Министерство науки и высшего образования Российской Федерации
Санкт-Петербургский Политехнический Университет Петра Великого
—
Институт компьютерных наук и кибербезопасности
Высшая школа кибербезопасности

ЛАБОРАТОРНАЯ РАБОТА № 3

«Протокол электронной цифровой подписи ГОСТ Р 34.10-2018»

по дисциплине «Криптографические методы защиты информации»

Выполнил
студент гр. 5151004/90101 Кондачков Е.Д.

Преподаватель
Ассистент Ярмак А.В.

Санкт-Петербург
2023

Содержание

Элементы оглавления не найдены.

1. Цель работы

Изучение протокола электронной цифровой подписи ГОСТ Р 34.10-2018, безопасность которого основана на задаче дискретного логарифмирования в группе точек эллиптической кривой.

2. Задачи работы

Согласно варианту разработать программу, реализующую криптоситему, поддерживающую формирование и проверку подписи по алгоритму ГОСТ Р 34.10-2018, а также допускать возможность использования различных ключей.

3. Ход работы

В ходе данной работы был реализована программа, позволяющая подписывать и проверять электронную цифровую подпись по алгоритму ГОСТ Р 34.10-2018. Для выполнения работы был получен вариант задания от преподавателя.

Вариант 10

```
p = 57896044623332830704464930175758866532580959320654190378215212919875855638347
r = 28948022311666415352232465087879433266289459622068172692541485718987902249339

a = 1
b = 35800948915040763394854698676083084630967836106516964913271803528707388006 22
xP = 34716160583222611645030789937385729759908872067425542316787922148347820731789
yP = 58988212064147591382013637178025684997934448166901693688396851241678354665 30
```

Рисунок 1 – Вариант задания

Для проверки программы использовался файл с простейшим текстом

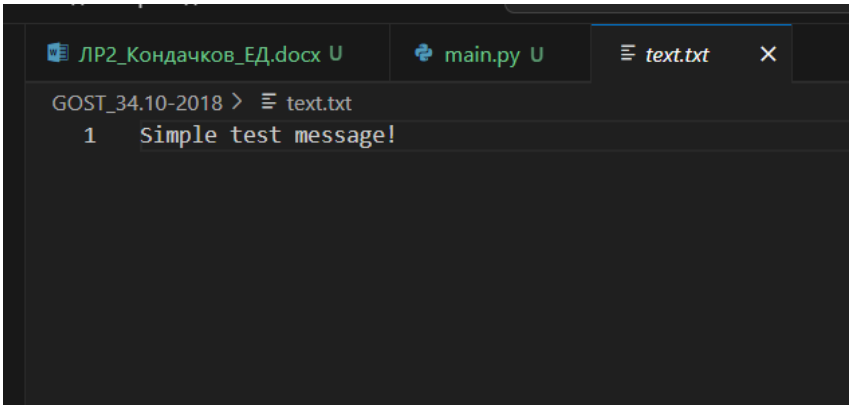

Рисунок 2 – Тестовый файл

Для формирования подписи были сгенерированы дополнительные параметры: ключ шифрования d и точка Q – использующаяся в качестве ключа расшифрования (Q = d*P).

```
Available fighters:
1. Willy Wonka (create signature)
2. Frodo Baggins (verify signature)

Choose your fighter: 1
Parameters were successfully generated!

xQ: 473813966279748192015883997775618416482647070789653760961765735632129161882 47
yQ: 532936249327746340686324588998731321934260159415598557122737115653250123533 5
d: 74032974420292903135071441799594433289190743388601719038257636498972242787 72

Enter the path to the file: text.txt
28483392354162546589754862573083300886693610932850336662336493899028635950388525478633712559922916240330821812918805756033730506122096234098129315131817 95
Sign was successfully generated!
```

Рисунок 3 – Сгенерированные параметры и хеш сообщения.

По всем указанным данным была получена ЭПЦ.

^text.txt

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Декодированный текст

00000000   30 82 01 53 31 82 01 4D 30 82 01 49 04 04 80 06  0‚.S1‚.M0‚.I..Ђ.
00000010   07 00 30 44 02 20 68 C0 EB 8E 01 A6 58 39 64 65  ..0D. hАлЋ.¦X9de
00000020   81 16 F4 0E 6D 07 2B 50 EA 41 F0 29 6D A5 DA 72  Ѓ.ф.m.+PкAр)mҐЪr
00000030   67 83 1A D9 E4 57 02 20 0B C8 4F F1 64 A0 A4 16  gѓ.ЩдW. .ИOcd ¤.
00000040   F1 21 FF 95 75 65 82 39 FA D8 F1 2D EA 04 26 24  с!я•ue‚9ъШс-к.&$
00000050   DF 8D 40 9E C9 59 46 87 30 81 B4 30 23 02 21 00  ЯЌ@ћЙYF‡0Ѓґ0#.!.
00000060   80 00 00 00 2C 63 A5 7B BB F1 FF 61 2D 43 7F 56  Ђ...,cҐ{»сяа-C.V
00000070   F9 75 44 D4 47 C2 76 83 6A DF C6 08 39 3A DF 4B  щuDФGBvѓjЯЖ.9:ЯK
00000080   30 25 02 01 01 02 20 07 EA 43 0B EA 86 89 5C 08  0%.... .кC.к†‰\.
00000090   30 F3 89 AC 27 06 BE C0 9E 04 C7 CC B0 D8 DD A7  0у‰¬'.sАћ.ЗМ°ШЭ§
000000A0   42 6C 29 F8 37 AF EE 30 44 02 20 4C C0 A6 8B A2  Bl)ш7Їo0D. LА¦‹ў
000000B0   AA 93 98 4B 4A 7E 36 40 43 0D 27 17 38 A5 F6 34  Є“.KJ~6@C.'.8Ґц4
000000C0   D2 9B 19 3A 6C F4 6A 89 FD 6D 8D 02 20 0D 0A 9D  Т›.:lфj‰эmЌ. ..ќ
000000D0   4F 01 A2 C9 BF 77 3D 65 5F CB F2 C4 E2 B8 8C 49  O.ўЙїw=e_ЛтДвёЊI
000000E0   BD CC 72 67 A6 5D 69 41 23 32 9A 3B 22 02 20 40  SMrg¦]iA#2љ;". @
000000F0   00 00 00 16 31 D2 BD DD F8 FF B0 96 A1 BF AB 7B  ....1TSЭшя°–Ўї«{
00000100   F6 2E A5 45 7E 32 68 FF 7C F3 5A 69 67 69 7B 30  ц.ҐE~2hя|уZigi{0
00000110   44 02 20 1C 65 DB 44 CF 8E B4 BF 5F 17 0D 6F 25  D. .eЫDПЋґї_..o%
00000120   FD 1F 6D 02 D3 7B CA BD D2 42 8D 5A 75 87 C0 64  э.m.У{KSTBЌZu‡Ad
00000130   AA D1 6B 02 20 26 B1 4A 68 4D B5 1A 11 77 0C AF  ЄCk. &±JhMµ..w.Ї
00000140   22 F5 5A 02 9E F3 08 1A E6 B5 36 C4 A8 1C 78 F4  "xZ.ћу..жµ6ДЁ.xф
00000150   13 C7 92 CE 2B 30 00                              .З’О+0.
```

Рисунок 4 – Сформированная подпись в шестнадцатиричном виде

```
Certificate  SEQUENCE  (2 elem)
   tbsCertificate  TBSCertificate  [?]  SET  (1 elem)
      serialNumber  CertificateSerialNumber  [?]  SEQUENCE  (4 elem)
         OCTET STRING  (4 byte) 80060700
         SEQUENCE  (2 elem)
            INTEGER  (255 bit) 473813966279748192015883997775618416482647070789653760961765735632129…
            INTEGER  (252 bit) 532936249327746340686324588998731321934260159415598557122737115653250…
         SEQUENCE  (4 elem)
            SEQUENCE  (1 elem)
               INTEGER  (256 bit) 57896044623332830704464930175758866532580959320654190378215212919875…
            SEQUENCE  (2 elem)
               INTEGER  1
               INTEGER  (251 bit) 35800948915040763394854698676083084630967836106516964913271803528707…
            SEQUENCE  (2 elem)
               INTEGER  (255 bit) 34716160583222611645030789937385729759908872067425542316787922148347…
               INTEGER  (252 bit) 58988212064147591382013637178025684997934448166901693688396851241678…
            INTEGER  (255 bit) 28948022311666415352232465087879433266289459622068172692541485718987…
         SEQUENCE  (2 elem)
            INTEGER  (253 bit) 12844724651458746428736183530639449905316741759471960873106692026814…
            INTEGER  (254 bit) 17501133717877560099626025154459342943463898910034135438713678592813…
   signatureAlgorithm  AlgorithmIdentifier  SEQUENCE  (0 elem)
```

Рисунок 5 – Расшифрованная подпись

4. Ответы на контрольные вопросы

1. Перечислите преимущества криптосистем на эллиптических кривых по сравнению с другими криптосистемами.

– На эллиптических кривых сложность алгоритма дискретного логарифмирования намного выше;

– Криптосистемы на эллиптических кривых для представления ключа требуют меньше бит, что приводит к упрощению многих операций, а также снижению требований к системе.

2. Почему в стандарте ГОСТ Р 34.10-2018 введено требование $\#E(\mathbb{F}p) \neq p$?

Если $E(\mathbb{F}p) = p$, где $E(\mathbb{F}p)$ – множество точек. Если p простое, то это означает, что порядок эллиптической кривой является простым числом и может быть уязвимой для атаки по сведению задачи дискретного логарифмирования к вычислению квадратного корня.

3. Если нарушитель имеет возможность обращать хэш-функцию, как он может подделать сообщение и подпись?

Может изменить исходное сообщение, вычислить новый хэш и подписать своим приватным ключом. В таком случае, при проверке подписи получатель будет считать подпись действительной, так как хэш соответствует исходному сообщению.

4. Почему случайный показатель k не должен повторяться в течение времени жизни ключа?

Случайность показателя k является гарантом уникальности значений подписи и её надежности.

5. Выводы по работе

Была разработана программа реализующая алгоритм подписи ГОСТ Р 34.10 – 2018, получены знания об устройстве механизма подписи на основе дискретного логарифмирования на эллиптических кривых и изучены преимущества данной схемы.

Приложение А