ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ
(РОССТАНДАРТ)

Технический комитет 026

«Криптографическая защита информации»

СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ

ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ПО ЗАДАНИЮ ПАРАМЕТРОВ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В СООТВЕТСТВИИ С ГОСТ Р 34.10-2012

Проект первой редакции,
ноябрь 2013,
rus-vop-lse-svs_ecc2012-00-rf

Москва

2013

Содержание

1. Введение

Документ определяет параметры эллиптических кривых стандарта **ГОСТ Р 34.10-2012** для случая эллиптических кривых с простым модулем p длины 512 бит, а также их идентификаторы. Данные параметры рекомендуются для совместимых реализаций протоколов ключевого обмена и схем электронной подписи в соответствии со стандартом **ГОСТ Р 34.10-2012**.

В случае эллиптической кривой с модулем p длины 256 бит предлагается использовать параметры, определённые в **RFC4357**.

Данный документ не отменяет использование иных параметров эллиптических кривых.

2. Область применения

Настоящий документ рекомендуется применять в системах защиты аутентичности данных на основе электронной подписи на базе стандарта электронной подписи ГОСТ Р 34.10-2012 в общедоступных и корпоративных сетях для защиты информации, не содержащей сведений, составляющих государственную тайну.

2.1 Текущий статус документа как проекта методической рекомендации ТК26

Передача проекта настоящей спецификации в ТК26 означает, что каждый ее автор соглашается с не эксклюзивным предоставлением IPR для ТК26, аналогично положениям стандарта Интернет IETF BCP 79.

Данный предварительный документ является открытым документом «Рабочей группы по сопутствующим криптографическим алгоритмам, определяющим ключевые системы» и Технического комитета по стандартизации «Криптографическая защита информации (ТК26)». Область распространения документа не ограничена.

При цитировании или ссылке на него из других документов следует ставить отметку «документ готовится к публикации».

Список предварительных документов ТК26 доступен по ссылке <http://www.tc26.ru/>.

3. Нормативные ссылки

Указанные в этом разделе спецификации ссылочные документы являются обязательными для их применения. Для датированных ссылок используют только указанное здесь издание. Для недатированных ссылок - последнее и актуальное издание со всеми изменениями и дополнениями:

ГОСТ 28147-89 — Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации, Государственный стандарт Союза ССР. Системы обработки информации. Защита криптографическая. «Алгоритм криптографического преобразования ГОСТ 28147-89», ГОСТ 28147-89, ИПК Издательство стандартов, 1996.

ГОСТ Р 34.10-2012 — Федеральное Агентство по техническому регулированию и метрологии. Национальный стандарт Российской Федерации, Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

3.1 Дополнительные ссылки

RFC4357 — В. Попов, И. Курепкин, С. Леонтьев, «Дополнительные алгоритмы шифрования для использования с алгоритмами по ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001 и ГОСТ Р 34.11-94» (Popov V., Kurepkin I. and S. Leontiev, Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms, IETF RFC 4357, January 2006).

4. Аннотация

Предлагаются параметры двух эллиптических кривых в соответствии с **ГОСТ Р 34.10-2012**. Наборы параметров имеют следующие идентификаторы:

I) id-tc26-gost-3410-12-512-paramSetA, «1.2.643.7.1.2.1.2.1.»
II) id-tc26-gost-3410-12-512-paramSetB, «1.2.643.7.1.2.1.2.2.»

5. Параметры

Для каждой эллиптической кривой параметры представлены значениями **p**, **a**, **b**, **q**, **x**, **y**, приведенными в виде чисел в десятичной и шестнадцатеричной системах счисления.

p – модуль, **a**, **b** – коэффициенты уравнения эллиптической кривой в канонической форме, **q** – порядок группы точек эллиптической кривой, (**x**,**y**) – порождающий элемент группы.

Кроме того, оба набора параметров представлены в виде структуры следующего типа:

```
SEQUENCE {
          a       INTEGER,
          b       INTEGER,
          p       INTEGER,
          q       INTEGER,
          x       INTEGER,
          y       INTEGER
         }
```

5.1 Набор параметров I. id-tc26-gost-3410-12-512-paramSetA.

p (*в десятичной системе счисления***) =** $2^{512}-569$

p (*в шестнадцатеричной системе счисления***) =** 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFDC7

a (*в десятичной системе счисления***) =** $-3 = 2^{512}-572$

a (*в шестнадцатеричной системе счисления***) =** 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFDC4

b (*в десятичной системе счисления***) =** 1219058002426623015618942475834009407551484
4064736231252208772337825397464478540423418981074322718899427039088997221609947354520590448683948135300824418144

b (*в шестнадцатеричной системе счисления***) =** 0xE8C2505DEDFC86DDC1BD0B2
B6667F1DA34B82574761CB0E879BD081CFD0B6265EE3CB090F30D27614CB4574010DA90DD862EF9D4E
BEE4761503190785A71C760

q (*в десятичной системе счисления*) = 13407807929942597099574024998205846127479365820592393377723561443721764030073449232318290585817636498049628612556596899500625279906416653993875474742293109

q (*в шестнадцатеричной системе счисления*) = 0xFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF27E69532F48D89116FF22B8D4E0560609B4B38ABFAD2B85DCACDB1411F10B275

x = 3

y (*в десятичной системе счисления*) = 61285671321593683755506766505341533718267088079063531322960495468664645454726071191345292217033369215164051073690286061910977477383675719244666942367955 56

y (*в шестнадцатеричной системе счисления*) = 0x7503CFE87A836AE3A61B8816E25450E6CE5E1C93ACF1ABC1778064FDCBEFA921DF1626BE4FD036E93D75E6A50E3A41E98028FE5FC235F5B889A589CB5215F2A4

```
SEQUENCE
{
    OBJECT IDENTIFIER
    id-tc26-gost-3410-12-512-paramSetA
    SEQUENCE
    {
     INTEGER
      00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
      C4
     INTEGER
      00 E8 C2 50 5D ED FC 86 DD C1 BD 0B 2B 66 67 F1
      DA 34 B8 25 74 76 1C B0 E8 79 BD 08 1C FD 0B 62
      65 EE 3C B0 90 F3 0D 27 61 4C B4 57 40 10 DA 90
      DD 86 2E F9 D4 EB EE 47 61 50 31 90 78 5A 71 C7
      60
     INTEGER
      00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FD
      C7
     INTEGER
      00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
      FF 27 E6 95 32 F4 8D 89 11 6F F2 2B 8D 4E 05 60
      60 9B 4B 38 AB FA D2 B8 5D CA CD B1 41 1F 10 B2
      75
```

```
      INTEGER 3
      INTEGER
       00 75 03 CF E8 7A 83 6A E3 A6 1B 88 16 E2 54 50
       E6 CE 5E 1C 93 AC F1 AB C1 77 80 64 FD CB EF A9
       21 DF 16 26 BE 4F D0 36 E9 3D 75 E6 A5 0E 3A 41
       E9 80 28 FE 5F C2 35 F5 B8 89 A5 89 CB 52 15 F2
       A4
     }
 }
```

5.2 Набор параметров II. id-tc26-gost-3410-12-512-paramSetB.

p (*в десятичной системе счисления***) =** 2^{511}+111

p (*в шестнадцатеричной системе счисления***) =** 0x80000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 00006F

a (*в десятичной системе счисления***) =** -3 = 2^{511}+108

a (*в шестнадцатеричной системе счисления***) =** 0x8000000000000000000000000000000 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 000006C

b (*в десятичной системе счисления***) =** 5472517130514047254760433071281657274171034389553769779747941603125796549693907036696237273952702637857580071293254240945079496484373854264998452887027990

b (*в шестнадцатеричной системе счисления***) =** 0x687D1B459DC841457E3E06CF6F5E2 517B97C7D614AF138BCBF85DC806C4B289F3E965D2DB1416D217F8B276FAD1AB69C50F78BEE1FA310 6EFB8CCBC7C5140116

q (*в десятичной системе счисления***) =** 6703903964971298549787012499102923063739682910296196688861780721860882015036922585419853748190383615062910947743405567510148398820717100282856877776119229

q (*в шестнадцатеричной системе счисления***) =** 0x80000000000000000000000000000000 0000000000000000000000000000000149A1EC142565A545ACFDB77BD9D40CFA8B996712101BEA0EC6346 C54374F25BD

x = 2

y (*в десятичной системе счисления***) =** 1391087797795557258711735874750463328666729297647553860794340434982072762491277963324668489993185089365703033494204180568181905548968011075910357787492797

y (*в шестнадцатеричной системе счисления***) =** 0x1A8F7EDA389B094C2C071E3647A8940F 3C123B697578C213BE6DD9E6C8EC7335DCB228FD1EDF4A39152CBCAAF8C0398828041055F94CEEEC7 E21340780FE41BD

```
SEQUENCE
{
    OBJECT IDENTIFIER
    id-tc26-gost-3410-12-512-paramSetB
    SEQUENCE
    {
     INTEGER
      00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      6C
     INTEGER
      00 68 7D 1B 45 9D C8 41 45 7E 3E 06 CF 6F 5E 25
      17 B9 7C 7D 61 4A F1 38 BC BF 85 DC 80 6C 4B 28
      9F 3E 96 5D 2D B1 41 6D 21 7F 8B 27 6F AD 1A B6
      9C 50 F7 8B EE 1F A3 10 6E FB 8C CB C7 C5 14 01
      16
     INTEGER
      00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      6F
     INTEGER
      00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      01 49 A1 EC 14 25 65 A5 45 AC FD B7 7B D9 D4 0C
      FA 8B 99 67 12 10 1B EA 0E C6 34 6C 54 37 4F 25
      BD
     INTEGER 2
     INTEGER
      00 1A 8F 7E DA 38 9B 09 4C 2C 07 1E 36 47 A8 94
      0F 3C 12 3B 69 75 78 C2 13 BE 6D D9 E6 C8 EC 73
      35 DC B2 28 FD 1E DF 4A 39 15 2C BC AA F8 C0 39
      88 28 04 10 55 F9 4C EE EC 7E 21 34 07 80 FE 41
      BD
    }
```

УДК 351.864.1:004:083.131 **ОКС 35.040** **П85**

Ключевые слова: *алгоритмы шифрования, безопасность*

Руководитель организации-разработчика:

Генеральный директор
ООО «КРИПТО-ПРО»

_____ Чернова Н.Г.

Руководитель разработки:

Директор по научной работе
ООО «КРИПТО-ПРО»

_____ Попов В.О.

Авторы документа:

Технический Директор
ООО «КРИПТО-ПРО»

_____ Леонтьев С.Е.

Заместитель начальника
отдела защиты информации
ООО «КРИПТО-ПРО»

_____ Ошкин И.Б.

Ведущий инженер-аналитик
ООО «КРИПТО-ПРО»

_____ Смышляев С.В.