper, which protects integrity, and hand-written signatures or embossed seals, which indicate the intent of the originator to be legally bound. In an electronic-based environment, controls must be in place that provide the same degree of assurance and certainty as in a paper environment. The financial community is responding to these needs.

The Accredited Standards Committee on Financial Services (ANSI X9) has developed several sets of standards based on public key cryptography to protect financial information:

  
  Part 1: *The Digital Signature Algorithm (DSA)* and
  
  Part 2: *The Secure Hash Algorithm -1 (SHA-1)*.


This Standard, *Prime Number Generation, Primality Testing, and Primality Certificates*, defines techniques for generating prime numbers that are needed as parameters in public key algorithms.

The use of this Standard, together with appropriate controls, may have considerable legal effect with respect to the apportionment of liability for erroneous or fraudulent transactions and the satisfaction of requirements for transaction
enforceability. The legal implications associated with the use of this Standard may have their origin in both case law
and legislation, including the Uniform Commercial Code Article 4A on Funds Transfers (Article 4A).

The details of Article 4A address (in part) the implementation of commercially reasonable security procedures and the
effect of using such procedures on the apportionment of liability between a customer and a bank. A security
procedure is used by Article 4A-201 "for the purpose of (i) verifying that a payment order is that of the customer, or (ii)
detecting error in the transmission or the content of the payment order or communication." The commercial
reasonableness of a security procedure is determined by the criteria established in Article 4A-201.
Prime Number Generation, Primality Testing, and Primality Certificates

1 Scope

In the current state of the art in public key cryptography, all methods require, in one way or another, the use of prime numbers as parameters to the various algorithms. This document presents a set of accepted techniques for generating primes.

It is intended that ASC X9 standards that require the use of primes will refer to this document, rather than trying to define these techniques on a case-by-case basis. Standards, as they exist today, may differ in the methods they use for parameter generation from those specified in this document. It is anticipated that as each existing ASC X9 standard comes up for its 5-year review, it will be modified to reference this document instead of specifying its own techniques for generating primes.

This standard defines methods for generating large prime numbers as needed by public key cryptographic algorithms. It also provides testing methods for testing candidate primes presented by a third party.

This standard allows primes to be generated either deterministically or probabilistically, where:

— A number shall be accepted as prime when a probabilistic algorithm that declares it to be prime is in error with probability less than $2^{-100}$.

— A deterministic prime shall be generated using a method that guarantees that it is prime.

In addition to algorithms for generating primes, this standard also presents primality certificates for some of the algorithms where it is feasible to do so. The syntax for such certificates is beyond the scope of this document. Primality certificates are never required by this standard. Primality certificates are not needed when a prime is generated and kept in a secure environment that is managed by the party that generated the prime.

A requirement placed upon the use of this standard, but out of scope, is as follows:

— When a random or pseudo-random number generator is used to generate prime numbers, an ANSI approved random number (or bit) generator (i.e., one that is specified in an ANSI X9 standard) shall be used. This requirement is necessary to ensure security.

NOTE—The $2^{-100}$ failure probability is selected to be sufficiently small that errors are extremely unlikely ever to occur in normal practice. Moreover, even if an error were to occur when one party tests a prime, subsequent tests by the same or other parties would detect the error with overwhelming probability. Furthermore, the $2^{-100}$ probability is an upper bound on the worst-case probability that a test declares any non-prime candidate to be prime; not all non-primes may reach this bound, and the probability that a non-prime generated at random passes such a test is much lower. Accordingly, the $2^{-100}$ bound is considered appropriate independent of the size of the prime being generated and the intended security level of the cryptosystem in which the prime is to be employed. For high-assurance applications, however, the deterministic methods may nevertheless be preferable.