

Network Working Group
Internet-Draft
Intended status: Informational
Expires: 24 August 2022

P. Gutmann
University of Auckland
20 February 2022

Standard PKC Test Keys
draft-gutmann-testkeys-00

Abstract

This document provides a set of standard PKC test keys that may be used wherever pre-generated keys and associated operations like digital signatures are required. Like the EICAR virus test file, these widely-known test keys can be detected and recognised by applications consuming them as being purely for testing purposes without assigning any security properties to them.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 24 August 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

Internet-Draft

TestKeys

February 2022

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10, 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1.	Introduction	2
1.1.	Conventions Used in This Document	3
2.	Widely-known Test Keys	3
2.1.	RSA Keys	3
2.2.	DLP Keys	15
2.3.	ECDLP Keys	24
3.	Contributors/Acknowledgements	26
4.	IANA Considerations	26
5.	Security Considerations	26
6.	Normative References	27
	Author's Address	27

[1.](#) Introduction

The widespread use of PKCs on the Internet has led to a proliferation of publicly-known but not necessarily acknowledged keys used for testing purposes or that ship preconfigured in applications. These keys provide no security, but since there's no record of them it's often not known that they provide no security. In order to address this issue, this document provides a set of widely-known test keys that may be used wherever a preconfigured or sample key is required, and by extension in situations where such keys may be used such as when testing digitally signed data.

The keys provided cover three major algorithm families, RSA, DLP-based algorithms such as DSA, DH, and Elgamal, and ECDLP-based algorithms such as ECDSA and ECDH. Although some of the algorithms and key sizes are no longer recommended, keys corresponding to those algorithms and key sizes are provided in order to accommodate the

large installed based of existing implementations that use them.

[1.1.](#) Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [\[RFC2119\]](#) and [\[RFC8174\]](#) when, and only when, they appear in all capitals, as shown here.

[2.](#) Widely-known Test Keys

This section provides the test keys for the algorithm groups in various sizes in a C-like notation that may be directly used in crypto code written in C- like languages such as C, C++, Java, JavaScript, Go, Swift, and Rust, covering the majority of languages likely to be used to implement crypto code.

Each element of the key is given in a form consisting of a count in bits followed by a byte string containing that key element in little-endian form. For example for the RSA p value it might be:

Sample key component

```
/* p */
512,
{ 0xCF, 0xDA, 0xF9, 0x99, 0x6F, 0x05, 0x95, 0x84,
  0x09, 0x90, 0xB3, 0xAB, 0x39, 0xB7, 0xDD, 0x1D,
  [...],
  0xE1, 0x2C, 0x0D, 0xF7, 0x30, 0xE2, 0xB8, 0x09,
  0x73, 0x50, 0x28, 0xF6, 0x55, 0x85, 0x57, 0x03 },
```

where 0xCF is the least-significant byte of the RSA p value and 0x03 is the most-significant byte of the value.

[2.1.](#) RSA Keys

The following widely-known test keys may be used for RSA.

RSA-1024 key

```
/* n */
1024,
{ 0xB0, 0xD1, 0x83, 0x52, 0xA8, 0x8F, 0x53, 0xD5,
  0x51, 0x6F, 0x46, 0xC2, 0x0E, 0x7A, 0x36, 0x7D,
  0x7D, 0xE8, 0x8A, 0xCF, 0x54, 0xA0, 0x19, 0xF6,
  0xDE, 0xF5, 0x7A, 0xB9, 0xB4, 0x4C, 0xED, 0xDB,
  0x22, 0x42, 0xB1, 0xBC, 0xA0, 0xFB, 0x1B, 0x5C,
  0xB8, 0x2B, 0x30, 0x36, 0x17, 0x6A, 0x63, 0x90,
  0x35, 0x64, 0xDE, 0xC6, 0xEB, 0x41, 0xDB, 0x2F,
```

Gutmann

Expires 24 August 2022

[Page 3]

Internet-Draft

TestKeys

February 2022

```
  0x8F, 0xC7, 0x87, 0xF4, 0xE5, 0x2E, 0x11, 0x49,
  0xE3, 0x33, 0x47, 0x57, 0x29, 0x73, 0xF6, 0x60,
  0xC3, 0xC7, 0x7C, 0xA9, 0xE0, 0x82, 0x1C, 0x2B,
  0x69, 0x5B, 0xE7, 0xAE, 0x9D, 0x7D, 0x30, 0xF4,
  0x07, 0x91, 0x10, 0xF4, 0x8A, 0xAE, 0x6F, 0x8B,
  0x70, 0x2D, 0x47, 0x4B, 0x29, 0x00, 0x81, 0x7F,
  0x28, 0x66, 0x24, 0x9B, 0xEC, 0x12, 0xA2, 0xB1,
  0x9B, 0x82, 0x78, 0x41, 0x68, 0x08, 0xF8, 0x1A,
  0xE1, 0xFC, 0xF9, 0xB7, 0x77, 0x8A, 0x62, 0x3F },
/* e */
17,
{ 0x01, 0x00, 0x01 },
/* d */
1023,
{ 0x48, 0x2E, 0x9F, 0x8F, 0xA4, 0xE4, 0x2D, 0xF3,
  0x0D, 0x75, 0x81, 0xCB, 0x42, 0xA1, 0xBD, 0x90,
  0xE9, 0x4F, 0x7F, 0x2B, 0x38, 0x7E, 0xCB, 0x5A,
  0xAE, 0x96, 0x43, 0xED, 0x7F, 0x9F, 0x50, 0x12,
  0x7F, 0x1F, 0xFE, 0xF2, 0xE4, 0x3C, 0xDE, 0x64,
  0xB1, 0x82, 0x60, 0x02, 0x14, 0xF9, 0x07, 0x80,
  0x1D, 0x6B, 0xFA, 0x4D, 0xF6, 0x48, 0x42, 0x34,
  0x5E, 0x5B, 0xB4, 0x32, 0xD3, 0x44, 0x45, 0x25,
  0xD8, 0x30, 0x16, 0x54, 0xC5, 0x44, 0x2B, 0x0A,
  0x5E, 0x11, 0xB9, 0xC7, 0xE2, 0x01, 0xFA, 0x32,
  0xF4, 0x1A, 0xBA, 0xF4, 0xF0, 0xA6, 0xE0, 0x3C,
  0xF0, 0xE0, 0xCB, 0x82, 0x66, 0xC6, 0x2A, 0xD1,
  0x1D, 0x95, 0x6D, 0x53, 0xC9, 0x46, 0x6E, 0x48,
  0x99, 0x5F, 0xEA, 0x26, 0x0C, 0x85, 0x36, 0xF0,
  0x41, 0xCB, 0x35, 0x62, 0xFA, 0xAC, 0x51, 0x1C,
```

```

    0x4D, 0x66, 0xA8, 0xFE, 0xD1, 0x11, 0xB2, 0x91 },
/* p */
512,
{ 0xE9, 0xD8, 0x6E, 0x4D, 0xC3, 0x4A, 0x98, 0x5A,
  0x7E, 0xC7, 0x5A, 0x6F, 0x54, 0xA7, 0x5C, 0xE4,
  0x51, 0x39, 0xE4, 0x52, 0x40, 0xB3, 0x86, 0xAB,
  0x71, 0x1D, 0xB7, 0x91, 0xBC, 0xD9, 0x87, 0x18,
  0xA1, 0x3B, 0xAF, 0x21, 0x8C, 0x24, 0x49, 0x36,
  0x46, 0x68, 0x07, 0x56, 0xCB, 0x50, 0xA6, 0xCB,
  0xEE, 0x15, 0x8E, 0x25, 0x21, 0x44, 0x99, 0x12,
  0x30, 0x1C, 0x0D, 0x41, 0x49, 0x11, 0x18, 0x45 },
/* q */
512,
{ 0xC1, 0x91, 0xFA, 0x3B, 0x55, 0x0B, 0x39, 0x1A,
  0x7C, 0xB0, 0x72, 0x83, 0x76, 0x27, 0x72, 0x95,
  0xE6, 0x1C, 0x65, 0x4F, 0x0B, 0xEF, 0x2F, 0x58,
  0xDC, 0xE5, 0xC9, 0x62, 0xA1, 0x0B, 0x7D, 0xD7,
  0x5F, 0x06, 0x01, 0x54, 0x65, 0xE5, 0x50, 0x76,
  0xE4, 0x66, 0x26, 0x3E, 0xEB, 0xCA, 0xED, 0x20,

```

```

    0xD2, 0xEB, 0xAB, 0x39, 0x31, 0x3E, 0x8B, 0xC5,
    0x67, 0x32, 0x0F, 0xE8, 0xB2, 0xDC, 0x62, 0xB3 },
/* u */
512,
{ 0xB9, 0x9D, 0x7F, 0x8F, 0x4D, 0x4D, 0x45, 0x5F,
  0x1F, 0xBA, 0x46, 0x2D, 0x99, 0x0A, 0x2E, 0x84,
  0x8C, 0x42, 0x8C, 0x1E, 0xBE, 0xE0, 0x1D, 0xC0,
  0x01, 0x84, 0xC8, 0xA7, 0x65, 0x83, 0xAD, 0x37,
  0x9F, 0x69, 0xAD, 0xAF, 0x54, 0x75, 0x54, 0x30,
  0xF6, 0x3C, 0x42, 0x53, 0xD1, 0xBB, 0x78, 0xCC,
  0x9B, 0xD2, 0x32, 0x64, 0x34, 0x00, 0x80, 0xB8,
  0x4C, 0x1A, 0x91, 0x7D, 0xE0, 0x8B, 0x6E, 0xDB },
/* exponent1 */
512,
{ 0xE7, 0x3A, 0xE0, 0x37, 0x7C, 0xB8, 0xB2, 0x56,
  0x29, 0xAE, 0xAE, 0xBA, 0x0F, 0x97, 0x3E, 0xBF,
  0x75, 0xA2, 0x2D, 0x27, 0x38, 0x5B, 0x4C, 0xFB,
  0x11, 0xEB, 0x34, 0xAD, 0xA3, 0x73, 0xE5, 0xA6,
  0x71, 0x28, 0x37, 0x50, 0x90, 0xE7, 0x00, 0x8D,
  0xEE, 0xA8, 0xC7, 0x39, 0x07, 0xEA, 0x44, 0x44,
  0xBA, 0xB4, 0x0D, 0xCE, 0xA1, 0x4A, 0xD7, 0xA1,
  0xA8, 0x78, 0xD4, 0x92, 0x8D, 0xD1, 0x9D, 0x91 },

```

```

/* exponent2 */
511,
{ 0x41, 0x99, 0x79, 0x16, 0x16, 0x72, 0x21, 0x3E,
  0x0A, 0xB7, 0xB9, 0x77, 0x37, 0xD9, 0x92, 0x89,
  0x9E, 0x5C, 0x4D, 0x31, 0x06, 0xB8, 0x5E, 0x71,
  0x5D, 0x1B, 0x3A, 0xAE, 0x84, 0x29, 0x62, 0xD2,
  0x54, 0x4F, 0xB2, 0xAF, 0xA9, 0x80, 0x97, 0x4E,
  0x53, 0x85, 0x12, 0xBD, 0x0C, 0x27, 0xCF, 0x48,
  0xEA, 0x72, 0x17, 0xAA, 0xE0, 0x37, 0x74, 0x22,
  0xC8, 0x20, 0x3D, 0x27, 0xFD, 0x45, 0x96, 0xE5 }

```

RSA-2048 key

```

/* n */
2048,
{ 0xB0, 0xF9, 0xE8, 0x19, 0x43, 0xA7, 0xAE, 0x98,
  0x92, 0xAA, 0xDE, 0x17, 0xCA, 0x7C, 0x40, 0xF8,
  0x74, 0x4F, 0xED, 0x2F, 0x81, 0x48, 0xE6, 0xC8,
  0xEA, 0xA2, 0x7B, 0x7D, 0x00, 0x15, 0x48, 0xFB,
  0x51, 0x92, 0xAB, 0x28, 0xB5, 0x6C, 0x50, 0x60,
  0xB1, 0x18, 0xCC, 0xD1, 0x31, 0xE5, 0x94, 0x87,
  0x4C, 0x6C, 0xA9, 0x89, 0xB5, 0x6C, 0x27, 0x29,
  0x6F, 0x09, 0xFB, 0x93, 0xA0, 0x34, 0xDF, 0x32,
  0xE9, 0x7C, 0x6F, 0xF0, 0x99, 0x8C, 0xFD, 0x8E,
  0x6F, 0x42, 0xDD, 0xA5, 0x8A, 0xCD, 0x1F, 0xA9,

```

```

0x79, 0x86, 0xF1, 0x44, 0xF3, 0xD1, 0x54, 0xD6,
0x76, 0x50, 0x17, 0x5E, 0x68, 0x54, 0xB3, 0xA9,
0x52, 0x00, 0x3B, 0xC0, 0x68, 0x87, 0xB8, 0x45,
0x5A, 0xC2, 0xB1, 0x9F, 0x7B, 0x2F, 0x76, 0x50,
0x4E, 0xBC, 0x98, 0xEC, 0x94, 0x55, 0x71, 0xB0,
0x78, 0x92, 0x15, 0x0D, 0xDC, 0x6A, 0x74, 0xCA,
0x0F, 0xBC, 0xD3, 0x54, 0x97, 0xCE, 0x81, 0x53,
0x4D, 0xAF, 0x94, 0x18, 0x84, 0x4B, 0x13, 0xAE,
0xA3, 0x1F, 0x9D, 0x5A, 0x6B, 0x95, 0x57, 0xBB,
0xDF, 0x61, 0x9E, 0xFD, 0x4E, 0x88, 0x7F, 0x2D,
0x42, 0xB8, 0xDD, 0x8B, 0xC9, 0x87, 0xEA, 0xE1,
0xBF, 0x89, 0xCA, 0xB8, 0x5E, 0xE2, 0x1E, 0x35,
0x63, 0x05, 0xDF, 0x6C, 0x07, 0xA8, 0x83, 0x8E,
0x3E, 0xF4, 0x1C, 0x59, 0x5D, 0xCC, 0xE4, 0x3D,
0xAF, 0xC4, 0x91, 0x23, 0xEF, 0x4D, 0x8A, 0xBB,

```

```

0xA9, 0x3D, 0x39, 0x05, 0xE4, 0x02, 0x8D, 0x7B,
0xA9, 0x14, 0x84, 0xA2, 0x75, 0x96, 0xE0, 0x7B,
0x4B, 0x6E, 0xD9, 0x92, 0xF0, 0x77, 0xB5, 0x24,
0xD3, 0xDC, 0xFE, 0x7D, 0xDD, 0x55, 0x49, 0xBE,
0x7C, 0xCE, 0x8D, 0xA0, 0x35, 0xCF, 0xA0, 0xB3,
0xFB, 0x8F, 0x9E, 0x46, 0xF7, 0x32, 0xB2, 0xA8,
0x6B, 0x46, 0x01, 0x65, 0xC0, 0x8F, 0x53, 0x13 },
/* e */
17,
{ 0x01, 0x00, 0x01 },
/* d */
2047,
{ 0x41, 0x18, 0x8B, 0x20, 0xCF, 0xDB, 0xDB, 0xC2,
0xCF, 0x1F, 0xFE, 0x75, 0x2D, 0xCB, 0xAA, 0x72,
0x39, 0x06, 0x35, 0x2E, 0x26, 0x15, 0xD4, 0x9D,
0xCE, 0x80, 0x59, 0x7F, 0xCF, 0x0A, 0x05, 0x40,
0x3B, 0xEF, 0x00, 0xFA, 0x06, 0x51, 0x82, 0xF7,
0x2D, 0xEC, 0xFB, 0x59, 0x6F, 0x4B, 0x0C, 0xE8,
0xFF, 0x59, 0x70, 0xBA, 0xF0, 0x7A, 0x89, 0xA5,
0x19, 0xEC, 0xC8, 0x16, 0xB2, 0xF4, 0xFF, 0xAC,
0x50, 0x69, 0xAF, 0x1B, 0x06, 0xBF, 0xEF, 0x7B,
0xF6, 0xBC, 0xD7, 0x9E, 0x4E, 0x81, 0xC8, 0xC5,
0xA3, 0xA7, 0xD9, 0x13, 0x0D, 0xC3, 0xCF, 0xBA,
0xDA, 0xE5, 0xF6, 0xD2, 0x88, 0xF9, 0xAE, 0xE3,
0xF6, 0xFF, 0x92, 0xFA, 0xE0, 0xF8, 0x1A, 0xF5,
0x97, 0xBE, 0xC9, 0x6A, 0xE9, 0xFA, 0xB9, 0x40,
0x2C, 0xD5, 0xFE, 0x41, 0xF7, 0x05, 0xBE, 0xBD,
0xB4, 0x7B, 0xB7, 0x36, 0xD3, 0xFE, 0x6C, 0x5A,
0x51, 0xE0, 0xE2, 0x07, 0x32, 0xA9, 0x7B, 0x5E,
0x46, 0xC1, 0xCB, 0xDB, 0x26, 0xD7, 0x48, 0x54,
0xC6, 0xB6, 0x60, 0x4A, 0xED, 0x46, 0x37, 0x35,
0xFF, 0x90, 0x76, 0x04, 0x65, 0x57, 0xCA, 0xF9,
0x49, 0xBF, 0x44, 0x88, 0x95, 0xC2, 0x04, 0x32,

```

```

0xC1, 0xE0, 0x9C, 0x01, 0x4E, 0xA7, 0x56, 0x60,
0x43, 0x4F, 0x1A, 0x0F, 0x3B, 0xE2, 0x94, 0xBA,
0xBC, 0x5D, 0x53, 0x0E, 0x6A, 0x10, 0x21, 0x3F,
0x53, 0xB6, 0x03, 0x75, 0xFC, 0x84, 0xA7, 0x57,
0x3F, 0x2A, 0xF1, 0x21, 0x55, 0x84, 0xF5, 0xB4,
0xBD, 0xA6, 0xD4, 0xE8, 0xF9, 0xE1, 0x7A, 0x78,
0xD9, 0x7E, 0x77, 0xB8, 0x6D, 0xA4, 0xA1, 0x84,
0x64, 0x75, 0x31, 0x8A, 0x7A, 0x10, 0xA5, 0x61,

```

```

    0x01, 0x4E, 0xFF, 0xA2, 0x3A, 0x81, 0xEC, 0x56,
    0xE9, 0xE4, 0x10, 0x9D, 0xEF, 0x8C, 0xB3, 0xF7,
    0x97, 0x22, 0x3F, 0x7D, 0x8D, 0x0D, 0x43, 0x51 },
/* p */
1024,
{ 0xDD, 0x10, 0x57, 0x02, 0x38, 0x2F, 0x23, 0x2B,
  0x36, 0x81, 0xF5, 0x37, 0x91, 0xE2, 0x26, 0x17,
  0xC7, 0xBF, 0x4E, 0x9A, 0xCB, 0x81, 0xED, 0x48,
  0xDA, 0xF6, 0xD6, 0x99, 0x5D, 0xA3, 0xEA, 0xB6,
  0x42, 0x83, 0x9A, 0xFF, 0x01, 0x2D, 0x2E, 0xA6,
  0x28, 0xB9, 0x0A, 0xF2, 0x79, 0xFD, 0x3E, 0x6F,
  0x7C, 0x93, 0xCD, 0x80, 0xF0, 0x72, 0xF0, 0x1F,
  0xF2, 0x44, 0x3B, 0x3E, 0xE8, 0xF2, 0x4E, 0xD4,
  0x69, 0xA7, 0x96, 0x13, 0xA4, 0x1B, 0xD2, 0x40,
  0x20, 0xF9, 0x2F, 0xD1, 0x10, 0x59, 0xBD, 0x1D,
  0x0F, 0x30, 0x1B, 0x5B, 0xA7, 0xA9, 0xD3, 0x63,
  0x7C, 0xA8, 0xD6, 0x5C, 0x1A, 0x98, 0x15, 0x41,
  0x7D, 0x8E, 0xAB, 0x73, 0x4B, 0x0B, 0x4F, 0x3A,
  0x2C, 0x66, 0x1D, 0x9A, 0x1A, 0x82, 0xF3, 0xAC,
  0x73, 0x4C, 0x40, 0x53, 0x06, 0x69, 0xAB, 0x8E,
  0x47, 0x30, 0x45, 0xA5, 0x8E, 0x65, 0x53, 0x9D },
/* q */
1024,
{ 0xCC, 0xF1, 0xE5, 0xBB, 0x90, 0xC8, 0xE9, 0x78,
  0x1E, 0xA7, 0x5B, 0xEB, 0xF1, 0x0B, 0xC2, 0x52,
  0xE1, 0x1E, 0xB0, 0x23, 0xA0, 0x26, 0x0F, 0x18,
  0x87, 0x55, 0x2A, 0x56, 0x86, 0x3F, 0x4A, 0x64,
  0x21, 0xE8, 0xC6, 0x00, 0xBF, 0x52, 0x3D, 0x6C,
  0xB1, 0xB0, 0xAD, 0xBD, 0xD6, 0x5B, 0xFE, 0xE4,
  0xA8, 0x8A, 0x03, 0x7E, 0x3D, 0x1A, 0x41, 0x5E,
  0x5B, 0xB9, 0x56, 0x48, 0xDA, 0x5A, 0x0C, 0xA2,
  0x6B, 0x54, 0xF4, 0xA6, 0x39, 0x48, 0x52, 0x2C,
  0x3D, 0x5F, 0x89, 0xB9, 0x4A, 0x72, 0xEF, 0xFF,
  0x95, 0x13, 0x4D, 0x59, 0x40, 0xCE, 0x45, 0x75,
  0x8F, 0x30, 0x89, 0x80, 0x90, 0x89, 0x56, 0x58,
  0x8E, 0xEF, 0x57, 0x5B, 0x3E, 0x4B, 0xC4, 0xC3,
  0x68, 0xCF, 0xE8, 0x13, 0xEE, 0x9C, 0x25, 0x2C,
  0x2B, 0x02, 0xE0, 0xDF, 0x91, 0xF1, 0xAA, 0x01,
  0x93, 0x8D, 0x38, 0x68, 0x5D, 0x60, 0xBA, 0x6F },
/* u */

```



```

{ 0x0A, 0x81, 0xD8, 0xA6, 0x18, 0x31, 0x4A, 0x80,
  0x3A, 0xF6, 0x1C, 0x06, 0x71, 0x1F, 0x2C, 0x39,
  0xB2, 0x66, 0xFF, 0x41, 0x4D, 0x53, 0x47, 0x6D,
  0x1D, 0xA5, 0x2A, 0x43, 0x18, 0xAA, 0xFE, 0x4B,
  0x96, 0xF0, 0xDA, 0x07, 0x15, 0x5F, 0x8A, 0x51,
  0x34, 0xDA, 0xB8, 0x8E, 0xE2, 0x9E, 0x81, 0x68,
  0x07, 0x6F, 0xCD, 0x78, 0xCA, 0x79, 0x1A, 0xC6,
  0x34, 0x42, 0xA8, 0x1C, 0xD0, 0x69, 0x39, 0x27,
  0xD8, 0x08, 0xE3, 0x35, 0xE8, 0xD8, 0xCB, 0xF2,
  0x12, 0x19, 0x07, 0x50, 0x9A, 0x57, 0x75, 0x9B,
  0x4F, 0x9A, 0x18, 0xFA, 0x3A, 0x7B, 0x33, 0x37,
  0x79, 0xED, 0xDE, 0x7A, 0x45, 0x93, 0x84, 0xF8,
  0x44, 0x4A, 0xDA, 0xEC, 0xFF, 0xEC, 0x95, 0xFD,
  0x55, 0x2B, 0x0C, 0xFC, 0xB6, 0xC7, 0xF6, 0x92,
  0x62, 0x6D, 0xDE, 0x1E, 0xF2, 0x68, 0xA4, 0x0D,
  0x2F, 0x67, 0xB5, 0xC8, 0xAA, 0x38, 0x7F, 0xF7 },
/* exponent1 */
1020,
{ 0x09, 0xED, 0x54, 0xEA, 0xED, 0x98, 0xF8, 0x4C,
  0x55, 0x7B, 0x4A, 0x86, 0xBF, 0x4F, 0x57, 0x84,
  0x93, 0xDC, 0xBC, 0x6B, 0xE9, 0x1D, 0xA1, 0x89,
  0x37, 0x04, 0x04, 0xA9, 0x08, 0x72, 0x76, 0xF4,
  0xCE, 0x51, 0xD8, 0xA1, 0x00, 0xED, 0x85, 0x7D,
  0xC2, 0xB0, 0x64, 0x94, 0x74, 0xF3, 0xF1, 0x5C,
  0xD2, 0x4C, 0x54, 0xDB, 0x28, 0x71, 0x10, 0xE5,
  0x6E, 0x5C, 0xB0, 0x08, 0x68, 0x2F, 0x91, 0x68,
  0xAA, 0x81, 0xF3, 0x14, 0x58, 0xB7, 0x43, 0x1E,
  0xCC, 0x1C, 0x44, 0x90, 0x6F, 0xDA, 0x87, 0xCA,
  0x89, 0x47, 0x10, 0xC3, 0x71, 0xE9, 0x07, 0x6C,
  0x1D, 0x49, 0xFB, 0xAE, 0x51, 0x27, 0x69, 0x34,
  0xF2, 0xAD, 0x78, 0x77, 0x89, 0xF4, 0x2D, 0x0F,
  0xA0, 0xB4, 0xC9, 0x39, 0x85, 0x5D, 0x42, 0x12,
  0x09, 0x6F, 0x70, 0x28, 0x0A, 0x4E, 0xAE, 0x7C,
  0x8A, 0x27, 0xD9, 0xC8, 0xD0, 0x77, 0x2E, 0x65 },
/* exponent2 */
1024,
{ 0x8C, 0xB6, 0x85, 0x7A, 0x7B, 0xD5, 0x46, 0x5F,
  0x80, 0x04, 0x7E, 0x9B, 0x87, 0xBC, 0x00, 0x27,
  0x31, 0x84, 0x05, 0x81, 0xE0, 0x62, 0x61, 0x39,
  0x01, 0x2A, 0x5B, 0x50, 0x5F, 0x0A, 0x33, 0x84,
  0x7E, 0xB7, 0xB8, 0xC3, 0x28, 0x99, 0x49, 0xAD,
  0x48, 0x6F, 0x3B, 0x4B, 0x3D, 0x53, 0x9A, 0xB5,
  0xDA, 0x76, 0x30, 0x21, 0xCB, 0xC8, 0x2C, 0x1B,
  0xA2, 0x34, 0xA5, 0x66, 0x8D, 0xED, 0x08, 0x01,
  0xB8, 0x59, 0xF3, 0x43, 0xF1, 0xCE, 0x93, 0x04,
  0xE6, 0xFA, 0xA2, 0xB0, 0x02, 0xCA, 0xD9, 0xB7,
  0x8C, 0xDE, 0x5C, 0xDC, 0x2C, 0x1F, 0xB4, 0x17,

```

```
0x1C, 0x42, 0x42, 0x16, 0x70, 0xA6, 0xAB, 0x0F,  
0x50, 0xCC, 0x4A, 0x19, 0x4E, 0xB3, 0x6D, 0x1C,  
0x91, 0xE9, 0x35, 0xBA, 0x01, 0xB9, 0x59, 0xD8,  
0x72, 0x8B, 0x9E, 0x64, 0x42, 0x6B, 0x3F, 0xC3,  
0xA7, 0x50, 0x6D, 0xEB, 0x52, 0x39, 0xA8, 0xA7 }
```

RSA-4096 key

```
/* n */  
4096,  
{ 0xB3, 0x8B, 0x49, 0x60, 0xE6, 0x3B, 0xE6, 0xA8,  
  0xDB, 0xA8, 0x9A, 0x82, 0x97, 0x8E, 0xF1, 0xF6,  
  0x32, 0x44, 0xE5, 0x57, 0x7D, 0x8C, 0xF5, 0x86,  
  0x16, 0xD5, 0xCA, 0x57, 0x59, 0xD4, 0x9C, 0xC8,  
  0xD9, 0x36, 0xC3, 0x38, 0xAA, 0x3C, 0xB9, 0xB1,  
  0x11, 0xC1, 0x49, 0x7E, 0x5B, 0x51, 0xAF, 0x69,  
  0x2F, 0x26, 0x11, 0xE6, 0x89, 0xF7, 0x67, 0x54,  
  0x80, 0xC0, 0xB0, 0xF4, 0xC3, 0x65, 0x4F, 0x43,  
  0xAF, 0x85, 0xFE, 0x8C, 0x8A, 0xD7, 0x34, 0xE0,  
  0x42, 0xA8, 0xAD, 0xA0, 0x5F, 0xD7, 0x65, 0x08,  
  0xE0, 0x0B, 0xA0, 0xF7, 0x56, 0xC3, 0x44, 0x3B,  
  0xBE, 0x83, 0x3E, 0xA7, 0xD1, 0x00, 0xD4, 0xFB,  
  0x36, 0x7E, 0xEB, 0xD6, 0x0B, 0xDB, 0x64, 0x86,  
  0x77, 0xFC, 0x7D, 0xEB, 0x94, 0x24, 0x4D, 0xAD,  
  0x1A, 0xF8, 0xEE, 0xD1, 0xC6, 0x58, 0x12, 0xC0,  
  0x3E, 0x7C, 0x73, 0xF7, 0xF3, 0x58, 0xE9, 0x41,  
  0xBC, 0x66, 0x45, 0x8F, 0xF7, 0xBB, 0x97, 0xA4,  
  0x9A, 0x98, 0xA1, 0x18, 0x07, 0xE0, 0x2C, 0x1A,  
  0x3B, 0x9A, 0xD3, 0x3A, 0x57, 0x3A, 0xE1, 0x80,  
  0xE1, 0xFF, 0x43, 0x2A, 0xE5, 0x58, 0x0C, 0xC9,  
  0xCA, 0xBF, 0xAB, 0x60, 0x2F, 0x32, 0x5B, 0xCD,  
  0xA0, 0x97, 0xE8, 0x7B, 0xC7, 0xA6, 0xD7, 0x4E,  
  0x34, 0xA8, 0x7D, 0x60, 0x8A, 0x43, 0xFE, 0xB2,  
  0xE4, 0xFF, 0xF1, 0xF4, 0xB8, 0xE7, 0x68, 0x6A,  
  0x98, 0x47, 0x5D, 0xB5, 0x1A, 0x6E, 0xBD, 0x08,  
  0x17, 0x2A, 0x57, 0x41, 0x77, 0x49, 0x24, 0x8B,  
  0x21, 0x55, 0xC8, 0xB9, 0x06, 0xE0, 0xD5, 0x40,  
  0xE8, 0xCB, 0x28, 0xF4, 0xC0, 0x0A, 0xDC, 0x9F,  
  0xE4, 0x75, 0x8A, 0x1A, 0xC3, 0x64, 0xAB, 0x39,  
  0xE4, 0xE1, 0x55, 0x28, 0x98, 0x54, 0x44, 0x15,  
  0x3F, 0xEE, 0xC6, 0xAD, 0x4C, 0x53, 0x48, 0xB2,  
  0xE3, 0x8F, 0xF5, 0x50, 0xF5, 0xFA, 0x58, 0x33,  
  0x97, 0x93, 0x37, 0x30, 0xC8, 0x08, 0x81, 0xBF,  
  0x11, 0xEE, 0xE8, 0xFE, 0x38, 0x6D, 0x5B, 0x51,  
  0x28, 0x49, 0xA9, 0x83, 0x99, 0x43, 0xAB, 0xF3,
```

0xD9, 0x72, 0x20, 0x76, 0x97, 0xB8, 0xEC, 0x24,
0x11, 0xA2, 0x61, 0x9D, 0x55, 0xCA, 0x04, 0x23,

Internet-Draft

TestKeys

February 2022

```
0x3C, 0x5A, 0x2C, 0xED, 0xC6, 0xF2, 0x86, 0xD8,  
0x29, 0xD0, 0xE8, 0x37, 0x20, 0x7B, 0x76, 0x52,  
0x9A, 0xA2, 0x44, 0x87, 0x21, 0x26, 0x8D, 0xC0,  
0x15, 0x0B, 0xB7, 0xB0, 0x7E, 0x73, 0x31, 0x3A,  
0x71, 0x3E, 0x58, 0x95, 0xBA, 0xAF, 0x3A, 0xDF,  
0xFA, 0x60, 0x39, 0x58, 0xC5, 0x67, 0xF8, 0x5C,  
0xF2, 0x5B, 0x1D, 0x80, 0xA2, 0x77, 0x56, 0xA3,  
0x0D, 0x1A, 0x50, 0xA1, 0xE4, 0x69, 0x8E, 0xDA,  
0x9A, 0x12, 0x2B, 0xB0, 0xAA, 0x7A, 0x60, 0xF7,  
0xCD, 0x22, 0x6C, 0xB1, 0x16, 0x5C, 0xFC, 0xF9,  
0xCA, 0x83, 0x0A, 0x60, 0x6C, 0xC0, 0xFB, 0x14,  
0x87, 0xF2, 0x49, 0xE5, 0xE0, 0xC7, 0x1C, 0x88,  
0x62, 0x6C, 0x57, 0x12, 0x80, 0x81, 0xDE, 0x76,  
0xC1, 0x23, 0x84, 0xB6, 0xD4, 0x48, 0xB6, 0x7F,  
0x0E, 0x71, 0x23, 0xAE, 0xEF, 0x74, 0xA8, 0x85,  
0x96, 0x03, 0x74, 0x75, 0x54, 0x83, 0xF2, 0x90,  
0xA7, 0xDE, 0x66, 0x46, 0x5E, 0x22, 0x7B, 0x2B,  
0x17, 0x31, 0x8F, 0x8A, 0x49, 0x05, 0x2B, 0x01,  
0x45, 0xFB, 0xA2, 0x83, 0x77, 0x2B, 0xC2, 0x9A,  
0x5B, 0x58, 0x12, 0xAC, 0xCE, 0xE3, 0xAB, 0x62,  
0x81, 0x70, 0x19, 0xE5, 0x48, 0x07, 0xF2, 0x88,  
0x97, 0x12, 0xB7, 0xB8, 0xF3, 0x03, 0xBA, 0x5F,  
0xE1, 0x47, 0xF9, 0xC2, 0xF3, 0x43, 0x4A, 0xB7,  
0x03, 0xC1, 0xD9, 0x46, 0x73, 0x43, 0x82, 0xA0,  
0xA3, 0x53, 0xF4, 0xE0, 0xCB, 0xBE, 0xA2, 0x6A,  
0x4B, 0xBF, 0x21, 0xCE, 0x9E, 0xB5, 0xE7, 0x9D,  
0x47, 0x57, 0xD7, 0xDE, 0x02, 0x7F, 0x20, 0xE5 },  
/* e */  
17,  
{ 0x01, 0x00, 0x01 },  
/* d */  
4095,  
{ 0x6A, 0xD1, 0xB0, 0xBB, 0x7C, 0xDF, 0x20, 0x91,  
0x4F, 0xF6, 0x94, 0xCE, 0xA3, 0x7B, 0x01, 0x4B,  
0xD7, 0x86, 0x93, 0xE8, 0x24, 0xA3, 0x4B, 0xA4,  
0x16, 0x4B, 0xE5, 0xD1, 0x68, 0x79, 0x8D, 0x3A,  
0x15, 0xB9, 0x76, 0x16, 0x6D, 0x7A, 0x29, 0x84,  
0x46, 0xAA, 0xF7, 0x9D, 0xBC, 0x98, 0xF1, 0xC2,  
0xA3, 0xB1, 0x83, 0xAE, 0xE4, 0x60, 0x94, 0x52,
```

0x7B, 0x33, 0xA9, 0x54, 0x46, 0x38, 0x2D, 0x1B,
0x78, 0xFF, 0x40, 0x7D, 0xBF, 0x50, 0xE0, 0x7D,
0x98, 0x4B, 0x20, 0xD9, 0xAC, 0x8B, 0xCA, 0xE9,
0xA7, 0xDA, 0x63, 0x4F, 0x24, 0x88, 0x92, 0x3C,
0xF5, 0x50, 0xC2, 0x63, 0x37, 0x7E, 0xC6, 0x38,
0x1B, 0xA9, 0x11, 0x88, 0xCC, 0x8F, 0x1F, 0xD4,
0xBC, 0xE8, 0x34, 0xC6, 0x86, 0xE1, 0xBE, 0x71,
0x01, 0xFE, 0x1E, 0xA0, 0x21, 0xE0, 0x5E, 0x6F,
0x8F, 0xFD, 0x9D, 0x45, 0x64, 0xBB, 0x7E, 0x33,

0x84, 0xF2, 0x57, 0xEA, 0x9A, 0x9A, 0x3A, 0x53,
0x4D, 0x43, 0x07, 0x7C, 0xF3, 0x9A, 0x94, 0xC2,
0x9A, 0xB9, 0xB7, 0x78, 0x1B, 0x53, 0xC5, 0xBC,
0x57, 0x38, 0xF6, 0x6E, 0x3B, 0xFA, 0xD1, 0xC8,
0xF0, 0xDE, 0x6E, 0x08, 0x90, 0xAB, 0xE6, 0x60,
0x85, 0x6E, 0x3B, 0x7C, 0x01, 0x41, 0xAB, 0x11,
0x35, 0x55, 0x15, 0x1A, 0xED, 0xC8, 0x1C, 0x6D,
0xB4, 0xBE, 0xED, 0xE6, 0x0A, 0x68, 0x6B, 0x00,
0x18, 0x4F, 0x45, 0x5A, 0x2D, 0x3A, 0xBB, 0x2E,
0x68, 0x11, 0xE1, 0xCD, 0xEA, 0x39, 0x53, 0x0B,
0x8F, 0xAE, 0xA8, 0xF8, 0x24, 0x36, 0x79, 0xC9,
0xDF, 0x76, 0x97, 0x8C, 0x5E, 0x01, 0x58, 0x57,
0xAC, 0xA5, 0x9D, 0x9F, 0xE4, 0xA6, 0x2D, 0x15,
0x09, 0xAE, 0x62, 0x6A, 0xFF, 0x8E, 0x0A, 0xDF,
0x95, 0xA4, 0xEB, 0x01, 0x49, 0xCA, 0xB7, 0x12,
0xEF, 0x3E, 0xC3, 0xD6, 0x02, 0x32, 0x8A, 0x6C,
0x50, 0x21, 0xBA, 0x1B, 0x35, 0xB8, 0x58, 0x3D,
0x9A, 0x90, 0x40, 0x55, 0x03, 0xF5, 0xFA, 0x0F,
0x42, 0x4C, 0x72, 0x86, 0x23, 0xFC, 0x81, 0xD3,
0xDD, 0x7B, 0xFF, 0x1B, 0xF7, 0x8C, 0x8E, 0x2E,
0xBD, 0x03, 0xA5, 0x11, 0x2D, 0xEB, 0x65, 0x89,
0x98, 0x6E, 0x49, 0xBD, 0x30, 0x07, 0x1A, 0xD8,
0x41, 0xA3, 0xCC, 0xA8, 0x07, 0x6C, 0xCF, 0xC7,
0x94, 0x63, 0x30, 0xB1, 0xFD, 0x1C, 0x21, 0x2A,
0xD3, 0xEB, 0xD3, 0x7D, 0x9A, 0x4D, 0x0A, 0x96,
0x95, 0xB8, 0x16, 0x8A, 0x08, 0x89, 0x32, 0x7D,
0x52, 0x6F, 0x16, 0xD1, 0x56, 0x37, 0xFA, 0x9D,
0xBF, 0x04, 0xB0, 0xB8, 0x3D, 0xD8, 0xB5, 0xC4,
0x05, 0x2D, 0xC5, 0x38, 0xB6, 0xCA, 0xE9, 0xC9,
0x2E, 0xC9, 0x70, 0x10, 0x7A, 0x2F, 0x1E, 0xE4,
0xD4, 0x7A, 0x65, 0xCC, 0xA5, 0xB9, 0x59, 0x6E,
0x42, 0x74, 0x91, 0x9B, 0xE7, 0xD1, 0xEC, 0x90,

```
0xE4, 0x50, 0xFE, 0x58, 0x58, 0xDC, 0x2E, 0x01,
0xE8, 0x4E, 0xBD, 0x92, 0x07, 0xD8, 0xEA, 0x20,
0xFA, 0x37, 0x14, 0x0E, 0x89, 0xD0, 0x10, 0xD6,
0x50, 0x1F, 0x22, 0x61, 0x97, 0x18, 0x04, 0xDE,
0x73, 0x68, 0x0F, 0xE6, 0x1C, 0x23, 0x5C, 0x8F,
0x4E, 0x63, 0x1F, 0xF0, 0x6D, 0xBD, 0xEE, 0x66,
0x6D, 0xBB, 0x9A, 0xFB, 0xFD, 0xA3, 0xB9, 0x71,
0xC3, 0x29, 0x0D, 0x7B, 0xDE, 0xF5, 0xC5, 0x78,
0x5A, 0x07, 0x1B, 0xE9, 0x4A, 0xE1, 0x8A, 0x0B,
0x2E, 0xD8, 0xAE, 0x67, 0x9A, 0xBA, 0xA6, 0x10,
0x85, 0x28, 0xA8, 0x5E, 0x31, 0x7F, 0x87, 0xA8,
0x99, 0xC5, 0x89, 0xF4, 0xA8, 0xAD, 0x42, 0x90,
0xA6, 0xCA, 0x1E, 0xF9, 0xF1, 0x4D, 0x8D, 0x0A,
0x7A, 0x66, 0xDC, 0x75, 0x0B, 0x69, 0xB1, 0x9C,
0xB2, 0x58, 0x28, 0xC3, 0xEA, 0xF0, 0x42, 0x21,
0x5C, 0x09, 0xAA, 0xD4, 0xA9, 0x54, 0xE8, 0x55 },
```

```
/* p */
2048,
{ 0xE0, 0x41, 0xBD, 0xF1, 0xC9, 0xB5, 0x69, 0xAC,
  0xF5, 0xE8, 0x02, 0x2D, 0x21, 0x1B, 0x87, 0x1B,
  0x5F, 0x29, 0x21, 0x41, 0xA5, 0x89, 0xFD, 0x0F,
  0x6D, 0xCB, 0x59, 0x47, 0x6B, 0x1C, 0x1D, 0xA4,
  0x01, 0x8D, 0xD7, 0xA1, 0xE1, 0x08, 0x39, 0x32,
  0x74, 0x5E, 0xF3, 0xC6, 0x6C, 0xF7, 0xFF, 0x31,
  0x3E, 0xED, 0x4C, 0xB1, 0x68, 0x1D, 0xEF, 0x9D,
  0x29, 0xCC, 0x3F, 0xE8, 0x7A, 0xF7, 0xAD, 0x19,
  0xE9, 0xEF, 0x34, 0x56, 0x62, 0xC9, 0xC4, 0xF4,
  0xE6, 0xE7, 0x07, 0xAA, 0x4E, 0x99, 0x49, 0x63,
  0x4C, 0x08, 0x64, 0x71, 0xA5, 0x5B, 0x67, 0x46,
  0xC2, 0xAE, 0xEF, 0x87, 0x71, 0xEF, 0x21, 0xA2,
  0xEE, 0x8A, 0xB4, 0xDE, 0xC4, 0xC2, 0x04, 0x3C,
  0x70, 0xCF, 0xBA, 0x89, 0xE5, 0xEB, 0x2F, 0x62,
  0xEA, 0x07, 0xC7, 0x4B, 0xD4, 0x16, 0x67, 0x69,
  0x12, 0xA9, 0x58, 0x9F, 0xB3, 0xED, 0x70, 0x28,
  0x8F, 0x8A, 0x03, 0xD1, 0x91, 0xC5, 0x8A, 0x88,
  0x96, 0xE8, 0xB2, 0x0F, 0x1E, 0xDE, 0x91, 0x80,
  0xCE, 0xD3, 0x03, 0x59, 0xF7, 0x5F, 0x48, 0xAF,
  0xE9, 0x7C, 0x46, 0xEE, 0x59, 0xC9, 0x27, 0x1E,
  0x71, 0x37, 0x55, 0x4A, 0xD7, 0x05, 0x56, 0x17,
  0x84, 0x8F, 0xD3, 0x04, 0x1C, 0xD6, 0x30, 0x47,
  0xF6, 0x46, 0x2C, 0x0E, 0x66, 0xE1, 0x83, 0x9F,
```

```

0x63, 0xC6, 0x12, 0xD4, 0xA3, 0x57, 0xF5, 0xE5,
0x76, 0x35, 0x6A, 0xAA, 0xE7, 0xC6, 0x4A, 0xC0,
0xBF, 0xD9, 0xD6, 0x5E, 0xDF, 0x4B, 0x2F, 0x34,
0xDA, 0xDB, 0xDF, 0x69, 0x06, 0x20, 0xC8, 0x95,
0xCA, 0x44, 0xD9, 0x61, 0xDA, 0x05, 0xB1, 0x36,
0x2B, 0x4A, 0xD5, 0xDA, 0xAC, 0xB9, 0x0F, 0xF5,
0x86, 0x33, 0x5E, 0xCD, 0x7E, 0x1D, 0x7A, 0x16,
0x00, 0xCB, 0x1A, 0xB3, 0x72, 0x69, 0x5B, 0x6E,
0xC7, 0x71, 0x76, 0x21, 0xDB, 0xBE, 0x93, 0x57 },
/* q */
2048,
{ 0xCC, 0xF5, 0x51, 0x29, 0xD3, 0xB9, 0x24, 0xC8,
0x38, 0xA7, 0x6C, 0xD3, 0x69, 0xD4, 0x6E, 0x9C,
0xB8, 0x13, 0xFE, 0x3B, 0x39, 0xBA, 0xF1, 0xEB,
0x10, 0x18, 0x47, 0xD3, 0x1D, 0x09, 0x13, 0x50,
0x03, 0xAB, 0x2F, 0xC2, 0x39, 0x43, 0x1C, 0xDA,
0x6E, 0x99, 0x08, 0x88, 0x3D, 0xE8, 0xA0, 0x54,
0x6E, 0x35, 0x28, 0x37, 0xD4, 0xEB, 0x95, 0xCB,
0x41, 0xD8, 0xEE, 0xC1, 0x4A, 0x66, 0xCD, 0x38,
0xC2, 0x24, 0x7E, 0x82, 0xA3, 0x94, 0x39, 0x29,
0x27, 0xBB, 0xF5, 0x70, 0xA8, 0x65, 0x5E, 0x0F,
0x2A, 0xC2, 0x43, 0xE5, 0xFB, 0x87, 0x6F, 0xD2,
0x0B, 0x48, 0x76, 0x73, 0xA2, 0x77, 0x2D, 0xA9,

```

```

0x70, 0xC1, 0xDF, 0x47, 0xA3, 0x2D, 0xEA, 0x8A,
0x75, 0xE7, 0x09, 0x54, 0x73, 0x22, 0x9C, 0x69,
0x3C, 0x88, 0x6A, 0x31, 0x6D, 0x2C, 0xEC, 0xBF,
0x03, 0x59, 0x7B, 0x04, 0xCA, 0x9E, 0xCA, 0xBD,
0xA3, 0x36, 0x6E, 0x07, 0x64, 0x88, 0x05, 0x9B,
0x24, 0x59, 0x6F, 0x5D, 0xF6, 0xE8, 0x56, 0x97,
0xDB, 0xE6, 0x2A, 0xB2, 0xF8, 0xCC, 0x71, 0xAC,
0x7F, 0x74, 0x3B, 0x64, 0x12, 0x6D, 0x01, 0xF2,
0xB3, 0x61, 0x27, 0x16, 0xEC, 0xA7, 0x69, 0x75,
0xE5, 0x14, 0xED, 0x4D, 0x78, 0xA3, 0x22, 0x90,
0xBE, 0x0A, 0x82, 0xF1, 0x44, 0x14, 0x99, 0x2B,
0xD1, 0x80, 0x3D, 0xAD, 0xC9, 0x83, 0xDD, 0xF2,
0x76, 0xD2, 0xCA, 0xE1, 0xA0, 0xA9, 0x03, 0xF9,
0x1E, 0x78, 0xBE, 0x3C, 0x0B, 0xCA, 0xF5, 0x8F,
0x3C, 0xE9, 0x8D, 0x12, 0x3A, 0xA6, 0xC8, 0x5F,
0x65, 0x51, 0xC5, 0x70, 0x07, 0xFE, 0x47, 0x7A,
0xC8, 0x7E, 0x03, 0x8B, 0x9A, 0x94, 0xAC, 0xC6,
0x20, 0xDE, 0x12, 0x25, 0x81, 0x05, 0x34, 0x4A,

```

```

    0x0C, 0xFB, 0x37, 0x65, 0x50, 0x5E, 0x8E, 0x7E,
    0xC8, 0x6A, 0xC0, 0x86, 0xF6, 0x55, 0x64, 0x23 },
/* u */
2048,
{ 0xD1, 0x0C, 0x91, 0x8D, 0xA9, 0xF2, 0x6D, 0xA9,
  0x4D, 0xFF, 0x3B, 0x09, 0x24, 0x3C, 0x8C, 0xC3,
  0xD4, 0x39, 0x02, 0x6D, 0xE6, 0x2B, 0x9E, 0x9F,
  0x37, 0xAC, 0x60, 0xBB, 0xD7, 0xA9, 0x52, 0xCB,
  0x07, 0x84, 0x94, 0xBD, 0x73, 0x7E, 0xCC, 0x3A,
  0x65, 0x0C, 0x93, 0xC4, 0x2E, 0xD7, 0xF6, 0x49,
  0x02, 0x07, 0xAE, 0x99, 0x6B, 0x3C, 0xD1, 0xFF,
  0x1F, 0x4D, 0x63, 0x9D, 0x61, 0xDD, 0xD1, 0xE7,
  0x12, 0x8D, 0x56, 0x3C, 0x1C, 0x16, 0xC8, 0xB3,
  0x9D, 0x94, 0xD5, 0xDE, 0x5E, 0x93, 0x7F, 0xE6,
  0x5A, 0x38, 0xB8, 0x19, 0xE4, 0x69, 0xF8, 0x8C,
  0x3C, 0xE0, 0x25, 0x21, 0xE2, 0xAD, 0xA9, 0xE3,
  0x46, 0xE6, 0xA1, 0xBD, 0x51, 0x27, 0xC7, 0xBD,
  0xB2, 0x1D, 0xA2, 0xC6, 0x11, 0xE3, 0x5F, 0x6C,
  0x89, 0xE7, 0xDD, 0x66, 0xA0, 0x66, 0xCB, 0x23,
  0x3E, 0xF9, 0x6B, 0xAD, 0x1A, 0xD3, 0x99, 0x94,
  0x0C, 0xAD, 0x05, 0x5A, 0xDF, 0x5C, 0x58, 0x79,
  0xF8, 0x30, 0xA8, 0x08, 0x3C, 0xA6, 0xD6, 0xC0,
  0x58, 0x58, 0xC2, 0x66, 0x03, 0x0A, 0x33, 0xBF,
  0xB4, 0xAD, 0x83, 0xB5, 0xCC, 0x92, 0x9F, 0x2F,
  0x6C, 0xA2, 0x1E, 0x50, 0x29, 0x54, 0x2B, 0x8A,
  0xEB, 0xE7, 0x6B, 0x69, 0x44, 0xE1, 0x86, 0x3E,
  0x39, 0x47, 0x3B, 0x6E, 0xD9, 0xAD, 0x92, 0x6A,
  0x7D, 0xBF, 0xE2, 0xC7, 0x28, 0xE2, 0x3C, 0x74,
  0xF6, 0x9B, 0xB0, 0xE0, 0x54, 0xF1, 0x9F, 0x14,
  0x6C, 0xE1, 0x9E, 0x1D, 0x23, 0x6B, 0x65, 0x34,

```

```

    0x30, 0xA7, 0x1D, 0xC4, 0xA7, 0x4A, 0xE2, 0x0E,
    0x0D, 0x14, 0x13, 0x31, 0x66, 0xA1, 0x8A, 0xDF,
    0x6E, 0xF7, 0xFE, 0xD9, 0x5C, 0xC4, 0x64, 0x35,
    0xFF, 0x4C, 0x96, 0x23, 0x2B, 0xD5, 0x64, 0x03,
    0xCC, 0x39, 0xFB, 0x16, 0xAD, 0xF2, 0x24, 0xB4,
    0xFD, 0xEB, 0x8A, 0xBA, 0xF4, 0x91, 0x31, 0xBF },
/* exponent1 */
2046,
{ 0x2F, 0x7C, 0x1C, 0x31, 0x37, 0x69, 0xCF, 0x6F,
  0x8D, 0x3E, 0x4C, 0x3F, 0xAC, 0x13, 0xFD, 0x1E,
  0xC1, 0x9E, 0x9E, 0xE9, 0x1C, 0x99, 0x44, 0x59,

```

```

0x61, 0x01, 0x3E, 0xED, 0x4D, 0x73, 0xCD, 0x9E,
0xED, 0xA9, 0x50, 0x30, 0x79, 0xCA, 0xD8, 0xF9,
0xA3, 0x04, 0x7C, 0x0F, 0xD7, 0x01, 0x08, 0x2B,
0x30, 0x4C, 0xE5, 0x01, 0x67, 0xAF, 0x77, 0x0E,
0x4B, 0x4C, 0x71, 0x77, 0xD3, 0x99, 0xE0, 0x30,
0x6D, 0x85, 0x76, 0x0A, 0x98, 0xAE, 0x6A, 0xA3,
0x04, 0xC5, 0x84, 0xAC, 0xFE, 0x29, 0x9D, 0x0D,
0x86, 0x8A, 0xFC, 0x61, 0xC8, 0x06, 0xBB, 0xAE,
0x93, 0x08, 0xA1, 0xB5, 0x87, 0x5D, 0x80, 0x3C,
0xD4, 0xCF, 0xD0, 0x0E, 0x9F, 0x91, 0x09, 0x7E,
0x96, 0xD0, 0x95, 0x8A, 0x1F, 0x82, 0x16, 0x2D,
0x96, 0xAA, 0x80, 0xFB, 0xC0, 0x73, 0xE1, 0xFF,
0xB0, 0xB0, 0xE5, 0x10, 0x23, 0xF4, 0x31, 0xDC,
0x94, 0xD0, 0x3F, 0x90, 0xBF, 0x92, 0x19, 0x8C,
0x64, 0x8F, 0xEF, 0x2C, 0x1E, 0x78, 0x38, 0x4D,
0x12, 0xFE, 0x41, 0x66, 0x6A, 0x67, 0xE5, 0xA7,
0x42, 0x04, 0x4B, 0xAC, 0xAA, 0x9C, 0x5A, 0x49,
0x2A, 0xE5, 0xF1, 0x8C, 0x80, 0x4D, 0x23, 0xF6,
0xA4, 0xDE, 0x23, 0x6B, 0x6A, 0x83, 0xBC, 0x03,
0x70, 0xD5, 0x58, 0xFC, 0xCF, 0xB2, 0x0E, 0xC1,
0xD0, 0x49, 0x9F, 0xB1, 0x20, 0xC9, 0x3E, 0x4B,
0x11, 0x25, 0xAC, 0x69, 0x75, 0xDC, 0x59, 0xF5,
0xC8, 0x69, 0xE2, 0xE7, 0x81, 0xD6, 0x94, 0xAF,
0x57, 0x6C, 0x59, 0x39, 0x0E, 0xD0, 0x20, 0x48,
0xFF, 0x64, 0x66, 0xB7, 0x3E, 0x88, 0x18, 0x07,
0x05, 0x51, 0xBA, 0x48, 0xAC, 0x6C, 0x1F, 0x41,
0xF8, 0xE1, 0xA5, 0xC0, 0x53, 0x65, 0x00, 0x75,
0xEA, 0x43, 0x17, 0x6B, 0x49, 0xDD, 0x9F, 0x3B,
0xAC, 0xC5, 0x8C, 0xA3, 0x0C, 0xB9, 0xA4, 0xCF },
/* exponent2 */
2047,
{ 0x57, 0x5A, 0x87, 0x09, 0x28, 0xAF, 0xD4, 0x39,
0x71, 0xCC, 0x09, 0xD9, 0xE1, 0x55, 0x24, 0xFF,
0xAE, 0x84, 0xF6, 0xEA, 0x0F, 0x24, 0xDA, 0x4E,
0xB1, 0x41, 0x67, 0xFB, 0x56, 0x78, 0xB3, 0xBE,
0x7A, 0x91, 0xCF, 0x7D, 0x1C, 0x22, 0xBA, 0x7D,
0x6E, 0x7D, 0xD2, 0xE1, 0x1E, 0x61, 0xB3, 0x53,

```

```

0xC8, 0xD4, 0xE7, 0x1B, 0x44, 0xA8, 0x53, 0xE3,
0x99, 0x60, 0xF8, 0x01, 0x71, 0xD0, 0x76, 0xCF,
0x26, 0x0F, 0x9F, 0xCB, 0xD6, 0x24, 0x2A, 0x68,
0x9C, 0x02, 0xC4, 0x0D, 0x0B, 0xF8, 0x88, 0x2A,

```



```

0x36, 0xB3, 0x2D, 0x75, 0x2B, 0xCB, 0x01, 0xA1,
0xA8, 0x25, 0x6E, 0x36, 0xC2, 0x9B, 0xC0, 0xDE,
0x62, 0xAC, 0x7E, 0x99, 0x6D, 0xB6, 0xF8, 0x2B,
0xA3, 0x2C, 0xA1, 0x11, 0x59, 0x30, 0xFB, 0x30,
0xEF, 0x17, 0xC5, 0x0A, 0xE3, 0xD9, 0x2D, 0xDE,
0x0B, 0x73, 0x6B, 0xB7, 0x13, 0x14, 0xB2, 0x9C,
0x38, 0x9F, 0xCE, 0x2D, 0x60, 0x6F, 0x88, 0xD4,
0x22, 0x9D, 0xEB, 0x95, 0x44, 0xD2, 0xA9, 0x75,
0x77, 0xC7, 0x95, 0x93, 0x49, 0xEE, 0xF8, 0xD3,
0xE8, 0x4E, 0x85, 0xB1, 0x95, 0x18, 0xD8, 0xA7,
0xB4, 0x44, 0x48, 0x00, 0xC1, 0x44, 0x68, 0xF2,
0x52, 0x7C, 0xA4, 0xD7, 0x4B, 0xFF, 0x5B, 0x90,
0x0D, 0x2F, 0x35, 0xB7, 0xD6, 0xA8, 0x60, 0xD0,
0x08, 0x2E, 0x7C, 0x1B, 0x41, 0xB3, 0xEE, 0x38,
0x94, 0xE4, 0x2A, 0x8C, 0x17, 0x89, 0x71, 0xA4,
0x0F, 0x94, 0xAE, 0x9F, 0xB0, 0xF7, 0x03, 0xC9,
0xD4, 0xD0, 0x45, 0xCB, 0xEB, 0x2B, 0x82, 0x63,
0x06, 0x2F, 0xDF, 0xD2, 0x6B, 0xD5, 0xB8, 0x69,
0x60, 0x62, 0x34, 0xE8, 0x9F, 0x2D, 0x96, 0xA5,
0xAB, 0x04, 0x7A, 0xFF, 0x79, 0x09, 0xDA, 0xCB,
0x64, 0xD4, 0xFD, 0x3B, 0x35, 0x11, 0xD7, 0xF1,
0xB9, 0x41, 0xA6, 0x64, 0xDF, 0x40, 0x6D, 0xB9 }

```

2.2. DLP Keys

The following widely-known test keys may be used for DLP-based algorithms such as DSA, DH, and Elgamal.

DLP-1024 key

```

/* p */
1018,
{ 0x03, 0x0C, 0xDF, 0xC3, 0x8F, 0xC3, 0xE4, 0x21,
  0x27, 0x90, 0xB0, 0xA4, 0x1E, 0x45, 0xB4, 0xE4,
  0xE8, 0x80, 0xDE, 0x8A, 0xBF, 0xD3, 0xAE, 0xCA,
  0x0B, 0x23, 0x8F, 0xB6, 0xCD, 0x73, 0x0C, 0xC3,
  0x18, 0x76, 0x93, 0x36, 0xD5, 0xB1, 0x80, 0xB2,
  0x80, 0x2A, 0x01, 0xBE, 0x4B, 0xC1, 0xAB, 0x84,
  0xFC, 0xE2, 0xFF, 0x48, 0x9B, 0x50, 0xC2, 0xD2,
  0x9D, 0xE9, 0x1E, 0xC0, 0xE6, 0x5B, 0x60, 0x64,
  0xFD, 0x0D, 0xE5, 0x37, 0xEA, 0xBA, 0x1C, 0x6C,
  0xDD, 0x27, 0xDC, 0x30, 0x30, 0x48, 0x1E, 0x8B,
  0xB9, 0x60, 0xAA, 0x8B, 0x8A, 0xEF, 0x93, 0x35,

```

```
    0x30, 0xE6, 0xB1, 0xCC, 0x51, 0x60, 0xBB, 0xFA,
    0xAF, 0x85, 0x0F, 0xF6, 0x57, 0x81, 0x12, 0x33,
    0x7D, 0x53, 0x03, 0x4E, 0x41, 0x63, 0xDC, 0x65,
    0x03, 0xBD, 0xF8, 0x89, 0x25, 0x81, 0x14, 0x1F,
    0xAB, 0x82, 0x55, 0xB6, 0xD9, 0x72, 0x7B, 0xB3 },
/* q */
160,
{ 0xEC, 0x41, 0xB9, 0xC0, 0x62, 0x1D, 0x5B, 0xDC,
  0xAF, 0x11, 0xD5, 0x19, 0x8F, 0x72, 0x08, 0x88,
  0x2E, 0x65, 0xBB, 0xDF },
/* g */
1017,
{ 0x01, 0x64, 0x87, 0xAC, 0xCF, 0xCD, 0x95, 0x50,
  0x51, 0xE0, 0x6E, 0x1C, 0x5B, 0xEF, 0x45, 0x2C,
  0x12, 0x63, 0xC7, 0x5D, 0x2B, 0x36, 0x50, 0x4F,
  0xB4, 0x27, 0x57, 0x35, 0xC2, 0x83, 0x32, 0x0B,
  0x63, 0xAC, 0x91, 0xC6, 0xF4, 0x02, 0x09, 0x32,
  0x53, 0x1C, 0xAB, 0x04, 0xB1, 0xCD, 0x72, 0xFD,
  0xF2, 0x9D, 0xE2, 0x4E, 0x27, 0x17, 0x97, 0xA7,
  0xDD, 0x21, 0x97, 0x67, 0x69, 0x31, 0xF9, 0x33,
  0x1D, 0x1F, 0x59, 0xEE, 0xE5, 0xBA, 0x2C, 0x7D,
  0x54, 0xAE, 0x13, 0x5C, 0x7F, 0x79, 0x41, 0x37,
  0xD8, 0xD8, 0x0E, 0xB6, 0x29, 0x28, 0x8E, 0x26,
  0x8A, 0x3B, 0xEB, 0xD2, 0x1F, 0x16, 0xA4, 0x03,
  0xF1, 0xD5, 0xDA, 0xD8, 0x3C, 0x1C, 0x47, 0x80,
  0x17, 0xA3, 0xCD, 0x26, 0x6F, 0x1B, 0xA4, 0x9B,
  0x89, 0x0D, 0xC0, 0x89, 0x21, 0x2E, 0x72, 0x26,
  0x1D, 0xA3, 0x67, 0xAF, 0x80, 0x3B, 0x02, 0x50 },
/* x */
157,
{ 0x11, 0xED, 0x99, 0x78, 0x5A, 0x81, 0x3A, 0x1B,
  0x0E, 0x96, 0xEC, 0xD3, 0x8D, 0x7F, 0x9B, 0xCE,
  0x9E, 0xBF, 0xD6, 0xFA },
/* y */
1018,
{ 0x02, 0x20, 0xB9, 0x42, 0xC2, 0x5C, 0x44, 0xDA,
  0x52, 0xB0, 0xD1, 0x76, 0x82, 0xEA, 0xC4, 0x36,
  0xEA, 0x7E, 0x81, 0xEC, 0x9F, 0x76, 0xE1, 0x05,
  0x75, 0x32, 0xAA, 0x67, 0xEA, 0xDD, 0x04, 0xAD,
  0xB8, 0xFD, 0x61, 0x81, 0xBA, 0x0B, 0x25, 0xF2,
  0x84, 0xDA, 0xAA, 0xAA, 0x05, 0xF3, 0xC8, 0x40,
  0x34, 0xD4, 0x17, 0xD3, 0x7B, 0x6E, 0x0A, 0x63,
  0x31, 0x8A, 0x0A, 0x79, 0x1F, 0x1D, 0x0D, 0xD4,
  0xF6, 0x8A, 0xFA, 0xE3, 0x35, 0xAA, 0x5D, 0xBE,
  0xA3, 0xF2, 0xF6, 0xD6, 0xDD, 0x73, 0x09, 0x26,
  0x24, 0x7F, 0xDC, 0x4D, 0x1B, 0x82, 0xDF, 0x8C,
  0x2D, 0x87, 0xAE, 0x8D, 0x36, 0xAD, 0xB9, 0xDD,
```

0x25, 0x13, 0x57, 0x8E, 0x8B, 0x99, 0xAA, 0x6A,

Internet-Draft

TestKeys

February 2022

0x0E, 0xDF, 0x67, 0x5F, 0xFC, 0x2F, 0xDE, 0xB6,
0x4B, 0x26, 0xE5, 0xBE, 0xD8, 0x53, 0x2D, 0xFD,
0x98, 0x11, 0x0F, 0xCF, 0xC9, 0xED, 0xF9, 0x38 }

DLP-2048 key

```
/* p */
2042,
{ 0x03, 0x2D, 0xD5, 0x53, 0x7D, 0x33, 0x7A, 0x91,
  0x34, 0x37, 0xD3, 0x5E, 0xA3, 0x43, 0x3D, 0xB0,
  0xE7, 0xB7, 0x21, 0x29, 0x8F, 0xBA, 0x87, 0x27,
  0xF2, 0xF9, 0xBE, 0x85, 0x6D, 0x6A, 0x14, 0x6B,
  0x92, 0x98, 0x8D, 0x50, 0x82, 0xF2, 0xC5, 0x72,
  0xB7, 0x70, 0x37, 0x63, 0xE8, 0x24, 0x54, 0xA7,
  0xA4, 0xA2, 0x25, 0x9B, 0x29, 0xAC, 0xE9, 0xB0,
  0xBC, 0x9B, 0x4B, 0x4D, 0x98, 0x5D, 0x6A, 0x9C,
  0x8C, 0xB6, 0x30, 0xE4, 0xE0, 0x9F, 0x48, 0x07,
  0x9F, 0x1B, 0xE8, 0x07, 0x69, 0x71, 0xDE, 0x92,
  0x68, 0x56, 0x70, 0xB9, 0x4C, 0xC9, 0x68, 0x7D,
  0xDC, 0x23, 0x3B, 0x30, 0xAF, 0x22, 0x94, 0xB0,
  0x30, 0xA6, 0xB4, 0x97, 0xF6, 0x46, 0xF9, 0x4E,
  0x1C, 0x17, 0xE8, 0x3A, 0x90, 0x4C, 0x2C, 0x1B,
  0x68, 0x44, 0x10, 0xCE, 0x04, 0x8F, 0xD9, 0xCD,
  0x64, 0x05, 0xA1, 0x4A, 0xA6, 0x8C, 0x2B, 0x8F,
  0x7F, 0x8B, 0xD0, 0x6E, 0x9F, 0x64, 0xC4, 0xBB,
  0x69, 0xCC, 0xBF, 0xBC, 0x80, 0x56, 0xAE, 0x41,
  0x4A, 0x8B, 0x2E, 0x35, 0xD6, 0x20, 0x5C, 0xDE,
  0xFB, 0x2A, 0x24, 0xA3, 0x79, 0xB8, 0xA1, 0x16,
  0x17, 0x50, 0x95, 0xFF, 0x57, 0xFF, 0x61, 0x55,
  0x12, 0x86, 0x86, 0xD9, 0x9B, 0x8E, 0x1F, 0x24,
  0x44, 0x63, 0x12, 0x71, 0xF0, 0x9C, 0x33, 0x4F,
  0x37, 0x22, 0x45, 0x2F, 0xE9, 0x26, 0x3F, 0xC3,
  0x34, 0x9E, 0x6F, 0x33, 0x07, 0xA6, 0x75, 0x4F,
  0xFD, 0x89, 0xD4, 0x43, 0x27, 0x38, 0x7D, 0xFD,
  0x40, 0x18, 0xA0, 0x2A, 0xEA, 0x6E, 0xF4, 0xC6,
  0x36, 0xA7, 0x69, 0xE7, 0xCE, 0xB7, 0x37, 0x19,
  0x19, 0x72, 0x49, 0xA8, 0x41, 0xA3, 0x0B, 0xE0,
  0xC4, 0xBE, 0x8E, 0xCB, 0x10, 0x7F, 0x38, 0x02,
  0xDC, 0x45, 0x83, 0xF8, 0xE0, 0x12, 0x94, 0xD5,
```

```

    0x2B, 0x62, 0x13, 0x67, 0xBD, 0x0C, 0x19, 0x53 },
/* q */
225,
{ 0x01, 0x95, 0x09, 0xB2, 0xED, 0xA8, 0x3B, 0x08,
  0x82, 0x73, 0x1B, 0x3F, 0xE8, 0x9C, 0x2E, 0xF6,
  0x9D, 0xB8, 0xD8, 0x36, 0x12, 0x34, 0x5D, 0x1A,
  0x66, 0xA5, 0x83, 0xB9, 0x11 },
/* g */

```

```

2040,
{ 0xAC, 0x5D, 0x12, 0x0E, 0x46, 0xD2, 0xBA, 0xD6,
  0x87, 0x88, 0x47, 0xCC, 0xE8, 0x70, 0xA6, 0x9E,
  0xDC, 0xAD, 0xC8, 0x6C, 0x85, 0x9C, 0x49, 0xBA,
  0xF7, 0xAD, 0xE4, 0x1E, 0xD9, 0x36, 0x8E, 0xC2,
  0x3B, 0x64, 0x54, 0xFB, 0x60, 0xEA, 0xDA, 0xAC,
  0xC6, 0x64, 0x2A, 0x6F, 0xDD, 0x32, 0x2B, 0x99,
  0xAB, 0x14, 0x75, 0x81, 0xB2, 0x1B, 0xEB, 0xE0,
  0x62, 0x94, 0xE3, 0x82, 0x0B, 0xC5, 0x56, 0xFA,
  0x54, 0x11, 0xB3, 0x1C, 0x37, 0x3B, 0x39, 0xA6,
  0x7D, 0x51, 0x8A, 0x54, 0x77, 0x13, 0x41, 0x5C,
  0x67, 0xAC, 0xEF, 0x18, 0xBC, 0x6B, 0xA9, 0x4C,
  0x95, 0x60, 0x0C, 0xB5, 0xBD, 0xA8, 0x3C, 0x84,
  0xAD, 0x58, 0xE5, 0x49, 0x1D, 0x26, 0x26, 0x1E,
  0xD4, 0xE5, 0x35, 0xAD, 0xB2, 0x2E, 0x35, 0xB0,
  0x6C, 0xC2, 0xB4, 0xC8, 0x9D, 0xA2, 0xDC, 0x63,
  0xE2, 0x9E, 0xDA, 0x06, 0xF0, 0x13, 0x80, 0x72,
  0x46, 0x55, 0x89, 0x32, 0xE9, 0xF2, 0xDC, 0x8B,
  0x93, 0x2E, 0x6B, 0x84, 0xB4, 0x07, 0xF5, 0x71,
  0x50, 0x9D, 0x06, 0xF7, 0x94, 0x30, 0xE9, 0x5D,
  0x46, 0xB2, 0xD0, 0x26, 0x14, 0x28, 0x84, 0x17,
  0x99, 0x98, 0x86, 0xA6, 0x71, 0x45, 0xED, 0x74,
  0x6A, 0x0C, 0xA8, 0xC0, 0x44, 0x41, 0x03, 0xF5,
  0x03, 0xE6, 0xBB, 0xE7, 0x45, 0x61, 0xC3, 0xAC,
  0xD1, 0x9A, 0xE5, 0x7A, 0x82, 0x67, 0xA1, 0xBC,
  0x3C, 0x49, 0x30, 0x83, 0xBB, 0x16, 0xC5, 0x97,
  0xA8, 0xAC, 0x99, 0x81, 0xFB, 0x70, 0x45, 0x87,
  0x17, 0xFB, 0x64, 0x9C, 0xA4, 0x61, 0xD4, 0x70,
  0xB4, 0xB3, 0x5E, 0x3E, 0x98, 0x64, 0xFA, 0x1A,
  0x59, 0x9B, 0xC0, 0x1E, 0x6F, 0xE9, 0x93, 0x0A,
  0x51, 0xF5, 0x79, 0xB0, 0x84, 0x01, 0x74, 0x25,
  0xB8, 0xD0, 0xA1, 0x02, 0x3F, 0xAE, 0xDD, 0xDC,
  0x57, 0xD1, 0xCE, 0x56, 0x25, 0x1C, 0xDA },

```

```

/* x */
223,
{ 0x64, 0x05, 0xBC, 0xDE, 0xB4, 0xF7, 0x68, 0x29,
  0x02, 0x23, 0xCE, 0x5D, 0xB5, 0x2A, 0x8A, 0x30,
  0xC2, 0x8A, 0xDC, 0x78, 0x02, 0xD9, 0x68, 0x1E,
  0xDC, 0xB4, 0x34, 0xE5 },
/* y */
2042,
{ 0x02, 0x30, 0x37, 0xB2, 0xD9, 0xC9, 0x9E, 0x75,
  0x3F, 0xD2, 0x79, 0xBF, 0xFC, 0xDE, 0xE9, 0x92,
  0x9C, 0x9B, 0xA1, 0xDE, 0xAA, 0x97, 0x0B, 0x03,
  0x72, 0xAF, 0x73, 0x35, 0xE5, 0x50, 0x21, 0x37,
  0x42, 0x99, 0xF3, 0x61, 0x02, 0x7C, 0x8D, 0x65,
  0xD5, 0x7A, 0xFB, 0x4D, 0x3C, 0xCD, 0x2B, 0x47,
  0x24, 0xB5, 0x3F, 0x09, 0xEB, 0xE2, 0x8C, 0xBF,

```

```

0x49, 0x9F, 0x6B, 0x4F, 0x86, 0x33, 0x49, 0x19,
0x8B, 0x24, 0xB2, 0xAB, 0x0D, 0x4C, 0xEC, 0xB6,
0xC4, 0xFD, 0x7E, 0x67, 0x2D, 0x4B, 0x2A, 0xCA,
0x9D, 0x39, 0xE3, 0xAE, 0x20, 0xF8, 0xEC, 0xD7,
0xFD, 0x77, 0x10, 0x7C, 0xE5, 0x4A, 0x66, 0xDD,
0xEE, 0x97, 0x44, 0xE4, 0x8C, 0xF8, 0xDD, 0x6B,
0xA9, 0xA5, 0x28, 0xC7, 0x51, 0xF0, 0x08, 0xC6,
0x6F, 0x19, 0x2A, 0x20, 0x4E, 0xC7, 0xF9, 0x38,
0x76, 0x91, 0x01, 0x79, 0xB1, 0x31, 0x1D, 0x97,
0x5B, 0x49, 0x25, 0xC5, 0x69, 0x90, 0x29, 0xFB,
0xD1, 0x14, 0xA5, 0xE7, 0x90, 0x19, 0x0A, 0x4D,
0x38, 0x9B, 0x94, 0x8F, 0x8F, 0x57, 0x6A, 0x8E,
0x45, 0xA5, 0x6B, 0xE0, 0xD4, 0xFD, 0x6C, 0xEA,
0x63, 0x1C, 0x5F, 0x53, 0x7E, 0xF9, 0x18, 0x59,
0x8E, 0x30, 0x52, 0x2F, 0x93, 0x64, 0x50, 0x66,
0x18, 0xC0, 0x45, 0x84, 0xCA, 0x6F, 0xD0, 0x75,
0x12, 0x12, 0x21, 0xA4, 0x60, 0xF9, 0x80, 0xC5,
0x4F, 0x80, 0x1D, 0x7D, 0x6D, 0x21, 0x9D, 0xF2,
0xA1, 0xDB, 0xEA, 0x3C, 0x8A, 0x03, 0xA0, 0x9F,
0x6B, 0xE9, 0x1B, 0xB6, 0x29, 0x6D, 0x79, 0x1A,
0x2A, 0x83, 0x80, 0xE8, 0x9D, 0x0C, 0xDD, 0x26,
0xF7, 0x66, 0x3E, 0x06, 0x9A, 0x83, 0x31, 0x49,
0xAD, 0x44, 0x2B, 0x2C, 0x13, 0x98, 0x87, 0x71,
0xF6, 0x54, 0xB8, 0x1F, 0x50, 0xE0, 0xD7, 0x26,
0x42, 0x47, 0xD6, 0x78, 0xEA, 0xEB, 0xB0, 0xF9 }

```

```

/* p */
4086,
{ 0x31, 0xD2, 0x55, 0x5F, 0xB2, 0xE8, 0x89, 0xF3,
  0x20, 0x83, 0x78, 0x79, 0x5A, 0xF4, 0x88, 0x5B,
  0x62, 0xD0, 0x13, 0x58, 0xBD, 0xF1, 0x17, 0xC0,
  0xB8, 0xAD, 0x4D, 0x22, 0xBE, 0x62, 0xCC, 0x93,
  0x34, 0x5B, 0x6E, 0xA8, 0xFC, 0x54, 0x0B, 0x56,
  0x8F, 0x50, 0x95, 0xBB, 0xA0, 0x90, 0x3E, 0xC5,
  0xEE, 0xD8, 0xC6, 0xAE, 0x52, 0x5D, 0x9A, 0xA7,
  0xE4, 0x99, 0x79, 0xF0, 0x8E, 0x6C, 0x4E, 0xDB,
  0xF5, 0x6A, 0x93, 0x29, 0x09, 0xA0, 0x6B, 0x6D,
  0x1E, 0x07, 0x57, 0x95, 0x3F, 0x90, 0x5B, 0x55,
  0x52, 0x99, 0x31, 0x5F, 0x42, 0x48, 0xF5, 0x4B,
  0x81, 0xEF, 0x5F, 0x05, 0x4D, 0x8D, 0x82, 0x4E,
  0x12, 0xAE, 0xAB, 0x82, 0x4B, 0x2C, 0x2F, 0x4C,
  0x5E, 0xDE, 0x04, 0x60, 0x30, 0xDC, 0x3B, 0x16,
  0xC2, 0x80, 0x59, 0x56, 0x85, 0xCA, 0x38, 0xC6,
  0xE7, 0x13, 0xD8, 0x2E, 0x4D, 0x1B, 0xFC, 0xD3,
  0x3D, 0x87, 0xDE, 0x26, 0x95, 0x4B, 0xA0, 0x05,

```

```

0xBC, 0x42, 0x17, 0x77, 0x39, 0xB2, 0x0F, 0x1E,
0x46, 0x13, 0x80, 0x79, 0xED, 0xE5, 0x91, 0x64,
0xCE, 0x67, 0x23, 0xE3, 0x51, 0xE4, 0xB2, 0xFC,
0xD5, 0x0D, 0x6E, 0xAB, 0xB4, 0x5D, 0xA8, 0x8F,
0xA4, 0xCD, 0x56, 0x24, 0x8A, 0xEA, 0x44, 0xAA,
0x2E, 0x41, 0xB8, 0xFF, 0x28, 0xBD, 0x37, 0x88,
0x00, 0x8C, 0x2E, 0xEF, 0x4B, 0xE1, 0x90, 0xA0,
0xAB, 0x5D, 0x7D, 0x80, 0x3C, 0x9A, 0xBE, 0xD7,
0xC7, 0xB7, 0x74, 0xB5, 0x0F, 0xA8, 0x38, 0x0D,
0xD7, 0xFE, 0x2B, 0x3D, 0x84, 0x85, 0xA3, 0xD8,
0x80, 0xEF, 0x51, 0xD5, 0x6B, 0x41, 0x1F, 0x73,
0xE6, 0x59, 0xE7, 0x9E, 0x0B, 0xFF, 0x32, 0x14,
0x53, 0x57, 0x3E, 0xC5, 0x0D, 0x9D, 0xD4, 0xD0,
0xAE, 0xCA, 0x30, 0x9D, 0x39, 0xE4, 0x38, 0x86,
0x27, 0x95, 0x03, 0xEF, 0x94, 0x98, 0x51, 0xE3,
0xD4, 0xDC, 0x71, 0xAB, 0xF3, 0xA7, 0x88, 0x63,
0xB9, 0x75, 0xC1, 0x06, 0x24, 0xCB, 0x51, 0x73,
0x4C, 0xDB, 0x58, 0x2A, 0x3A, 0x48, 0xC6, 0xD7,
0x08, 0x47, 0x83, 0x6E, 0x80, 0x8B, 0x0E, 0x22,

```

```

0x48, 0xB8, 0xFA, 0x8A, 0x8C, 0x55, 0xA3, 0x57,
0xE8, 0x30, 0x54, 0xD6, 0x48, 0xB2, 0xCC, 0xA5,
0xB8, 0xA3, 0xB1, 0x68, 0x91, 0xAD, 0x52, 0x35,
0x6E, 0x92, 0x87, 0x1A, 0xF5, 0x99, 0xA5, 0x6E,
0x90, 0xC9, 0x34, 0x33, 0xA5, 0x4A, 0x52, 0xFD,
0x42, 0xE2, 0xBE, 0x65, 0x15, 0xC8, 0xCE, 0xC3,
0x73, 0x94, 0x07, 0x0C, 0x26, 0xCA, 0xC5, 0xCA,
0x8C, 0x26, 0x1D, 0x2D, 0x50, 0x21, 0x88, 0x6B,
0xB9, 0x4C, 0x4E, 0x99, 0xFA, 0x78, 0xD2, 0x53,
0x7C, 0xCA, 0xF5, 0xA1, 0x92, 0xC9, 0xC2, 0xAF,
0x77, 0xA0, 0x78, 0x33, 0x45, 0x1F, 0x12, 0x2D,
0xA9, 0xE6, 0xFD, 0x7B, 0x83, 0x92, 0x12, 0x9E,
0xE4, 0x9A, 0x56, 0x07, 0x5F, 0x1A, 0x37, 0x05,
0x00, 0x4C, 0x06, 0xBD, 0x36, 0x7F, 0xBF, 0xCB,
0x9A, 0x07, 0x4A, 0x02, 0xE1, 0x65, 0x25, 0x27,
0x2D, 0xF9, 0xD3, 0x33, 0xCB, 0x91, 0x9B, 0x5B,
0x61, 0x14, 0x07, 0xF7, 0xF7, 0xA4, 0xD9, 0xE1,
0x1E, 0xD2, 0x85, 0xA4, 0x75, 0x95, 0xEA, 0x74,
0x0C, 0xBF, 0xA1, 0x6B, 0xD2, 0xFB, 0xB8, 0x0A,
0xD2, 0xA5, 0xE6, 0x36, 0x04, 0x47, 0x80, 0x8B,
0x1E, 0xC5, 0x07, 0x58, 0xB8, 0x56, 0xF6, 0xDC,
0xA4, 0x25, 0xD9, 0x36, 0xB4, 0x9E, 0xEA, 0x5B,
0x7E, 0xAA, 0x40, 0x79, 0xA3, 0x15, 0x3D, 0xED,
0x32, 0x12, 0x76, 0x4D, 0x00, 0x06, 0xF0, 0x09,
0x36, 0x28, 0x4B, 0x96, 0xD6, 0x8B, 0xC9, 0x74,
0xFD, 0xAF, 0x77, 0xB6, 0x45, 0x78, 0x36, 0x38,
0xC5, 0x1E, 0xB1, 0x18, 0x8A, 0x91, 0x72, 0xA0,
0x37, 0xDE, 0x49, 0xDA, 0x48, 0x1A, 0x9B },
/* q */

```

```

305,
{ 0x01, 0xFF, 0x30, 0x36, 0x06, 0x89, 0x3F, 0x53,
  0xBE, 0x41, 0x12, 0xF9, 0x60, 0x18, 0xF9, 0x9C,
  0xCF, 0xB9, 0x67, 0x82, 0x7E, 0x49, 0x40, 0x36,
  0x98, 0x2F, 0xAF, 0x24, 0x06, 0xD2, 0x5D, 0x8B,
  0xCC, 0x52, 0x48, 0xDB, 0x2B, 0xCB, 0x13 },
/* g */
4085,
{ 0x19, 0x89, 0x03, 0x1B, 0x12, 0xB8, 0x83, 0x5D,
  0x66, 0x5C, 0x9F, 0x42, 0x31, 0x05, 0x24, 0xA0,
  0x64, 0x9E, 0xEC, 0x4C, 0x2C, 0x4A, 0xBA, 0xAC,
  0xAD, 0x5D, 0x54, 0x8C, 0xE0, 0xFA, 0xF5, 0x3E,

```

0xCA, 0x38, 0x67, 0xAA, 0xE6, 0x18, 0x7D, 0x5F,
0x63, 0xC0, 0xF6, 0x6B, 0x56, 0xE8, 0x00, 0xAD,
0x5D, 0x09, 0x58, 0x8C, 0xA4, 0x25, 0xBC, 0xE6,
0xBD, 0x33, 0x97, 0x6B, 0xBA, 0xC9, 0x68, 0x63,
0xD1, 0xC2, 0x6E, 0x4F, 0x48, 0x27, 0x67, 0x05,
0x63, 0xFB, 0x9C, 0xA5, 0x16, 0x5C, 0x3C, 0x9F,
0x14, 0x1D, 0x2E, 0x7D, 0x77, 0xA6, 0x11, 0x95,
0x55, 0x4D, 0x9C, 0xE6, 0xA3, 0x25, 0xB9, 0x34,
0x2A, 0x5F, 0x0A, 0xDE, 0x00, 0x7E, 0xED, 0x69,
0xF3, 0x2C, 0x78, 0x67, 0x8C, 0x5F, 0x30, 0x2C,
0xAF, 0x97, 0x62, 0xFC, 0xC0, 0xD6, 0x22, 0xD2,
0xBF, 0xA5, 0xFF, 0x72, 0x4B, 0x59, 0x49, 0x21,
0x1C, 0x66, 0x2E, 0xD3, 0xD8, 0x14, 0x1E, 0xAF,
0xAB, 0xB6, 0x28, 0x65, 0xC2, 0xF2, 0xA6, 0x44,
0xA5, 0xDC, 0x34, 0x0F, 0x24, 0x0F, 0x73, 0x61,
0x53, 0x3C, 0x65, 0x64, 0xCD, 0x9E, 0x33, 0xB6,
0x58, 0xC1, 0x39, 0x71, 0xEC, 0xDA, 0x66, 0x2E,
0x1C, 0x79, 0xB5, 0x88, 0x7E, 0xA2, 0x46, 0x1E,
0x35, 0xA6, 0xBA, 0x2B, 0xD0, 0x20, 0x80, 0xF8,
0xE5, 0xC6, 0xC8, 0xBE, 0x7B, 0xFB, 0xB9, 0x6C,
0xF4, 0x1F, 0x07, 0xD5, 0xBD, 0xC9, 0x65, 0x00,
0xB5, 0x6C, 0x53, 0x4B, 0x70, 0x36, 0x99, 0x56,
0x8F, 0x70, 0x0B, 0x9A, 0xD5, 0xEF, 0xFC, 0x1E,
0xE8, 0xBE, 0x2F, 0x70, 0x39, 0x50, 0xAC, 0xD3,
0xB8, 0x8C, 0x24, 0x3F, 0x82, 0xA2, 0xE9, 0xF5,
0x01, 0xE3, 0x87, 0x84, 0x4E, 0x77, 0xAA, 0x90,
0x2D, 0xC0, 0xD7, 0xD9, 0x6E, 0xBE, 0x4E, 0x4B,
0xC8, 0xB3, 0xAB, 0x09, 0x64, 0xAC, 0x28, 0xB1,
0x54, 0xCD, 0x15, 0x35, 0xA4, 0x06, 0x55, 0x40,
0x83, 0x39, 0x8E, 0x0B, 0xE6, 0xAC, 0x9B, 0x26,
0xFF, 0x9A, 0xF4, 0xC2, 0xCD, 0xA9, 0x55, 0x17,
0x51, 0x15, 0x2F, 0xBD, 0x4C, 0xC2, 0xD7, 0xF1,
0x9A, 0x9E, 0x7F, 0x41, 0xA5, 0x6E, 0xBB, 0xEF,
0x3C, 0xD5, 0x1D, 0xF6, 0xB1, 0x08, 0x48, 0x06,
0x15, 0xA8, 0xF3, 0xED, 0x99, 0x9F, 0xEC, 0x7F,
0x0F, 0x3C, 0x53, 0x87, 0x55, 0x27, 0x70, 0x74,

0xB3, 0xA8, 0x0D, 0x4B, 0x6A, 0x84, 0x71, 0x26,
0xE1, 0xB9, 0xDF, 0xE2, 0x38, 0x96, 0xF5, 0xB1,
0x97, 0x53, 0x83, 0x9B, 0x18, 0xA7, 0xE6, 0x69,
0x3E, 0x9F, 0xB1, 0x3D, 0x11, 0x58, 0xA3, 0xAB,
0xAF, 0x4E, 0x04, 0x62, 0x7D, 0xEB, 0x96, 0x12,


```

0xD9, 0x59, 0x4D, 0x33, 0x26, 0x1A, 0xE5, 0x93,
0x67, 0xFF, 0xCA, 0xDE, 0xC3, 0xB5, 0xAF, 0xFF,
0xCB, 0xDF, 0xED, 0x45, 0x0B, 0x53, 0x8B, 0xC8,
0xD8, 0x8D, 0x29, 0x8E, 0xDD, 0x27, 0xB3, 0x36,
0xE8, 0xF5, 0xEE, 0x6D, 0x46, 0x1F, 0x57, 0x40,
0x3B, 0xB4, 0x6D, 0xBC, 0x04, 0xB6, 0xD9, 0x00,
0xC7, 0x48, 0x72, 0x8D, 0xE7, 0x8F, 0x68, 0x8F,
0xCD, 0x9A, 0x90, 0x29, 0x4E, 0xEA, 0x95, 0xE7,
0xCE, 0x48, 0x2A, 0x39, 0xB0, 0x62, 0xE8, 0x04,
0xFC, 0xCB, 0x6E, 0xF7, 0xD1, 0x35, 0x94, 0xB9,
0x35, 0x0E, 0xC2, 0x0F, 0xB5, 0x02, 0xA8, 0x4C,
0x4E, 0x30, 0x96, 0xC5, 0x90, 0xAA, 0x29, 0x63,
0x78, 0x79, 0x0D, 0x81, 0x9E, 0xC2, 0xC5, 0x0D,
0xD5, 0xF5, 0x46, 0xF5, 0xE3, 0xE4, 0xD9, 0x69,
0xEC, 0x33, 0xDA, 0x45, 0x52, 0x14, 0xD7, 0xA0,
0x5C, 0xAA, 0xF8, 0x87, 0xB5, 0xE8, 0x9B, 0x09,
0xE6, 0xB2, 0xCF, 0x0D, 0x56, 0x43, 0xC3, 0x85,
0x48, 0x01, 0x8A, 0x87, 0x7B, 0x5A, 0x17, 0x72,
0x40, 0x2B, 0x4B, 0x29, 0xF3, 0x5C, 0x8B },
/* x */
305,
{ 0x01, 0xA7, 0x77, 0x11, 0xB8, 0x9D, 0x45, 0x53,
  0x27, 0x29, 0x01, 0xBA, 0x09, 0x5A, 0x7F, 0xFC,
  0x14, 0x9C, 0x8C, 0x05, 0xB0, 0x2F, 0xDD, 0x04,
  0x0D, 0xC9, 0x98, 0x97, 0x11, 0x5B, 0xCE, 0xC3,
  0xE6, 0x14, 0xF2, 0x55, 0x7F, 0x9C, 0x0C },
/* y */
4086,
{ 0x2A, 0x49, 0x11, 0x73, 0x18, 0x65, 0x11, 0x4B,
  0x8A, 0x6C, 0x6F, 0x8E, 0x40, 0x7D, 0x55, 0xC3,
  0x9A, 0xB7, 0x10, 0xBB, 0x45, 0xCA, 0xBA, 0x94,
  0xE6, 0xB1, 0x85, 0x87, 0xD2, 0x8F, 0x9C, 0x6C,
  0x69, 0x4C, 0x01, 0x9A, 0x09, 0xB2, 0x6F, 0x44,
  0x8C, 0x2A, 0x33, 0x55, 0xA5, 0x67, 0xB1, 0xA0,
  0xC8, 0x61, 0x82, 0x2E, 0x19, 0xC6, 0xFA, 0xDE,
  0x8C, 0x43, 0xAA, 0x61, 0xC3, 0xBF, 0x39, 0xB6,
  0x95, 0xE2, 0xA2, 0x74, 0x55, 0x2F, 0xE8, 0x5C,
  0x76, 0x5B, 0x8A, 0x1E, 0xF7, 0x8D, 0x1B, 0x42,
  0x97, 0xEF, 0x4C, 0x31, 0x3F, 0xE8, 0xDB, 0xF2,
  0x22, 0x11, 0x30, 0xC5, 0xEE, 0x91, 0xF9, 0xE3,
  0xD3, 0xBB, 0xF2, 0x9C, 0xC4, 0x7B, 0x1B, 0xAB,
  0xAF, 0x17, 0x9C, 0xBA, 0x8B, 0xD4, 0x5B, 0xA9,
  0x61, 0xD7, 0x0A, 0xB6, 0xBD, 0x7A, 0xA0, 0x75,

```

0xFB, 0x2A, 0x15, 0x33, 0x14, 0xFC, 0x3B, 0x2C,
0x3B, 0x89, 0x86, 0x6E, 0x68, 0x2C, 0x7A, 0x95,
0x8D, 0x3B, 0x78, 0x87, 0xF0, 0xD7, 0xD8, 0xF4,
0x0D, 0xF5, 0x5E, 0x6E, 0x51, 0x5D, 0x1F, 0xBB,
0x88, 0x77, 0x8E, 0xAF, 0x8E, 0xF1, 0xE8, 0xF3,
0x11, 0x9A, 0x74, 0x98, 0x80, 0x66, 0x7C, 0xA8,
0xEC, 0xC4, 0x6B, 0xFA, 0x10, 0xBA, 0xC4, 0x67,
0x4B, 0x77, 0xB9, 0x4E, 0xB0, 0xE9, 0x2A, 0x76,
0xA6, 0xC0, 0x81, 0x59, 0xD1, 0xF4, 0x06, 0xB6,
0x68, 0x5F, 0xE8, 0x5B, 0x41, 0xA8, 0xD8, 0x04,
0x93, 0x91, 0x8A, 0xF5, 0x29, 0x9A, 0x1C, 0x6A,
0x11, 0x3D, 0xE2, 0xF9, 0x74, 0x27, 0xCD, 0x87,
0xC4, 0xBA, 0x28, 0x2A, 0x65, 0x5D, 0x6A, 0x4E,
0xE7, 0x15, 0x01, 0x2E, 0x0C, 0x75, 0x0C, 0xC3,
0xB1, 0xE5, 0xC0, 0xF2, 0x2B, 0xC8, 0x2A, 0xD2,
0x3E, 0xB4, 0xC0, 0xEC, 0xF4, 0x80, 0xAC, 0xB7,
0xD7, 0x31, 0x21, 0x57, 0xDB, 0xB7, 0xE0, 0xE5,
0x23, 0x78, 0xE9, 0xFF, 0x46, 0xEE, 0xEF, 0x04,
0xAF, 0x47, 0x4F, 0x2C, 0x4C, 0x55, 0xDF, 0xFF,
0xCF, 0x79, 0x8B, 0x90, 0x3F, 0x49, 0xEA, 0x43,
0xD0, 0x60, 0xEF, 0x23, 0xED, 0x7D, 0x63, 0x89,
0x7B, 0xCB, 0x2F, 0xF1, 0x39, 0xAB, 0x0D, 0x80,
0x5F, 0xF7, 0x85, 0x87, 0xCC, 0xE6, 0xF1, 0xF2,
0xCE, 0x39, 0x07, 0xBB, 0xDA, 0x5A, 0x67, 0x39,
0xCF, 0x62, 0x47, 0x2C, 0xA2, 0x11, 0x85, 0x18,
0xDA, 0xFE, 0x90, 0x7C, 0x4B, 0xEA, 0x88, 0xDC,
0xAE, 0x39, 0x01, 0x07, 0x3A, 0xB6, 0xCC, 0x60,
0xA5, 0x60, 0xC9, 0xA4, 0xD6, 0x33, 0x1E, 0x29,
0xF8, 0x8A, 0xFE, 0xB9, 0x99, 0xA6, 0x4A, 0xE4,
0xDB, 0xC7, 0xBF, 0x02, 0x22, 0xA9, 0xD4, 0x19,
0x3A, 0x20, 0xE8, 0x1B, 0x40, 0x30, 0xF3, 0x28,
0xE3, 0xA9, 0xCB, 0x7C, 0x92, 0x62, 0x04, 0x98,
0x47, 0x4F, 0xCB, 0x64, 0xDA, 0xE1, 0xBB, 0xD7,
0x9E, 0x4A, 0x9C, 0x04, 0x76, 0x47, 0x5E, 0xF0,
0xF9, 0xAB, 0x5E, 0x89, 0xAE, 0x4D, 0x5A, 0xAE,
0x9F, 0x87, 0x60, 0x21, 0xFA, 0x0B, 0xB2, 0x82,
0x17, 0xCF, 0x27, 0x8D, 0x3A, 0xE9, 0xED, 0xDC,
0x1C, 0x57, 0xBE, 0x5E, 0x17, 0xDC, 0x0D, 0x94,
0x8E, 0x02, 0xFC, 0x05, 0xFE, 0xDF, 0x74, 0x07,
0x05, 0xD8, 0xDC, 0xDC, 0x9D, 0x4B, 0x9C, 0xE6,
0x80, 0x93, 0x65, 0x74, 0x94, 0x01, 0x5E, 0x05,
0x17, 0x78, 0x96, 0xF1, 0x29, 0xFD, 0xFF, 0xB5,
0xFF, 0x4A, 0xF5, 0x7C, 0x64, 0xD1, 0x51, 0xEC,
0xEC, 0x8E, 0x74, 0x7B, 0x72, 0x67, 0xFA, 0x2D,
0x8C, 0xF5, 0x97, 0x5E, 0x84, 0xC2, 0xEF, 0xAC,
0x18, 0xDF, 0x16, 0xF2, 0xD8, 0x98, 0x0C, 0xE4,
0x09, 0xC0, 0x3A, 0x1B, 0xC2, 0xB9, 0x5B, 0x34,
0x34, 0x18, 0x98, 0xC6, 0xA5, 0xC6, 0x28, 0x54,

Internet-Draft

TestKeys

February 2022

0xB8, 0x53, 0x33, 0xE1, 0x4A, 0xA8, 0xE9 }

[2.3.](#) ECDLP Keys

The following widely-known test keys may be used for ECDLP-based algorithms such as ECDA and ECDH.

P256 key

```
/* qx */
256,
{ 0x42, 0x25, 0x48, 0xF8, 0x8F, 0xB7, 0x82, 0xFF,
  0xB5, 0xEC, 0xA3, 0x74, 0x44, 0x52, 0xC7, 0x2A,
  0x1E, 0x55, 0x8F, 0xBD, 0x6F, 0x73, 0xBE, 0x5E,
  0x48, 0xE9, 0x32, 0x32, 0xCC, 0x45, 0xC5, 0xB1 },
/* qy */
256,
{ 0x6C, 0x4C, 0xD1, 0x0C, 0x4C, 0xB8, 0xD5, 0xB8,
  0xA1, 0x71, 0x39, 0xE9, 0x48, 0x82, 0xC8, 0x99,
  0x25, 0x72, 0x99, 0x34, 0x25, 0xF4, 0x14, 0x19,
  0xAB, 0x7E, 0x90, 0xA4, 0x2A, 0x49, 0x42, 0x72 },
/* d */
256,
{ 0xE6, 0xCB, 0x5B, 0xDD, 0x80, 0xAA, 0x45, 0xAE,
  0x9C, 0x95, 0xE8, 0xC1, 0x54, 0x76, 0x67, 0x9F,
  0xFE, 0xC9, 0x53, 0xC1, 0x68, 0x51, 0xE7, 0x11,
  0xE7, 0x43, 0x93, 0x95, 0x89, 0xC6, 0x4F, 0xC1 }
```

P384 key

Internet-Draft

TestKeys

February 2022

```
/* qx */
384,
{ 0x5B, 0x09, 0x01, 0xB8, 0x85, 0x23, 0x29, 0x6E,
  0xB9, 0x19, 0xD5, 0x0F, 0xFA, 0x1A, 0x9C, 0xB3,
  0x74, 0xBC, 0x4D, 0x40, 0x95, 0x86, 0x28, 0x2B,
  0xFE, 0xCA, 0x11, 0xB1, 0xD9, 0x5A, 0xDB, 0xB5,
  0x47, 0x34, 0xAF, 0x57, 0x0B, 0xF8, 0x2B, 0x72,
  0x28, 0xCF, 0x22, 0x6B, 0xCF, 0x4C, 0x25, 0xDD },
/* qy */
384,
{ 0xBC, 0xFE, 0x3B, 0x1A, 0x3A, 0xD3, 0x94, 0x30,
  0xEF, 0xF7, 0x63, 0xE1, 0xD6, 0x8D, 0x2E, 0x15,
  0x1D, 0x91, 0x72, 0x0B, 0x77, 0x95, 0xB5, 0x8D,
  0xA6, 0xB3, 0x46, 0x39, 0x61, 0x3A, 0x8F, 0xB9,
  0xB5, 0xA8, 0xDA, 0x48, 0xC6, 0x74, 0x71, 0x17,
  0xF9, 0x91, 0x9E, 0x84, 0x24, 0xF3, 0x7E, 0xC8 },
/* d */
384,
{ 0xE2, 0x56, 0x33, 0x28, 0xDF, 0xAB, 0xF6, 0x81,
  0x88, 0x60, 0x6B, 0x91, 0x32, 0x42, 0x81, 0xC1,
  0xD5, 0x8A, 0x44, 0x56, 0x43, 0x1B, 0x09, 0xD5,
  0x10, 0xB3, 0x5F, 0xEC, 0xC9, 0xF3, 0x07, 0xCA,
  0x18, 0x22, 0x84, 0x6F, 0xA2, 0x67, 0x13, 0x71,
  0xA9, 0xA8, 0x1B, 0xAC, 0x0E, 0x35, 0x74, 0x9D }
```

P521 key

Internet-Draft

TestKeys

February 2022

```
/* qx */
521,
{ 0x01, 0xD0, 0xFD, 0x72, 0x57, 0xA8, 0x4C, 0x74,
  0x7F, 0x56, 0x25, 0x75, 0xC0, 0x73, 0x85, 0xDB,
  0xEB, 0xF2, 0xF5, 0x2B, 0xEA, 0x58, 0x08, 0x3D,
  0xB8, 0x2F, 0xDD, 0x15, 0x31, 0xD8, 0xAA, 0xE3,
  0xCC, 0x87, 0x5F, 0xF0, 0x2F, 0xF7, 0xFA, 0x2D,
  0xA2, 0x60, 0xD8, 0xEB, 0x62, 0xD6, 0xD2, 0xF5,
  0xD6, 0x49, 0x27, 0x8E, 0x32, 0x17, 0x36, 0xA0,
  0x62, 0x8C, 0xBB, 0xB3, 0x03, 0x08, 0xB6, 0xE6,
  0x18, 0xDB },
/* qy */
521,
{ 0xF6, 0x2A, 0xD2, 0x04, 0xC6, 0x46, 0x03, 0x59,
  0xBC, 0x81, 0x8A, 0xB8, 0x96, 0x1B, 0xF0, 0xF0,
  0xFC, 0x0E, 0xC5, 0xAA, 0xE8, 0xA4, 0x28, 0x17,
  0x3C, 0xE5, 0x6F, 0x00, 0xDE, 0x9B, 0x15, 0x7C,
  0x1E, 0x5C, 0x82, 0xC6, 0x4F, 0x56, 0x2F, 0xCA,
  0xDE, 0xFC, 0x4A, 0x4C, 0x28, 0xF6, 0xD3, 0x42,
  0xCF, 0x3E, 0xF6, 0x16, 0xFC, 0x82, 0xD3, 0x3B,
  0x72, 0x85, 0xC9, 0x21, 0xF2, 0xBF, 0x36, 0xFD,
  0xD8 },
/* d */
521,
{ 0x01, 0xD9, 0x24, 0xDC, 0xCA, 0x0A, 0x88, 0x7F,
  0x8D, 0x99, 0x76, 0x7A, 0x37, 0xD8, 0x74, 0xE6,
  0x37, 0xA1, 0x2C, 0xCB, 0x47, 0x7D, 0x6E, 0x08,
  0x66, 0x53, 0x56, 0x69, 0x4D, 0x68, 0xB7, 0x65,
```

0x5E, 0x50, 0x69, 0x63, 0x8F, 0xDE, 0x7B, 0x45,
0xC8, 0x54, 0x01, 0x3D, 0xC7, 0x7A, 0x35, 0xB1,
0x86, 0x55, 0xB8, 0x4C, 0x96, 0x6A, 0x60, 0x22,
0x0D, 0x40, 0xF9, 0x1E, 0xD9, 0xF5, 0x14, 0x58,
0x02, 0xEA }

[3.](#) Contributors/Acknowledgements

[4.](#) IANA Considerations

[5.](#) Security Considerations

The intent of publishing known keys in this form is that they may be easily recognised as being test keys when encountered. It should go without saying that these keys should never be used or relied upon in production environments.

Gutmann

Expires 24 August 2022

[Page 26]

Internet-Draft

TestKeys

February 2022

The author awaits the inevitable CVEs.

[6.](#) Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997, <<http://www.ietf.org/rfc/rfc2119.txt>>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [RFC 8174](#), May 2017, <<http://www.ietf.org/rfc/rfc8174.txt>>.

Author's Address

Peter Gutmann
University of Auckland
Department of Computer Science
Auckland
New Zealand
Email: pgut001@cs.auckland.ac.nz

