

Standard Public Key Cryptography (PKC) Test Keys

Стандартные тестовые ключи для криптографии с открытым ключом

Аннотация

Этот документ представляет набор стандартных ключей для криптографии с открытым ключом (Public Key Cryptography или PKC) которые можно применять везде, где требуются заранее созданные ключи и связанные с ними операции, такие как цифровые подписи. Подобно тесту вирусов Европейского института антивирусных компьютерных исследований (European Institute for Computer Antivirus Research или EICAR) и файлам базового теста спама (Generic Test for Unsolicited Bulk Email или GTUBE), эти общеизвестные тестовые ключи могут быть обнаружены и распознаны приложениями, использующими их исключительно для тестирования, не предполагая каких-либо свойств защиты.

Статус документа

Документ не относится к категории Internet Standards Track и публикуется для информации.

Документ относится к категории Internet Standards Track.

Документ является результатом работы IETF¹ и представляет согласованный взгляд сообщества IETF. Документ прошёл открытое обсуждение и был одобрен для публикации IESG². Дополнительную информацию о стандартах Internet можно найти в разделе 2 в RFC 7841.

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <https://www.rfc-editor.org/info/rfc9500>.

Авторские права

Авторские права (Copyright (c) 2023) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К документу применимы права и ограничения, указанные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<https://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно. Фрагменты программного кода, включённые в этот документ, распространяются в соответствии с упрощённой лицензией BSD, как указано в параграфе 4.e документа IETF Trust Legal Provisions, без каких-либо гарантий (как указано в Revised BSD License).

Этот документ может содержать материалы из документов IETF или участников IETF³, опубликованных или публично доступных до 10 ноября 2008 г. Лица, контролирующие авторские права на некоторые из таких материалов могли не предоставить IETF Trust прав на изменение таких материалов вне контекста стандартизации IETF⁴. Без получения соответствующей лицензии от лиц, контролирующих авторские права на такие материалы, этот документ не может быть изменён вне контекста стандартизации IETF, а также не могут открываться производные работы за пределами контекста стандартизации. Исключением является лишь форматирование документа для публикации в качестве RFC или перевод на другие языки.

Оглавление

1. Введение.....	1
2. Общеизвестные тестовые ключи.....	2
2.1. Ключи RSA.....	2
2.2. Ключи DLP.....	10
2.3. Ключи ECDLP.....	15
3. Взаимодействие с IANA.....	16
4. Вопросы безопасности.....	17
Адреса авторов.....	17

1. Введение

Широкое использование криптосистем с открытым ключом в Internet привело к распространению общеизвестных, но не всегда признанных ключей, применяемых для тестирования или поставки в приложениях с предустановленной конфигурацией. Эти ключи не обеспечивают защиты, но по причине отсутствия каких-либо записей о ключах полагающиеся на них стороны часто не знают об отсутствии защиты. Для решения этой проблемы данный документ представляет набор стандартных открытых тестовых ключей, которые могут применяться везде, где нужен заранее созданный или эталонный ключ, а также (за счёт расширений) - в ситуациях, где такие ключи могут применяться, например, при тестировании цифровых подписей для данных. Назначение ключей примерно соответствует назначению тестового файла EICAR (файл без вирусов для проверки антивирусной продукции) и файлу GTUBE, применяемому в продукции для обнаружения спама.

¹Internet Engineering Task Force - комиссия по решению инженерных задач Internet.

²Internet Engineering Steering Group - комиссия по инженерным разработкам Internet.

³В оригинале - IETF Contributions. *Прим. перев.*

⁴В оригинале - IETF Standards Process. *Прим. перев.*

Ключи охватывают три основных семейства алгоритмов:

- RSA;
- алгоритмы, основанные на задаче дискретного логарифмирования (Discrete Logarithm Problem или DLP), такие как DSA, Diffie-Hellman (DH), Elgamal;
- алгоритмы, основанные на задаче дискретного логарифмирования эллиптической кривой (Elliptic Curve Discrete Logarithm Problem или ECDLP), такие как ECDSA и Elliptic Curve Diffie-Hellman (ECDH).

Хотя некоторые алгоритмы и размеры ключей больше не являются рекомендуемыми, соответствующие алгоритмы и размеры ключей представлены в документе для большой базы имеющихся реализаций, использующих их.

Документ не пытается охватить всё возможные семейства и типы алгоритмов, поскольку их слишком много и постоянно появляются новые, а некоторые выходят из употребления. Если аналогичные документы будут создаваться для других алгоритмов, им следует обновлять этот документ, а для простоты реализации и применения документам следует поддерживать совместимость с форматом и соглашениями об именовании, принятыми здесь.

2. Общеизвестные тестовые ключи

В этом разделе представлены тестовые ключи разных размеров для групп алгоритмов в нотации в стиле языка C, которые можно напрямую включать в криптокод, написанный на языках, подобных C, таких как C, C++, Java, JavaScript, Go, Swift, Rust, что охватывает большинство языков, применяемых для реализации криптокода.

Наряду с форматом исходного кода ключи представлены также в закодированном виде в формате секретных ключей OpenSSL, который многие приложения могут обрабатывать напрямую.

Каждый элемент ключа приведён с указанием числа битов (значение, из которого берётся номинальный размер ключа), за которым следует строка байтов элемента ключа с порядком big-endian. Например, ниже представлен образец компонента ключа для значения RSA p, где 0xCF является старшим байтом значения RSA p, а 0x03 — младшим.

```
/* 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 },
```

В дополнение к данному ключа каждому ключу назначено рекомендуемое имя для использования в исходном коде как средство указания каждого из ключей.

2.1. Ключи RSA

Представленные ниже общеизвестные тестовые ключи могут применяться для RSA.

Ключ RSA-1024 testRSA1024

```
/* 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,
  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 }

```

Кодированная форма ключа RSA-1024.

```

-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKbQCw0YNSqI9T1VFvRsIOejZ9feiKz1SgGfbe9Xq5tEzt2yJCsbyg
+xtcuCswNhdqY5A1ZN7G60HbL4/Hh/T1LhFJ4zNHVy1z9mDDx3yp4IICk2lb566d
fTD0B5EQ9Iqub4twLuDLKQCBfyhmJJvsEqKxm4J4QWgI+Brh/Pm3d4piPwIDAQAB
AoGASC6fj6TkLfmNdYHLQqG9kO1Pfys4fstarpZD7X+fUBJ/H/7y5DzeZLGCYAIU
+QeAHWv6TfZIQjReW7Qy00REJdgdwF1TFRCsKXhG5x+IB+jL0Grr08KbgPPDgy4Jm
xirRHZvtU81GhkiZX+omDIU28EHLNWL6rFEctWao/tERSPecQQDp2G5Nw0qYWn7H
Wm9Up1zkUTnkUkCzhqtxHberVnmHGKE7ryGMJEK2RmgHVstQpsvUFY41IUSZEjAc
DUFJERhFAkEawZH601ULORp8SHKDidyleYcZU8L7y9Y30XJYqELfdcfBgFUZEvQ
duRmJj7ryu0g0uurOTE+i8VnMg/ostxiswJBAOc64Dd8uLJWka6uug+XPr91oi0n
OfTm+xHrNK2jc+WmcSg3UJdnAI3uqMc5B+pERLq0Dc6hStehqHjUko3RnZECQEGZ
eRYWciE+Cre5dzfZkomeXE0xBrhecV0bOq6EKWLSVE+yr6mAl05Thrk9DCfPSOpy
F6rgN3QiyCA9J/1FluUCQC5nX+PTU1FXx+6Ri2ZCi6EjEKMhr7gHcABhMinZYOT
N59pra9UdVQw9jxCU9G7eMyb0jJkNACuEwakX3qi27b
-----END RSA PRIVATE KEY-----

```

Ключ RSA-2048 testRSA2048.

```

/* 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, 0x0C, 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 */
1020,
{ 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 }

```

Кодированная форма ключа RSA-2048.

```

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAsPnoGUOnrpiSqt4XynxA+HRP7S+BSObI6qJ7fQAVSPtRkqso
tWxQYLEYzNex5ZSHTGypibVsJylvCfuToDTfMu18b/CZjP2Ob0LdpYrNH615hvFE
89FU1nzQF15oVLOpUgA7wGiHuEVawrGfey92UE68mOyUVXGweJIVDdxqdMoPvNNU
186BU02v1BiEsXoiox+dWmuvV7vfyZ79Ttoh/LUK43YvJh+rhrv4nKuF7ihjVjBd9s
B6idJj70HF1dzOQ9r8SRI+9NirupPTkF5AKNe6kUhKJ1luB7S27ZkvB3tSTT3P59
3VVJvnzOjaA1z6Cz+4+eRvcysqhrRgFlwI9TEwIDAQABAoIBAEYiyDP29vCzx/+
ds3LqnI5BjUuJhXUnc6AWX/PCgVAO+8A+gZRgvct7PtZb0sm6P9ZcLrweomlGezI
FrL0/6xQaa8bBr/ve/a81550gcjFo6fzEw3Dz7ra5fbSiPmu4/b/kvrg+Br1177J
aun6uUAs1f5B9wW+vbR7tzbT/mxaUeDiBzKpe15GwcvbJtdIVMa2YErtRjc1/5B2
BGVXyvlJv0SILcIEMsHgnAFOp1ZgQ08adZvillQ8XVMOahAhP102A3X8hKdXPyrx
IVWE9bs9ptTo+eF6eNl+d7htpKGEZHUXinoQpWEBTv+iOoHsVunkeJ3vjLP3lyI/
fYONQ1ECgYEASRBXAjgvIys2gfU3keImF8e/TprLgelI2vbWmV2j6rZCg5r/AS0u
pii5CvJ5/T5vfJPNgPBy8B/yRDs+6PJ01GmnlhOkG9JAIPkv0RBZvR0PMBtbp6nT
Y3yo1lwamBVBfY6rc0sLTzosZh2aGoLzrHNMQFMGaauORzBFpY51U50CgYEAzPH1
u5DI6Xgeplvr8QvCUueEsCOgJg8Yh1UqVoY/SmQh6MYAv1I9bLgwrB3WW/7kqIoD
fj0aQV5buVZI2l0MomtU9KY5SFIsvPv+JuUpy7/+VE01ZQM5fY8wiYQCiVZYj9X
Wz5LxMNoz+gT7pwllCsC4N+R8aoBk404aF1gum8CgYAj7VTq7Zj4TFV7Soa/T1eE
k9y8a+kdoYk3BASpChJ29M5R2KEAYV9wrBklHTz8VzSTFTtKHEQ5W5csAhoL5Fo
qoHzFFi3Qx7MHESQb9qHyolHEMNx6QdsHUN7rLEnaTTyrXh3ifQtD6C0yTmFXUIS
CW9wKapOrnyKJ9nI0HcuZQKbQCMtoV6e9VGX4AEfpuHvAanMYQFgeBiYTkBklTQ
XwozhH63uMmOmS0G87Sz1TmrXadjAhy8gsG6I0pWan7QgBuFznQ/HOKwTm+gTkw
AsrZt4zeXNwsH7QXHEJCFnCMqw9QzEozTrNtHJhNboBuVnYcoueZEJrP8OnUG3r
UjmopwKBgAqB2KYUMUQAovYcBnEflDmyZv9BTvNHBR21KkMYqv5LlVdaBxVfile0
2ri04p6BaAdvzXjKeRrGNEKohNBPOSfYCOM16NjL8hIZB1CaV3WbT5oY+jp7Mzd5
7d56RZOE+ERK2uz/7JX9vSM/LbH9pJibd4e8mikDS9ntciqOH/3
-----END RSA PRIVATE KEY-----

```

Ключ RSA-4096 testRSA4096.

```
/* 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,
  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, 0xEE, 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,
0xD0, 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 }

```

Кодированная форма ключа RSA-4096.

```

-----BEGIN RSA PRIVATE KEY-----
MIIEKAIABAACAgEAs4tJYOY75qjbqJqC147x9jJE5Vd9jPWGFtXKv1nUnMjZNSM4
qjy5sRHBSX5bUa9pLyYR5on3Z1SAwLD0w2VPPQ6+F/oyK1zTgQqiToF/XZQJqC6D3
VsNEO76DPqFRANT7Nn7r1gVbZIZ3/H3r1CRNRR47tHGWBLaPnxz9/NY6UG8zkWP
97uXpJqYoRgH4Cwa05rTolc64YDh/0Mq5VgMycq/q2AvMlvNoJfoe8em1040qH1g
ikP+suT/8fs452hqmEddtRpuvQgXKldBd0kkiyFVYlK64NVA6Mso9MAK3J/kdYoa
w2SrOeThVSiYVEQVP+7GrUxTSLlJj/VQ9fpYM5eTNzDICIG/Ee7o/jhtWLEoSAMD
mUOr89lyIHaXuOwkeEaJhnVXKBCM8WiztxvKG2CnQD6cge3ZSmqJEhyEmjcAVC7ew
fnMxOnE+WJ6rZrf+mA5WMVn+FzyWx2AondWow0aUKHkaY7amHirsKp6PFIImyx
Flz8+cqDCmBswPsUh/JJ5eDHHIhibFcSgIHedsEjhLbUSLZ/DnejrU90qIWWA3R1
VIpykKfeZkZeInsrFzGPikkFKWFF+6KDdyvCmltYEzqz046tigXAZ5UgH8oiXERE4
8wO6X+FH+cLzQ0q3A8HZRNNDgqCjU/Tgy76iaku/Ic6eteedRlfx3gJ/IOUCAWEA
AQKCAgBq0bC7fN8gkU/2lM6jwFL14aT6CSjs6QWS+XRaHmNohW5dhZteimERqr3
nbyY8cKjsY0u5GCUUsnzqVRGOC0beP9Afb9Q4H2YSyDzrIvK6afaY08kiJI89VDC
Yzd+xjgbqRGIzI8fLLzoNMaG4b5xAf4eochgXm+P/Z1FZLt+M4TyV+qamjPTTUMH
fPOalMKaubd4G1PFvFc49m47+thI8N5uCJCrc5mCFbjt8AUGrETVvFRrtyBxttL7t
5gpoawAYT0ValTq7LmgR4c3qOVMLj66o+CQ2ecndfpeMXgFYV6ylnZ/kpiOVCA5i
av+OCT+VpOsBSscq3Eu8+w9YCMopsUCG6GzW4WD2akEBVA/X6D0JMcoYj/IHT3Xv/
G/eMji69A6URletliZhuSb0wBxryQaPMqAdsZ8eUYzCx/RwhKtPr032aTQqWlbgW
igiJMn1SbxbRVjf6nb8EsLg92LXEBS3FOLbK6ckuyXAQei8e5NR6Zcy1uVluQnSR
m+eR7JdkUP5YWNWuAehOvZIH2Oog+jcUDONQENZQHyJhLxgE3nNoD+YcIlyPTMMf
8G297mZtu5r7/a05ccMpdXve9cV4Wgcb6Urhigsu2K5nmrqmEIUoqF4xf4eomcWJ
9KiTQpCmyh758U2NcNpm3HULabGcs1gow+rwQiFcCarUqVTtoVQKCAQEA4EG98cm1
aaz16AItIRuHG18pIUglif0PbctZR2scaHQBjdeh4Qg5MnRe88Zs9/8xPulMsWgd
750pzD/oevftGenVNFziyct05uchqk6ZSWNMGRxpvtNrsKu74dx7yGi7oq03sTc
BDxwz7qJ5esvYuoHx0vUfmdpEqlYn7PtcCiPigPRkcWkiJbosg8e3pGAzTMDWfdf
SK/pfEbuWcknHnE3VUxXBVYXhI/TBbzWMEf2Riw0ZuGdn2PGETsJv/XldjVqqqfG
SsC/2dZe30svNnrB32kGIMIvYkTZydoFsTYrStXarLkP9YYzXs1+HXOWAMsas3Jp
Wz7HcXyH276TVwKCAQEAzPVRKdO5JMg4p2zTadRunLgT/jsuvHkrEBh0x0JE1AD
qy/COUMc2m6ZCIG96KBubjUcn9TrlctB207BSmbNOMIkfoKj1DkPj7v1cKh1Xg8q
wkPl+4dv0gtIdnOidy2pcMHfR6Mt6op15wlUcyKcaTyIajFtLOY/Al17BMqeyr2j
Nm4HZIgfmyRzb1326FaX2+YqsvjMcaX/dtKEm0B8rNhJxbsp2115RTtTXijIpC+
CoLxRBSZK9GAPa3Jg93ydtLK4aCpA/keeL48C8r1jzpzpRI6pshfzVHFCAf+R3rI
fgOLmpSsxiDeEiWbTRKDPs3ZVBejn7IasCG91VkiWkCAQAvfBwxN2nPB40+TD+s
E/0ewZ6e6RYzRF1hAt7tTXPNnu2PUDB5ytj5owr8D9cBCCswTOUBZ693DktMcXfT

```

```
meAwbyYV2CpiuaqMEXySs/imdDYaK/GHIBruukwihtYddgDzUz9AOn5EJfjbQlYof
ghYtlqqA+8Bz4f+wsOUQI/Qx3JTQP5C/khmMZI/vLB54OE0S/kFmamflp0IES6yq
nFpJKuXxjIBNI/ak3iNrao08A3DVWPzPsg7B0EmfsSDJPKsRjXpddxZ9chp4ueB
1pSvV2xZOQ7QIEj/ZGa3PogYBwVRukisbB9B+OglwFNlAHXqQxdrSd2f06zFjKMM
uaTPAoIBAFdahwkor9Q5ccwJ2eFVJJP+uhPbqDyTaTrFBZ/tWeLo+epHPfRwiunlu
fdLhHmGzU8jU5tEteQFPjMWD4AXHQds8mD5/LliQqaJwCxAOL+IgcNrmtdSvLaaGo
JW42wpa3mKsfplttvgroyyhEVkw+zDvF8UK49kt3gtza7cTFLKcoJ/OLWBviniQI
neuVRNKpdXfHlZnJ7vjT6E6FsZUY2Ke0REGawURO8lJ8pNdL/luQDS81t9aoYNAl
LnwbQbPuOJTkKowXiXGkD5Sun7D3A8nU0EXL6yuCYwYv39Jr1bhpYGI06J8tLqWr
BHr/eQnay2TU/Ts1EdfxuUGmZn9AbbkCggEBANEMkY2p8m2pTf87CSQ8jMPUOQJt
5iuenzenYLvXqVLLB4SUVXN+ZdplDJPELtf2SQIhrplrPNH/H01jnhWd0ecSjVY8
HBbIs52Uld5ek3/mWji4GeRp+Iw84CUh4q2p40bmoblRj8e9sh2ixhHjX2yJ591m
oGbLiZ75a60a05mUDKOFWt9cWHn4MKgIPKbWwFhYwmYDCjO/tK2DtcySny9soh5Q
KVQriuvna21E4YY+OUc7btmtkmp9v+LHKOI8dPabsOBUB8Z8UboGehSNrZTQwpx3E
p0riDg0UEzFmoYrfbvf+2VzEZDX/TJYjK9Vka8w5+xat8iS0/euKuvSRMb8=
-----END RSA PRIVATE KEY-----
```

2.2. Ключи DLP

Ниже представлены общеизвестные тестовые ключи для алгоритмов на основе DLP, таких как DSA, DH, Elgamal.

Ключ DLP-1024 testDLP1024.

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

Кодированная форма ключа DLP-1024.

```

-----BEGIN DSA PRIVATE KEY-----
MIIBuQIBAAKBGAMM38OPw+QhJ5CwpB5FtOTogN6Kv9Ouygsjj7bNcwzDGHaTntWx
gLKAKGg+S8GrhPzi/0ibUMLsnekewOzBYGT9DeU36rocbN0n3DAwSB6LuWCqi4rv
kzUw5rHMUWC7+q+FD/ZXgRIzfvMDTkFj3GUDvfiJJYEUH6uCVbbZcnuzAhUA7EG5
wGIdW9yvEdUZj3IiC5lu98CgYABZiesz82VUFHgbhxb70UsEmPHXsS2UE+0J1c1
woMyC2Oskcb0AgkyUxyrBLHncv3yneJOJxeXp90hl2dpMfkzHR9Z7uW6LH1UrhNc
f31BN9jYDrYpKI4miivr0h8WpAPxldrYPBxHgBejzSzvG6SbiQ3AiSEuciYdo2ev
gDsCUAKBgAiguULCXETAUrDRdoLqxDbqfoHsn3bhBXUyqmfq3QStuPlhgboLJfKE
2qqqBfPIQDTUF9N7bgpjMYoKeR8dDd2ivrjNadvqPy9tbdcwkmJH/cTRuC34wt
h66NNq253SUTV46LmapqDt9nX/wv3rZLJuW+2FmT/ZgRD8/J7fk4AhQR7Z14WoE6
Gw6W7NONf5vOnr/W+g==
-----END DSA PRIVATE KEY-----

```

Ключ DLP-2048 testDLP2048.

```

/* 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 }

```

Кодированная форма ключа DLP-2048.

```

-----BEGIN DSA PRIVATE KEY-----
MIIDTAIBAAKCAQADLdVtFTN6kTQ3016jQz2w57chKY+6hyfy+b6FbWoUa5KYjVCC
8sVyt3A3Y+gkVKekoiWbKazpsLybS02YXWqcjLYw5OCfSAefG+gHaXHeKmhWcLlM
yWh93CM7MK8i1LAWprSX9kb5ThwX6DqQTCwbaEQZqzSP2c1kBaFKpowrj3+L0G6f
ZMS7acy/vIBWrkFKiy411iBc3vsqJKN5uKEWF1CV/1f/YVUSHobZm44fJERjEnHw
nDNPNyJFL+kmP8M0m8zbZ1T/2JLEMnOH39QBigKupu9MY2p2nznrc3GRlySahB
owvgxL6OyxB/OALcRYP44BKU1StiE2e9DBlTAh0BlQmy7ag7CIJzGz/onC72nbjY
NhIOXRmpYO5EQKCAQAARF0SDkbsutaHiEfM6HCmntytyGyFnEm6963kHtk2jsI7
zFT7YOrarMZkKm/dMiuZqxRlgbIb6+BilOCC8VW+1QRsxw3OzmmfVGVHhcTQVxn
rO8YvGupTJVgDLW9qdyErVj1SR0mJh7U5TWtsi41sGzCtMidotxj4p7aBvATgHJG
VYky6fLci5Mua4S0B/VxUJ0G95Qw6V1GstAmFCiEF5mYhqZxRe10agyowERBA/UD
5rvnRWHdRNGa5XqCz6G8PEKw7sWxZeorJmB+3BFhx7ZJykYdRwtLNePphk+hpZ
m8Aeb+mTC1H1ebCEAXQlunChAj+u3dxX0c5WJRzaaIBAAIwN7LZyZ51P9J5v/ze
6ZKcm6HeqpcLA3KvczLUCNE3QpnzYQJ8jwXVevtNEM0rRyS1Pwnr4oy/SZ9rT4Yz
SRmLJLKrDUzstsT9fmctSyrKnTnjriD47Nf9dxB85Upm3e6XROSM+NlrrqaUoxlHw
CMZvGSogTsf50HaRAXmMR2XW0klxWmQKfVRFKXnkbKTTib1I+PV2qORaVr4NT9
bOpjHF9TfvkYWY4wUi+TZFBmGMBFhmPv0HUSEiGkYPmAxAU+AHX1tIZ3yodvqPIod
oJ9r6Ru2KW15GiqDgOidDN0m92Y+BpqDMUmtRcSse5iHcfZUuB9Q4NcmQkfwEorr
sPkCHGQFvN6092gpAiPOXBuqijDCitx4AtloHty0NOU=
-----END DSA PRIVATE KEY-----

```

Ключ DLP-4096 testDLP4096.

```

/* 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, 0xEE, 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, 0xD0,
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, 0x7E,
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,
0xB8, 0x53, 0x33, 0xE1, 0x4A, 0xA8, 0xE9 }

```

Кодированная форма ключа DLP-4096.

```

-----BEGIN DSA PRIVATE KEY-----
MIIGXgIBAAKCAf8x01VfsuiJ8yCDeHla9IhbytATWL3x8C4rU0ivmLMkzRbbqj8
VAwJlCVu6CQPsXu2MauUl2ap+SzefCOBE7b9WqTKQmga20e1eVP5BbVVKZMV9C
SPVLge9fBU2Ngk4SrquCSyvwTF7eBGaw3DsWwoBZVoXKOMbnE9guTRv80z2H3iaV
S6AFvEIXdzmyDx5GE4B57eWRZM5nI+NR5LL81Q1uq7RdqI+kzVYkiupEqi5BuP8o
vTeIAIwu70vhkKCRX2APJq+18e3dLUPqDgN1/4rPYSFo9ia71HVA0Efc+Z554L
/zIUU1c+xQ2d1NCyujC0eQ4hieVA++UmFHj1Nxxq/OniG05dcEGJMT8o2zbWC06
SMbXCEeDboCLDiJTuPqKjFWjv+gwVNZIssyluKOxaJGtUjVukoca9ZmlbpDJND01
SL9QuK+ZRXIzsNz1AcMJsrfyowmHS1QIYhrUxOmf401N8yvWhkscnCr3egeDNF
HxItqeb9e40SEp7kmlYHXx03BQMBR02f7/LmgdKauF1JScT+dMzy5Gbw2EUB/f3
pNnhHtKfPwHV6nQMv6Fr0vu4CtK15jYER4CLHsUHLhW9tykJdk2tJ7qW36qQHmJ
FT3tMhJ2TQAG8Ak2KEuW1ovJdP2vd7ZFeDY4xR6xGIQRcqA33knaSBqbAicB/za2
Bok/U75BEvlgGfmcz7lgn5JQDaYL68kbtJdi8xSSNsryxMCGgH/GYkDGxK4g1lm
XJ9CMQkoGSe7EwsSrqsrv1UjOD69T7KOGeq5hh9X2PA9mtW6ActXQ1YjKq1vOa9
M5drus1oY9HCbk9IY2cFY/ucpRZcPJ8UHS59d6YR1VvNnOajJbk0K18K3GB+7Wnz
LHhnjF8wLK+XVvzAl1Lsv6X/cktZSSEczi7T2BQer6u2KGXC8qZEpdw0DyQpC2FT
PGVkzZ4zt1jBOXHs2mYUHHmliH6iRh41pror0CCA+OXGyL57+71s9B8H1b3JZQC1
bFNLcDazVo9wC5rV7/we6L4vcD1QrNO4jCQ/gqLp9QHjh4ROd6qQLcDX2W6+Tkvi
s6sJZKwosVTNFTWkBlVAgzmOC+asmyb/mvTCzalVF1EVL71Mwtfxmp5/QaVuu+88
1R32sQhIBhW08+2Zn+x/DzxTh1UncHSzqA1LaoRxxJuG53+I41vWx11ODmxin5mk+
n7E9EVijq690BGJ965YS2V1NMyYa5ZnN/8rew7Wv/8vf7UULU4vI2I0pjt0nszbo
9e5tRh9XQDu0bbwEttkAx0hyjeePaI/NmpApTuqV585IKjmwYugE/Mtu99E11Lk1
DsIPtQkOTE4w1sWQqiljeHkNgZ7CxQ3V9Ub14+Tzaewz2kVSNegXKR4h7Xomwnm
ss8NVkPDhUgBiod7WhdyQCtLkfnCiWKAf8qSRFzGGURS4psb45AfVXDmrcQu0XK
upTmsYWH0o+cbG1MAZoJsm9EjCoZVaVnsaDIYYIuGcb63oxDqmHDvzm2leKidFuv
6Fx2W4oe940bQpFvTDE/6NvyIhEwxe6R+ePTu/KcxHsbq68XnLqL1FupYdcKtr16
oHX7KhUzFPw7LDuJhm5oLHqVjTt4h/DX2PQN9V5uUV0fu4h3jq+08ejeZp0IMBm
fkjsGv6ELrE20t3uU66Sp2psCBWdH0BrZoX+hbQajYBJORivUpmhxqET3i+XQN
zyfEuigqZV1qTucVAS4MdQzDseXA8ivIKtI+tmDs9ICst9cxIVfbt+DlI3jp/0bu
7wSvR08sTFFx/895i5A/SepD0GDvI+19Y417yy/xOasNgF/3hYfM5vHyZjkHu9pa
ZznPYkcsOHGfGNr+kHxL6ojcrjkbBzq2zGC1YMmk1jMeKfik/rmZpkrk28e/AiKp
1Bk6I0gbQDDzKOopy3ySYgSYR0/LZNRhu9eeSpwEdkde8PmrXomuTVqun4dgIfoL
soIXzyeNount3BxVx14X3A2UjgLBf7fdAcF2NzcnUuc5oCTZXSUAUV4FF3iW8Sn9
/7X/SvV8ZNF7OyOdhtyZ/otjPWXXoTC76wY3xby2Jgm5AnAOHvCuVs0NBiYxqXG
KFS4UzPhSqqjpaicBp3cRuJ1FUycpAboJWn/8FJyMBbAv3QONyZiXEVvOw+YU81V/
nAw=
-----END DSA PRIVATE KEY-----

```

2.3. Ключи ECDLP

Ниже представлены общеизвестные тестовые ключи для алгоритмов на основе ECDLP, таких как ECDSA и ECDH.

Ключ P256 testECCP256.

```

/* 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 }

```

Кодированная форма ключа P256.

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEOBwLW92AqkWunJXowVR2Z5/+yVPBAFhNEedDk5WJxk/BoAoGCCqGSM49
AwEHoUQDQgAEQIvI+I+3gv+17KN0RFLHKh5Vj71vc75eSOkYMsxFxbFsTNEMLjV
uKFxOelIgsiZJKZNCX0FBmrfpCkKk1Ccg==
-----END EC PRIVATE KEY-----
```

Ключ P384 testECCP384.

```
/* 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 },
/* cy */
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 }
```

Кодированная форма ключа P384.

```
-----BEGIN EC PRIVATE KEY-----
MIGkAgEBBDDiVjMo36v2gYhga5EyQoHB1YpEVkMbCdUQs1/syFMHyghig+iZxNx
qagbrA41dJ2gBwYFK4EEACKhZANiAARbCQG4hSMpbrkZ1Q/6GpyzdLxNQJWgKcV+
yhGx2VrbtUc0r1cL+CtyKM8ia89Mjd28/jsaOtOUMO/3Y+HWjS4VHZFyC3eVtY2m
s0Y5YtqPubWo2kjGdHEX+ZGehCTzfsq=
-----END EC PRIVATE KEY-----
```

Ключ P521 testECCP521.

```
/* 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 },
/* cy */
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 }
```

Кодированная форма ключа P521.

```
-----BEGIN EC PRIVATE KEY-----
MIHcAgEBBEIB2StcygqIf42Zdno32HTmN6Esy0d9bghmU1ZpTWi3ZV5QaWOP3ntF
yFQBpCd6NbGGVbhMlmpgIglA+R7Z9RRYAucqBwYFK4EEACOhgYkDgYYABAHQ/XJX
qEx0f1YlDcBzhdvr8vUr61gIPbgv3RUx2KrjzIdf8C/3+i2iYnJrYtbs9dZJ44y
FzagYoy7swMituYY2wD2KtIEkxYDwbyBirIWG/Dw/A7FquikKbc85W8A3psVfB5c
gszPVi/K3vxKTCj200LPPvYW/ILTO3KFySHyvbz92A==
-----END EC PRIVATE KEY-----
```

3. Взаимодействие с IANA

Этот документ не требует действий IANA.

4. Вопросы безопасности

Цель публикации известных ключей в таком виде состоит в том, чтобы эти ключи можно было легко распознать как тестовые. Эти ключи никогда не следует применять или полагаться на них в действующих средах.

Авторы ожидают неизбежных CVE (Common Vulnerabilities and Exposures).

Адреса авторов

Peter Gutmann

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

Corey Bonnell

DigiCert
Email: corey.bonnell@digicert.com

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru