

**МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И.УЛЬЯНОВА (ЛЕНИНА)
Кафедра ИБ**

**ОТЧЁТ
по лабораторной работе №8
по дисциплине «Криптография и защита информации»
Тема: Изучение цифровой подписи**

Студент гр. 6304
Преподаватель

Корытов П.В.
Племянников А.К.

Санкт-Петербург
2019

Цель работы

Исследовать алгоритмы создания и проверки цифровой подписи, алгоритмы генерации ключевых пар RSA, DSA, ECDSA и получить практические навыки работы с ними, в том числе и в программном продукте CrypTool 1.

1. Генераторы ключевых пар

1.1. Основные теоретические положения

1.1.1. RSA

1. Генерация двух больших простых чисел p, q
2. Вычисление $n = p \cdot q$
3. Выбор $e < n$, взаимно простого с $\varphi(n)$
4. Вычисление $d : e \cdot d = 1 \bmod \varphi(n)$
5. (e, n) — открытый ключ, d — закрытый ключ, p, q — уничтожаются

1.1.2. DSA

1. Выбирается p длиной $[512, 1024]$ бит с числом битов, кратным 64.
2. Выбирается число q с тем же размером дайджеста 160 бит, такое, что $(p - 1) = 0 \bmod q$
3. Выбирается $e_1 : e_1^q = 1 \bmod p$
4. Выбирается $d \in \mathbb{Z} : d < q$, вычисляется $e_2 = e_1^d \bmod p$
5. (e_1, e_2, p, q) — открытый ключ, d — закрытый ключ

1.1.3. ECDSA

1. Выбирается эллиптическая кривая $E_p(a, b)$, p — простое число
2. Выбирается q — простое число — порядок одной из циклических подгрупп группы точек эллиптической кривой: $q \times (x_0, y_0) = 0$
3. Выбирается закрытый ключ — d
4. Выбирается точка на кривой $e_1 = (x_1, y_1)$
5. Выбирается точка на кривой $e_2 = d \times e_1$
6. Открытый ключ — (a, b, q, p, e_1, e_2)

1.2. Формулировка задания

1. Перейти к утилите «Digital Signatures/PKI->PKI/Generate...».
2. Сгенерировать ключевые пары по алгоритмам RSA-2048, DSA-2048, EC-239. Зафиксируйте время генерации в таблице.
3. С помощью утилиты «Digital Signatures/PKI-> PKI/Display...» вывести

сгенерированный открытый ключ и сохранить соответствующий скриншот.

1.3. Ход работы

1. Открыта утилита генерации ключей.

Generation of Asymmetric Key Pair

Algorithm

☒ RSA
Bit length of RSA modulus: 1024

☐ DSA
Bit length of DSA prime number: 1024

☐ Elliptic curves
Identifier (bit length and curve parameter): prime239v1

User data

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

Last name: Pavel

First name: Korytov

Key identifier (optional):

PIN: ****

PIN verification: ****

The domain parameter of the selected elliptic curve will be shown below.

| Parameters | Value of the parameter | Bit len... |
|------------|------------------------|------------|
| | | |

Base for presentation of numbers

☐ Octal ☒ Decimal ☐ Hexadecimal

Generate new key pair... PKCS #12 Import Show key pair... Close

Рисунок 1. Интерфейс утилиты генерации ключей

2. Измерено время генерации ключевых пар.

| Алгоритм | Время создания ключа (с.) |
|----------|---------------------------|
| RSA-2048 | 2.938 |
| DSA-2048 | 9.343 |
| EC-239 | 0.014 |

3. Полученные сертификаты:

Листинг 1. сертификат с DSA-2048

```

1  Version:                2 (X.509v3–1996)
2  SubjectName:            CN=Korytov Pavel [1576328015], DC=cryptool, DC=org
3  IssuerName:             CN=CrypTool CA 2, DC=cryptool, DC=org
4  SerialNumber:           C1:C5:9D:B5:B0:ED:58:C6
5  Validity — NotBefore:   Sat Dec 14 15:53:44 2019 (191214125344Z)
6                        NotAfter:   Mon Dec 14 15:53:44 2020 (201214125344Z)
7  Public Key Fingerprint: ECA4 959C 25A4 91F4 C141 0D19 2007 EC14
8  SubjectKey:             Algorithm NIST–DSA (OID 1.3.14.3.2.12),
9                        DSA prime p (no. of bits = 2048):
10                        0  FF9C4976 1BD7309A 0DE01B7C A1D36F52
11                        10 337A9441 AF107FFA EAA7B05D C659C55E
12                        20  C3C8E741 63496435 18B071E8 4A2359EB
13                        30  32CFAC12 C892F704 63823D1A 3E61EABB
14                        40  6B049E81 EBEF7281 31CB4F05 94597E86
15                        50  F6D99A9E 3684512C D3CCA7FA 03ED14A8
16                        60  456F2E3F D786B886 532474D9 4B17BFC6
17                        70  E99C86E6 C7FB2323 04448A14 714D0B82
18                        80  021602BC 1B924C88 6B91D89A BF4CDB88
19                        90  506DF7C9 2D3839DF E4A850A4 229EF1C9
20                        A0  294BC928 16E53A27 CE0D46D0 51BF623C
21                        B0  BC5A4EF8 3D613AB7 0B9AB54A 48336B47
22                        C0  DC519FFE 038F017F 283F0B55 FD4F9509
23                        D0  C1294CD3 F4980CBE BF34C15C DC4E6097
24                        E0  E18AE59D BF6DEDDF A862C13E 1F922AD9
25                        F0  E00D6F82 CD140E97 0850AF9A 62ABE6E5
26                        DSA prime q (no. of bits = 160):
27                        0  8C5DE7DD 4B519D7C 77A13EB4 D799C3A1
28                        10  4C03D457
29                        DSA base g (no. of bits = 2048):
30                        0  FD73D8DD 3C8B90A2 AADE22DD 7AF1AC50
31                        10  9603AB27 C30DFB83 20CA2BE5 AC29663E
32                        20  69D66E5D 4E10C19F C9C610C8 AF6BC387
33                        30  437CEC82 6C444F84 893D4201 840A2709

```

```

34      40 77E38D7F DA52B44E 5746C629 2A07F957
35      50 82D2C692 F73FAAD1 EE258402 4AD13BC2
36      60 327B3337 AD31EEDE 6A803B31 DE74C7BE
37      70 847C91E0 A2E1E6D1 282C01DD 5C975B81
38      80 9A845EDD 641123C0 03F8DC02 61DEC5D4
39      90 C9E61243 74AF8A74 44B99C0A 52D8333F
40      A0 E078086A 69FEADED 32818A2C 89EF85D7
41      B0 124B10FD 10EA4171 52623091 6C0152DD
42      C0 ED508E56 8D7BA365 3E22A918 9104714F
43      D0 CFB647BD 60D0E194 26F489B3 452CCCE7
44      E0 334AFEC2 4CCC392E AEB3367F 70DD4811
45      F0 96D5B975 0707DC1B 2C12D0CC D6B030A3
46      Public y (no. of bits = 2048):
47          0 FCB8FB62 04942D20 CD5B19E1 7BD1206F
48         10 AA03E4EE 132EEE78 F99E0210 047299C8
49         20 C1EC2F30 D29BF7A7 5AA210A7 B141EC2F
50         30 73F93C99 01040F15 DCBFF4D1 4F44F720
51         40 5D4009F8 FA09896B 78B89EC0 7AA8962A
52         50 BD842A9F 779EA2A6 B76C0631 69D89F08
53         60 D0966519 893C68CC 767E82EB 498DB831
54         70 D4DDC4DC 2AF2440E 35D43DF3 14B0BD56
55         80 878C99BD E9E01ABA F2DD3C25 0FD2D129
56         90 70E0AA42 BC6B491A BACA22BE 3DC77CE7
57        A0 5473816C DC6E29EF 878196F4 A1382668
58        B0 CC63CBA8 62E2E892 C881A7EE 6798DBD5
59        C0 B0830CA1 ADE3A419 217DDA8C 4CE69DED
60        D0 D38B2AC0 7FBFEB1B 303B11C0 8EBC3057
61        E0 A6ED1A96 A64E9A0E 6DBDB7D7 E9ADC743
62        F0 C0362E46 96921A7D D72050C5 CFE5FF54
63      Certificate extensions:
64      Private extensions:
65          OID 2.206.5.4.3.2:
66              PrintableString:
67                  |[Pavel][Korytov][DSA—2048][15763|
68                  |28015]                                |
69
70      SHA1 digest of DER code of ToBeSigned:
71          0 C4269313 FAC1E183 3F8C9D0C 43755F1C
72         10 A9A9990E
73      Signature:                                     Algorithm sha1WithRSASignature (OID
          1.3.14.3.2.29), NULL

```

| | | | | | |
|----|--|----------|----------|----------|----------|
| 74 | 0 | 6D3A6019 | 31860C95 | 46592B70 | 729DADAD |
| 75 | 10 | FD063FC9 | 0B66F172 | 584192D2 | 00DD078D |
| 76 | 20 | A178E672 | FFE70273 | F501ED0C | B7E1AD6E |
| 77 | 30 | 0AF31039 | 46107521 | 46E672AE | 431ABB00 |
| 78 | 40 | D7F3F6FC | D2E35D8F | F96C6FD7 | 37A95527 |
| 79 | 50 | ACB9A00D | E179A185 | D5802CC9 | 63B95F3A |
| 80 | 60 | 069800E5 | 772C7BC9 | BDBE6850 | 5A5B98F1 |
| 81 | 70 | CF959233 | 7D92B22B | FAEB9D87 | 62C79A02 |
| 82 | 80 | 047FE3F8 | 5D26254F | 80D26FC7 | CB5BC753 |
| 83 | 90 | 074D3EB7 | D5F01316 | 65816BFF | 2E433D69 |
| 84 | A0 | 08453A9F | 4C1C2529 | 1EE7E9F6 | D77FC779 |
| 85 | B0 | FF9C4066 | B7357444 | 4BD51033 | 65E7ADCB |
| 86 | C0 | 8AC3A71E | 011762A8 | 9E8EC8C8 | D88D2BA3 |
| 87 | D0 | 5109BDF9 | 1DAD377E | 10ADE706 | 26FD3DB9 |
| 88 | E0 | F78BB6EE | BF5968B7 | 6C8AB6A2 | 8E51910C |
| 89 | F0 | BD54B472 | D6FFA464 | 6CA595B9 | A8A1A71E |
| 90 | Certificate Fingerprint (MD5): | | | | |
| | 06:89:96:27:AF:CF:5B:F7:D3:1F:08:7A:71:40:9B:F9 | | | | |
| 91 | Certificate Fingerprint (SHA-1): 0B44 DF73 4F21 D914 402E 4128 1ED3 5548 | | | | |
| | F8F5 311A | | | | |

Public Key (Asymmetric)

Key owner: Korytov Pavel

Key type: EC-prime239v1

Date key created: 14.12.2019 15:54:28

Domain parameters of elliptic curve 'EC-prime239v1':

| Parameters | Value of the parameter | Bit len... |
|--|--|------------|
| Elliptic curve E described through the curve equation: $y^2 = x^3 + ax + b \pmod{p}$: | | |
| a | 883423532389192164791648750360308885314476597252960362792450860609699836 | |
| b | 738525217406992417348596088038781724164860971797098971891240423363193866 | 239 |
| p | 883423532389192164791648750360308885314476597252960362792450860609699839 | 239 |
| Point G on curve E (described through its (x,y) coordinates): | | |
| x | 110282003749548856476348533541186204577905061504881242240149511594420911 | 236 |
| y | 869078407435509378747351873793058868500210384946040694651368759217025454 | 239 |
| G has the prime order r and the cofactor k (r*k is the number of points on E): | | |
| k | 1 | 1 |
| r | 883423532389192164791648750360308884807550341691627752275345424702807307 | 239 |
| The public key 'W' = (x,y) is a point on curve E and a multiple of G: | | Bit len... |
| x = | 737607481742258675660668427801556273168707706976767565895304548702537505 | 239 |
| y = | 765328663424480120242698081314508961509180465979269813586639665050902058 | 239 |

Base for presentation of numbers:

☐ Octal
 ☒ Decimal
 ☐ Hexadecimal

Back

Рисунок 2. Публичные параметры ключа с EC-239

Листинг 2. сертификат с RSA-2048

```

1  Version:                2 (X.509v3--1996)
2  SubjectName:            CN=Korytov Pavel [1576327992], DC=cryptool, DC=org
3  IssuerName:             CN=CrypTool CA 2, DC=cryptool, DC=org
4  SerialNumber:          55:5C:A5:00:BB:2B:4B:AB
5  Validity — NotBefore:   Sat Dec 14 15:53:15 2019 (191214125315Z)
6                        NotAfter:   Mon Dec 14 15:53:15 2020 (201214125315Z)
7  Public Key Fingerprint: FC1F 91AB 932D BF9C D851 7554 1E8E 8C9A
8  SubjectKey:             Algorithm rsa (OID 2.5.8.1.1), Keysize = 2048
9                        Public modulus (no. of bits = 2048):
10                        0  F82FD7FA 4FFD8DEC E81010BC 507EC3DD
11                        10 A9F58F7F 5B26BA46 73353C8E 43F2A1B9
12                        20 C24FA82E 8E922703 A7860257 F38A7A2A
13                        30 135A5474 2950E81F 4B491A85 C498C1F8
14                        40 591F92F0 EF7DA58E AA0523CE 8F4B9C47
15                        50 324E4F29 BC19F55B B912111F 2E3468A4
16                        60 6BCEDAE5 5C766614 06FB0D00 60F63180

```

```

17      70  63713624 45BC40AB E770C61E 08C91054
18      80  6928EF91 64390054 39578551 95A5470C
19      90  8A47D117 8B324A61 63CF411C F18F27B8
20      A0  2647EFC0 67CC3D62 519D7369 8B46A023
21      B0  4F032012 7F8247CD C90C7977 CF69D221
22      C0  0044AC2E 33948080 06C2822B 25787031
23      D0  1E32896A 4F7144CB F759F87A 4F0A1F9D
24      E0  18668460 7B55FD38 6A2C0025 B2DBB2F7
25      F0  91B0C813 49927DFA 6B115F6B 5EA9B457
26      Public exponent (no. of bits = 17):
27      0  010001
28      Certificate extensions:
29      Private extensions:
30      OID 2.206.5.4.3.2:
31      PrintableString:
32      |[Pavel][Korytov][RSA—2048][15763|
33      |27992] |
34
35      SHA1 digest of DER code of ToBeSigned:
36      0  40914DDA 0D84A682 05AD52DC A9B522B0
37      10 C727FCA6
38      Signature: Algorithm sha1WithRSASignature (OID
      1.3.14.3.2.29), NULL
39      0  AC481096 0A5EDDD2 A67ED4C9 AACB87C4
40      10 C7F2D9E6 3F32B4C3 6518EFDE AD52A276
41      20 546B44EE 1A5B88E2 6A121082 8E2B3CB5
42      30 BAB580EA 30C8D488 DADB0C15 FFAE3944
43      40 A16880F9 F6B76244 74E7F7BE F00910A0
44      50 ABAAFA31 117EDA06 736DF454 5198197D
45      60 2CFD5155 80B8F09D 4C58684F 12B569E3
46      70 F9E33835 DC9140F5 532B0D2A 1A20A62D
47      80 5DAB6DC0 B829EC8C 13FEB53C C231582A
48      90 0755E85E DD9EEF5A 6EC71B2F 915CE447
49      A0 25ED3D4F 0474B9D2 7FBB05F0 C6B26F13
50      B0 A40D92FF 1BD99B2C F5F4DAE0 A3EDA794
51      C0 A326A275 3DF857D2 E1881C45 FEF6F5FF
52      D0 304E904C CD79B084 313E9C73 6A3D9DBE
53      E0 041029B9 09B18428 E4D27486 A08EDB59
54      F0 9ECE7AA1 129A664E 95D9AA18 80991923
55      Certificate Fingerprint (MD5):
      53:48:F1:81:AA:3F:70:E6:4F:AA:D8:F9:41:2F:8F:24

```


2. Процессы создания и проверки цифровой подписи

2.1. Основные теоретические положения

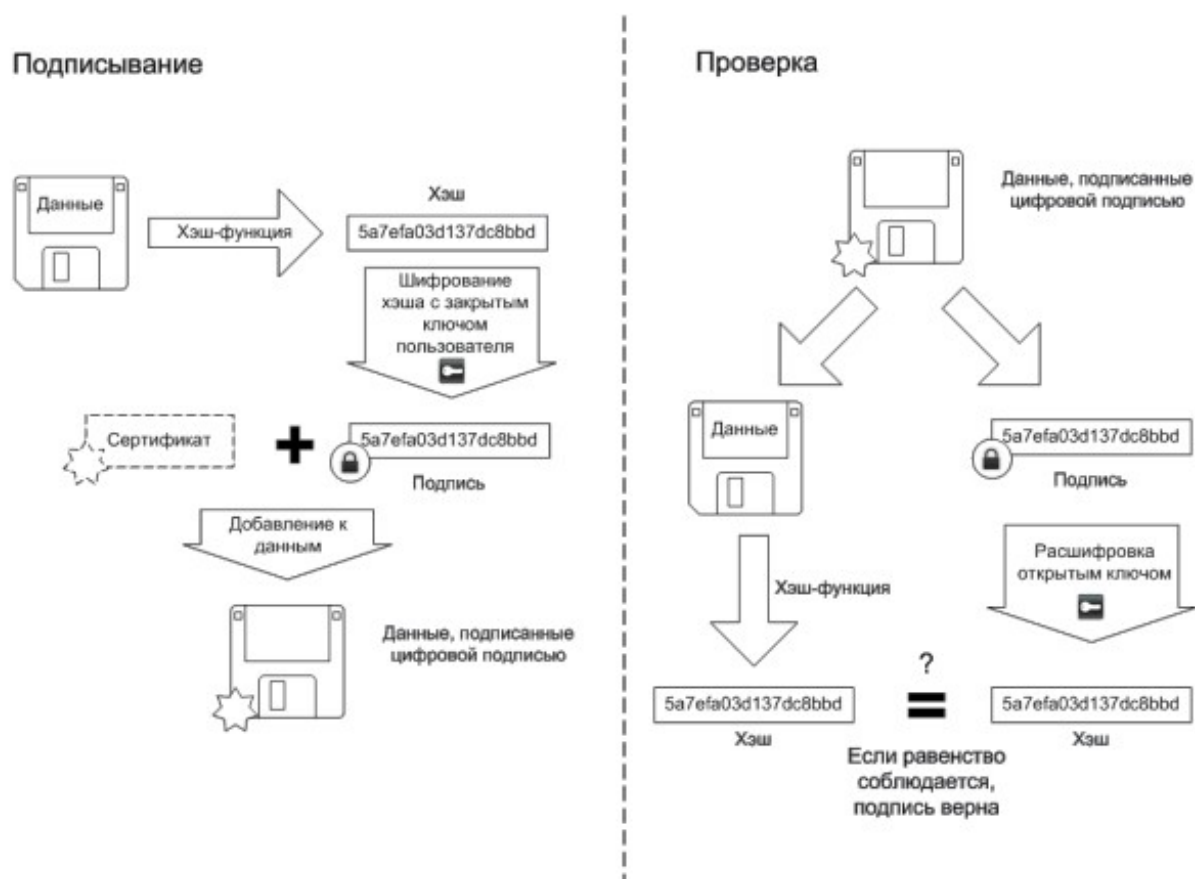


Рисунок 3. Обобщенная схема подписывания и проверки цифровой подписи

2.2. Формулировка задания

1. Открыть текст не менее 5000 знаков. Перейти к приложению Digital Signatures/ > Sign Document...
2. Задайте хэш-функцию, и другие параметры цифровой подписи.
3. Создайте подпись ключами, сгенерированными в предыдущем задании. Зафиксируйте время создания цифровой подписи для каждого ключа.
4. Сохраните скриншот цифровой подписи с помощью приложения Digital Signatures/PKI-> Extract Signature.
5. Выполните процедуру проверки подписи Digital Signatures/PKI-> Verify Signature для случаев сохранения и нарушения целостности исходного текста. Сохраните скриншоты результатов.

2.3. Ход работы

1. Создан текст, удовлетворяющий требованиям.

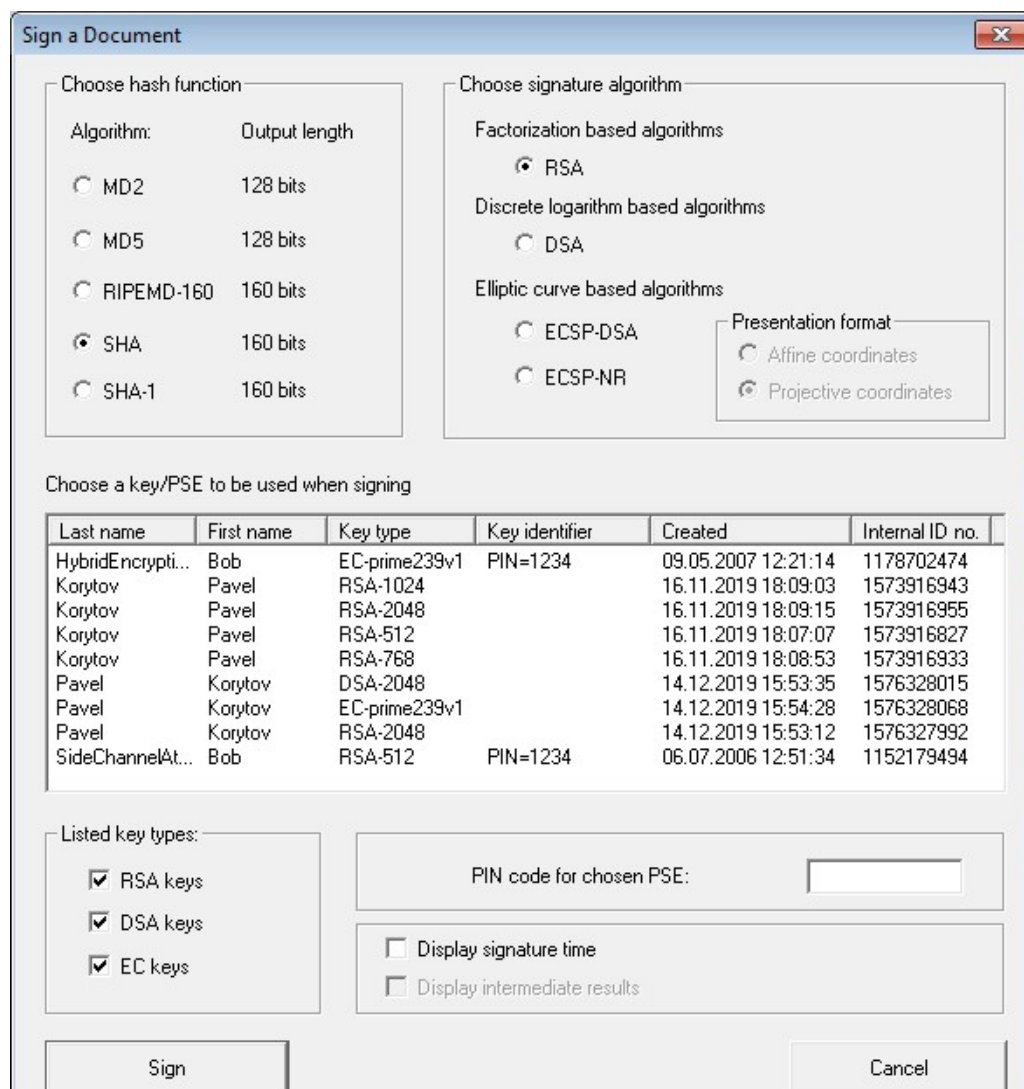


Рисунок 4. Утилита подписания документа

2. Измерено время подписания всеми созданными ключами.

| Алгоритм | Время подписания (с.) |
|----------|-----------------------|
| RSA-2048 | 0.016 |
| DSA | 0.000 |
| EC-239 | 0.031 |

3. Извлечены сигнатуры подписей:

Листинг 3. сигнатура RSA-2048

```

1  000000  20 2D D7 64 8D 4A 31 C8 7F 06 F5 4C 58 4A  —xd.J1È..õLXJ
2  0000E0  7F D0 7F 3B C6 48 17 08 28 66 7A 91 E8 BF  .Đ.;ÆH..(fz.è¿
3  0001C0  BF 90 64 C4 00 E1 CE 17 D3 23 C7 47 92 6C  ¿.dÄ.áÎ.Ó#ÇG.l

```

| | | | |
|----|-------|---|------------------|
| 4 | 0002A | 09 D4 44 26 E6 E7 94 7A F7 AB 7E 0F 7C 44 | .ÔD&æç.z÷«~. D |
| 5 | 00038 | 69 D1 7F EB 3D 8B 5C F7 51 EF 4A D3 70 1F | iÑ.ë=.÷QİJÓp. |
| 6 | 00046 | 26 23 B4 54 EE 03 34 09 BF 9C 23 7A 57 9F | &#‘Tî.4.¿. #zW. |
| 7 | 00054 | AE 23 81 47 3F B1 08 81 41 B9 0E 40 FA 4E | ©#.G?±..A¹. @úN |
| 8 | 00062 | CD 07 0C BD C7 52 17 C7 8D 73 90 21 CE 48 | Í..½ÇR.Ç.s. !ÎH |
| 9 | 00070 | 20 94 95 56 DB 57 C7 C6 AD 55 8A F6 9D 01 | ..VÛWÇÆU.ö.. |
| 10 | 0007E | 1F 9E F0 19 31 59 AF FB BF 0B BF 61 26 13 | ..ð.1Y˘û¿.¿a&. |
| 11 | 0008C | 06 0F 70 E4 A3 9F 55 AD 69 8E 59 22 D3 F9 | ..päf. U i .Y"Óù |
| 12 | 0009A | D6 58 E4 F3 60 A6 37 B0 18 96 71 17 37 35 | ÖXäó` 7°..q.75 |
| 13 | 000A8 | 10 17 EB 64 01 6F 34 A6 96 F2 D4 EE 93 9E | ..ëd.o4 .òÔî.. |
| 14 | 000B6 | 29 D6 81 53 E1 8C 4B 9F 23 61 7D 68 E2 DB |)Ö.Sá.K.#a}hâÛ |
| 15 | 000C4 | 0D 54 F6 7E B8 07 B1 CB A7 87 3C A4 75 C8 | .Tö~. .±Ë§.<ruÈ |
| 16 | 000D2 | 61 F4 41 2D E4 C4 09 CA 04 4D C4 DA 85 23 | aôA–äÄ.Ê.MÄÚ.# |
| 17 | 000E0 | 59 4D 53 50 4F F1 8C 53 5C 69 7C 57 52 C6 | YMSP0ñ.S\i WRÆ |
| 18 | 000EE | 84 01 4B 36 18 EC 75 10 3E 35 93 BC FD 2F | ..K6.ìu.>5.¼ý/ |
| 19 | 000FC | 6C 33 5B 45 | l3[E |

Листинг 4. сигнатура DSA-2048

| | | | |
|---|-------|---|-----------------|
| 1 | 00000 | 30 2C 02 14 61 1C 00 13 2E 1E 6C 01 A6 C8 | 0,...a.....l.¡È |
| 2 | 0000E | 54 B5 91 42 FE 81 D9 1B 36 F1 02 14 77 26 | Тμ.Вр.Ù.6ñ..w& |
| 3 | 0001C | AC 4A D2 60 FD D6 6E 51 56 E2 76 4E 38 18 | ~JÒ`ýÖnQVâvN8. |
| 4 | 0002A | 2D F2 4C AC | —òL— |

Листинг 5. сигнатура EC-239

| | | | |
|---|-------|---|------------------|
| 1 | c: | | |
| 2 | 00000 | 17 4C E8 3A 07 AF 98 16 8B 46 21 02 97 B2 | .Lè:..˘...F!...² |
| 3 | 0000E | 7B 63 3B 99 F8 CC 48 C2 5C 36 C6 A0 E4 62 | {c;.øİHÂ\6Æ äb |
| 4 | 0001C | 00 CC | .İ |
| 5 | | | |
| 6 | d: | | |
| 7 | 00000 | 54 66 E8 D7 68 F3 F5 24 61 94 C4 B2 E8 A1 | Tfè×hóô\$a.Ä²è; |
| 8 | 0000E | 7F 48 AB AA 11 9B 00 FC 9D FB B0 32 4A E7 | .H«²...ü.û°2Jç |
| 9 | 0001C | 5B A1 | [i |

4. Выполнена проверка подписей.



(a) Успешная валидация



(b) Ошибка валидации

Рисунок 5. Валидация подписей

| Алгоритм | Время успешной проверки (с.) | Время неудачной проверки (с.) |
|----------|------------------------------|-------------------------------|
| RSA-2048 | 0.000 | 0.000 |
| DSA | 0.014 | 0.000 |
| EC-239 | 0.000 | 0.000 |

3. Схемы цифровой подписи на эллиптических кривых

3.1. Основные теоретические положения

d — закрытый ключ, (a, b, q, p, e_1, e_2) — открытый ключ.

Алгоритм подписания:

1. Выбирается секретное случайное число $r : r \in (1, q - 1)$
2. Выбирается третья точка на кривой: $P(u, v) = r \times e_1$
3. Вычисляется первая часть подписи по формуле:

$$S_1 = u \bmod q,$$

где q — абсцисса.

4. Вычисляется вторая часть подписи по формуле:

$$S_2 = (h(M) + d \times S_1) \times r^{-1} \bmod q,$$

где $h(M)$ — дайджест сообщения, d — закрытый ключ

Алгоритм проверки:

1. Вычисляются промежуточные результаты:

$$A = h(M) \times S_2^{-1} \bmod q$$

$$B = S_2^{-1} \times S_1 \bmod q$$

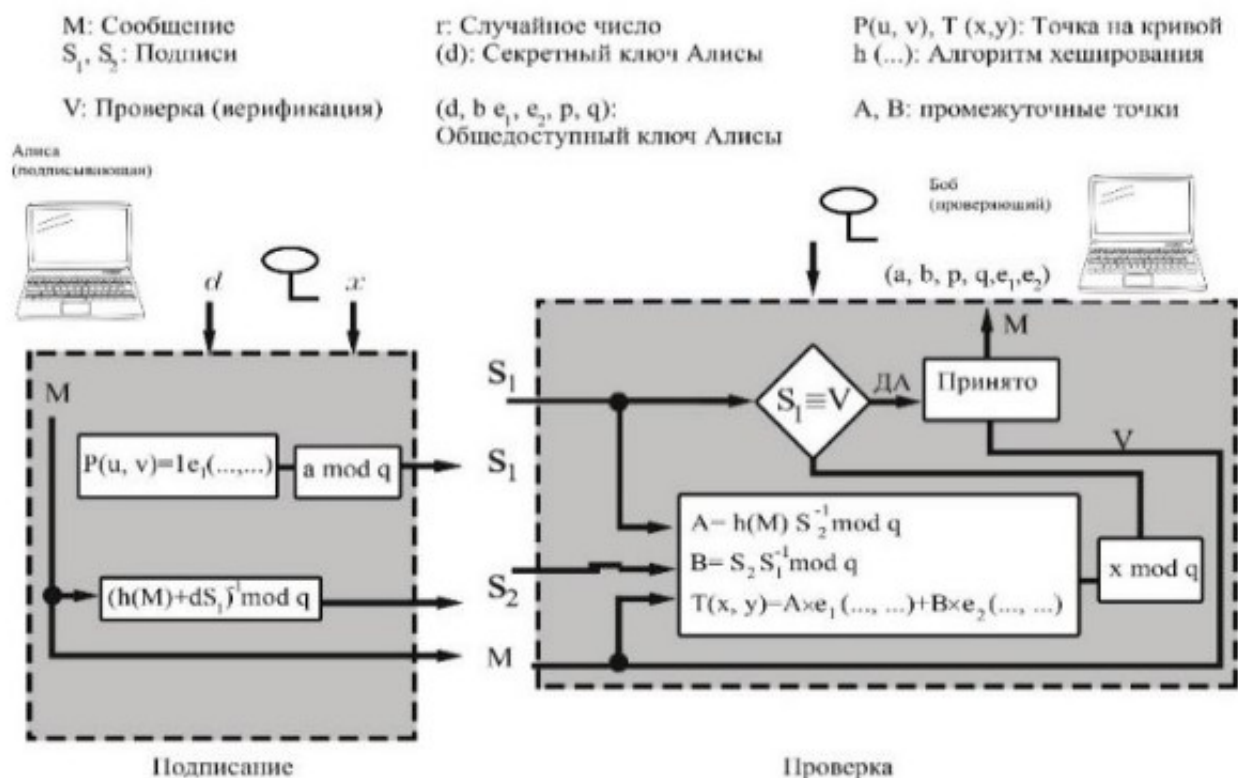


Рисунок 6. Схема цифровой подписи ECDSA

2. Восстанавливаем третью точку:

$$T(x, y) = A \times e_1 + B \times e_2$$

3. Верификатор $V = x \bmod q$ сравнивается с S_1

3.2. Формулировка задания

1. Выполните процедуру создание подписи «Digital Signatures/PKI-> Sign Document...» алгоритмом ECSP-DSA в пошаговом режиме (Display inter.results). Зафиксируйте скриншоты последовательности шагов.
2. Выполните процедуру проверки подписи ECSP-DSA для случаев сохранения и нарушения целостности исходного текста. Сохраните скриншоты результатов.
3. Проверить лекционный материал по ECDSA, выполнив создание и проверку подписи сообщения M (принять $M = h(M)$) приложением Indiv.Procedure->Number Theory->Point Addition on EC.

3.3. Ход работы

1. Выполнено создание подписи алгоритмом ECSP-DSA.

```

1 Signature originator: Korytov Pavel
2
3 Domain parameters to be used 'EC-prime239v1':
4
5   a =
      883423532389192164791648750360308885314476597252960362792450860609699836
6   b =
      738525217406992417348596088038781724164860971797098971891240423363193866
7   Gx =
      110282003749548856476348533541186204577905061504881242240149511594420911
8   Gy =
      869078407435509378747351873793058868500210384946040694651368759217025454
9   k = 1
10  r =
      883423532389192164791648750360308884807550341691627752275345424702807307
11
12 Secret key s of the signature originator:
13
14   s =
      754683591577674149644405092121277381337060051863400825003553528855773730
15
16 Chosen signature algorithm: ECSP-DSA with hash function SHA-1
17
18 Size of message M to be signed: 5808 bytes
19
20 Continue ...
21
22 Calculate a 'hash value' f (message representative) from message M, using
    the chosen hash function SHA-1.
23
24   f = 1024522355235258970340836052886279629474824494520
25
26 Continue ...
27
28 Create a random one-time key pair (secret key, public key) = (u,V)
29 with the domain parameters of 'EC-prime239v1' (V=(Vx,Vy) is a point on the
    elliptic curve):
30
31   u =
      178419650035660251992372905265022780058011316959682011257555633719175666

```

```

32   Vx  =
      803690003354748327524759484566994085287007112563762869183794766105775915
33   Vy  =
      589757706342295080645801881200117652994487281995321096455218380961437553
34
35   Continue ...
36
37   Convert the group element Vx (x co-ordinates of point V on elliptic curve)
      to the number i:
38
39   i  =
      803690003354748327524759484566994085287007112563762869183794766105775915
40
41   Continue ...
42
43   Calculate the number c = i mod r (c not equal to 0):
44
45   c  =
      803690003354748327524759484566994085287007112563762869183794766105775915
46
47   Continue ...
48
49   Calculate the number d = u(-1)*(f + s*c) mod r (d not equal to 0):
50
51   d  =
      612042122264557627635592100620793119781476463255607182476715616964867191
52
53   Continue ...
54
55   Signature generation finished.
56   The signature consists of the two numbers c and d.

```

2. Выполнена проверка подписей.



(a) Успешная валидация



(b) Ошибка валидации

Рисунок 7. Валидация подписей

3. Проведена проверка лекционного материала.

Генерация ключей ECDSA

- Выбирается эллиптическая кривая $E_p(a, b)$, p – простое
- Для дальнейших вычислений выбирается другое простое число q – порядок одной из циклических подгрупп группы точек эллиптической кривой : $q \times (x_0, y_0) = O$
- Выбирается целое число d , $1 < d < q - 1$ и назначается закрытым ключом
- Выбирается точка на кривой $e_1 = (x_1, y_1)$
- Вычисляется другая точка на кривой $e_2 = d \times e_1$
- Объявляется открытый ключ (a, b, p, q, e_1, e_2)

Рисунок 8. Слайд с описанием генерации ключей ECDSA

- Выбирается секретное случайное число, r , $1 < r < q - 1$
- Выбирается третья точка на кривой, $P(u, v) = r \times e_1$
- Используем абсциссу u , чтобы вычислить первую часть подписи
$$S_1 = u \bmod q$$
- Используем дайджест сообщения $h(M)$, закрытый ключ d , секретное случайное число r и S_1 , чтобы вычислить вторую часть подписи
$$S_2 = (h(M) + d \times S_1) \times r^{-1} \bmod q$$

(a) ECDSA подписание

- Используем M, S_1, S_2 для получения промежуточных результатов A и B :
$$A = h(M) \times S_2^{-1} \bmod q$$
$$B = S_2^{-1} \times S_1 \bmod q$$
- Затем восстанавливаем третью точку
$$T(x, y) = A \times e_1 + B \times e_2$$
- Верификатор $V =$
 $x \bmod q$ сравниваем с S_1

(b) ECDSA проверка

Рисунок 9. Подписание и проверка

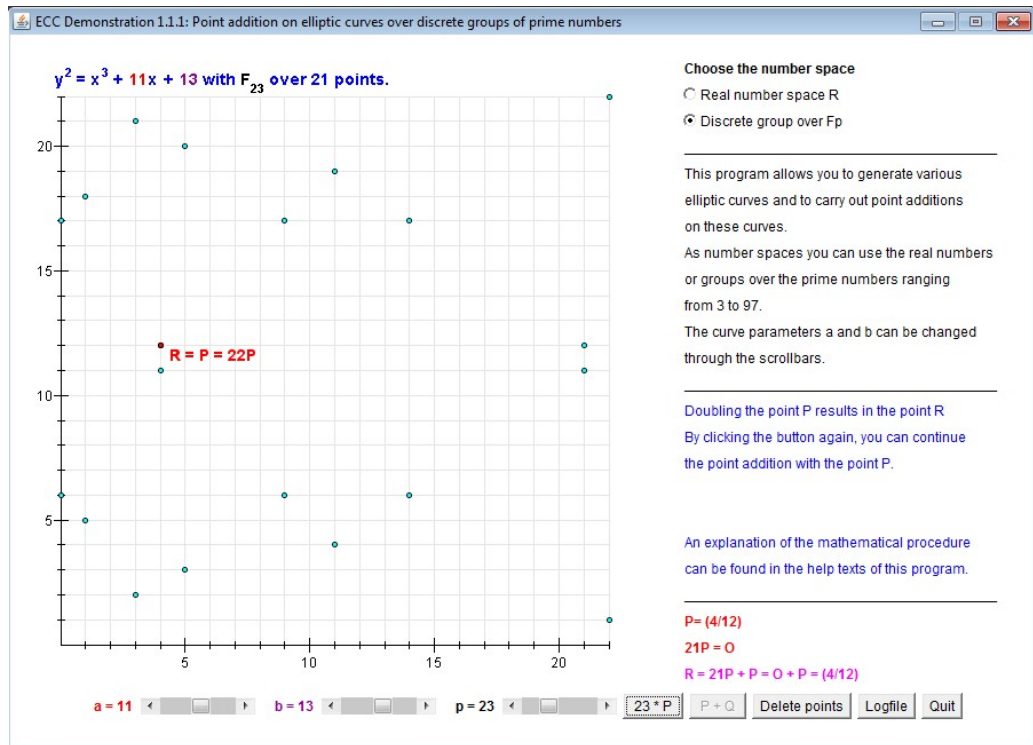


Рисунок 10. Утилита для вычислений на эллиптических кривых

Генерация ключей:

- Выбрана эллиптическая кривая $y^2 = x^3 + 11x + 13$ над F_{23} .
 $a = 11, b = 13, p = 23$
- $P := (4, 12)$
- Путем перебора: $21 \times (4, 12) = O \Rightarrow q = 21$
- $d := 10$ — закрытый ключ
- $e_1 := (14, 17)$
- $e_2 = d \times e_1 = 10 \times (14, 17) = (5, 3)$
- Открытый ключ — $(11, 13, 23, 21, (14, 17), (5, 3))$

Подписание:

- $r := 13$
- $(u, v) = 13 \times (14, 17) = (14, 6)$
- $S_1 = u \bmod q = 14 \bmod 21 = 14$
- $M := 99, h(M) := M$.

$$\begin{aligned} S_2 &= (h(M) + d \times S_1) \times r^{-1} \bmod q \\ &= (99 + 10 \times 14) \times 13^{-1} \bmod 21 = 20 \end{aligned}$$

Проверка:

- $A = h(M) \times S_2^{-1} \bmod q = 99 \times 20^{-1} \bmod 21 = 6$

- $B = S_2^{-1} \times S_1 \bmod 21 = 7$
- $(x, y) = A \times e_1 + B \times e_2 = (14, 6) + O = (14, 6)$
- $x = S_1$ — проверка пройдена.

4. Демонстрация процесса подписи в среде PKI

4.1. Формулировка задания

1. Запустить демонстрационную утилиту «Digital Signatures/PKI-> Signature Demonstration...».
2. Получите сертификат на ранее сгенерированную ключевую пару RSA-2048.
3. Выполните и сохраните скриншоты всех этапов создания цифровой подписи документа.
4. Сохраните скриншот сертификата для проверки этой цифровой подписи

4.2. Ход работы

1. Запущена указанная утилита.

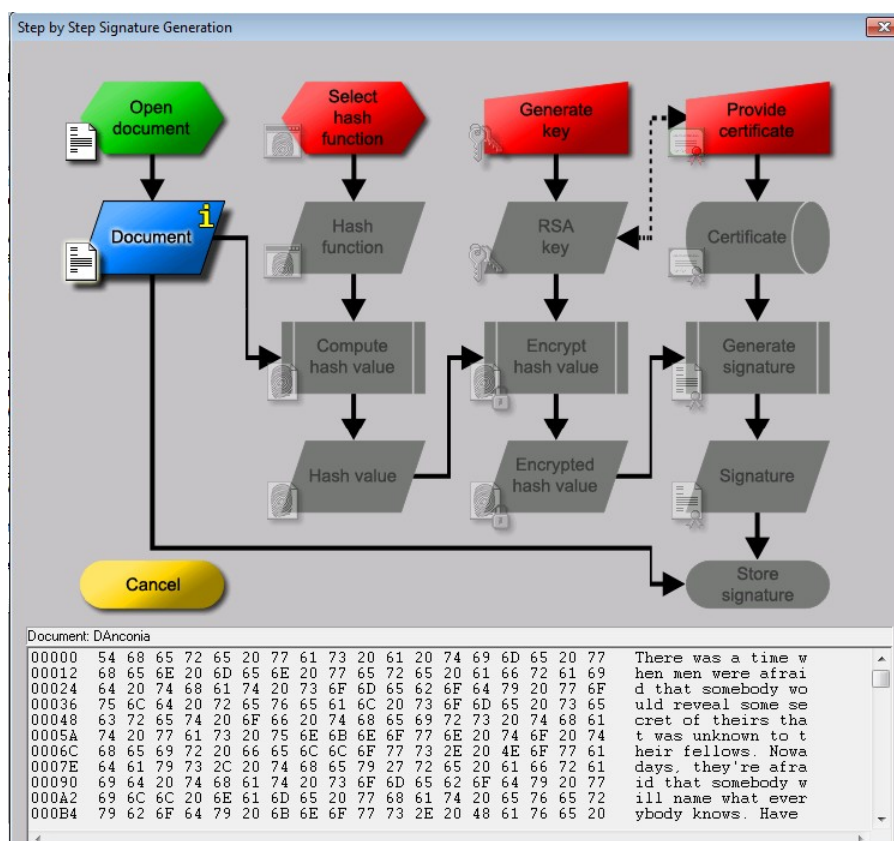


Рисунок 11. Вид Signature Demonstration

(а) Выбрана хэш-функция SHA-1

Листинг 7. хэш-функция

| | | |
|---|-----------------|--|
| 1 | Name: | SHA-1 |
| 2 | Length in bits: | 160 |
| 3 | Algorithm ID: | 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 |

(b) Вычислен SHA-1 хэш текста

Листинг 8. хэш текста

| | |
|---|---|
| 1 | B3 75 2B DA 2C EC 38 6A AE BD 4A A2 B7 78 B1 3D 8C 3C 9D B8 |
|---|---|

(c) Сгенерирован RSA-ключ

Листинг 9. ключ

| | | |
|---|--------------------------|---|
| 1 | Bit length of N: | 304 |
| 2 | RSA modulus N: | 5 153 404 714 761 008 744 896 344 126 074 269 264 270 224 690 453 913 630 460 946 340 383 627 809 721 221 384 320 487 569 |
| 3 | $\phi(N) = (p-1)(q-1)$: | 5 153 404 714 761 008 744 896 344 126 074 269 264 270 224 685 849 812 918 367 971 768 861 525 030 822 887 495 081 938 944 |
| 4 | Public key: | 65537 |
| 5 | Private key: | 2 239 403 892 025 554 542 409 676 737 819 386 215 071 665 300 949 338 878 834 879 045 507 230 592 685 124 631 466 782 721 |

(d) Хэш зашифрован созданным ключом

Листинг 10. шифрование текста

| | | |
|---|-----------------------|--|
| 1 | Padding string: | 01 00 |
| 2 | Algorithm ID: | 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 |
| 3 | Hash value: | B3 75 2B DA 2C EC 38 6A AE BD 4A A2 B7 78 B1 3D 8C 3C 9D B8 |
| 4 | | |
| 5 | ASN-1 hash value: | 01 00 30 21 30 09 06 05 2B 0E 03 02 1A 05 00 04 14 B3 75 2B DA 2C EC 38 6A AE BD 4A A2 B7 78 B1 3D 8C 3C 9D B8 |
| 6 | Length in bits: | 296 |
| 7 | | |
| 8 | Encrypted hash value: | 20 BA E4 EF B1 1F 42 67 38 1B B6 49 D1 09 73 4D F1 AF F3 54 FB C4 34 52 BC 92 A0 AB 1E 82 6C 62 8F A6 AA F6 5A 8B |
| 9 | Length in bits: | 304 |

(e) Создан сертификат для созданной ключевой пары

Листинг 11. созданный сертификат

```

1  Version:                2 (X.509v3–1996)
2  SubjectName:            CN=Korytov Pavel [1576340635], DC=cryptool,
                           DC=org
3  IssuerName:             CN=CrypTool CA 2, DC=cryptool, DC=org
4  SerialNumber:          C1:C5:9D:B5:B0:ED:58:C8
5  Validity — NotBefore:   Sat Dec 14 19:23:59 2019 (191214162359Z)
6                        NotAfter:   Mon Dec 14 19:23:59 2020 (201214162359Z)
7  Public Key Fingerprint: E597 C0CC BD38 A551 F1C0 57A8 29AA 5A47
8  SubjectKey:             Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
9                        Public modulus (no. of bits = 302):
10                        0  287A48C1 4EAE7ABC 9CE3B671 A8F17A9E
11                        10  73C560FC 9EA3A31A 983A4AD2 9998E4E4
12                        20  9243DCBA 9091
13                        Public exponent (no. of bits = 17):
14                        0  010001
15  Certificate extensions:
16  Private extensions:
17      OID 2.206.5.4.3.2:
18      PrintableString:
19          |C:\Users\Pavel\AppData\Roaming\C|
20          |rypTool\PSE/[Pavel][Korytov][RSA|
21          |–304][1576340635].pse          |
22
23  Signature:              Algorithm sha1WithRSASignature (OID
                           1.3.14.3.2.29), NULL
24      0  E591AF77 622429A2 200280D3 1DE5CFA7
25      10  83518937 5A04C2CC 64504B41 8238CD93
26      20  EAC5F7EC C46C209F 4E914E65 551A36B3
27      30  13D75A95 26CEFDFA 54DA1FA5 0DFC67F6
28      40  B959221B F590D9C8 9AF239F8 62C6817F
29      50  DEDDD8A0 E0098935 C736E4D5 22F311FE
30      60  D734C889 9E806E34 B23CA73F 2AD49051
31      70  0475FD0A EB9B5CCF 60AF6137 718FA882
32      80  B06092DB B3AA47E1 9B9D5029 60F94D74
33      90  1208FA1B E6CA9C44 2C975F01 F3B1C4EF
34      A0  B81D7DBD 7FE10DF6 BCB88B76 860BFF25
35      B0  35D26EBD 3FA5DFA2 A17532A1 CDBF2329
36      C0  CB427768 46827020 B42D7284 FACA2C87
37      D0  91A9C216 C4622B4E BA3D6098 7B1B1F7C
38      E0  6F8DCAB6 CC3ECF1C 09C67759 EEE17BE5
39      F0  DE7C4378 F974F29B 27DEA9B2 D266591C

```

40 Certificate Fingerprint (MD5):
 FB:DC:4E:2C:F4:89:02:AC:8B:A8:69:64:05:FD:69:6A

41 Certificate Fingerprint (SHA-1): E69C ABA9 29BB 941D E728 4D38 E271
 3CE6 8E38 FB8C

(f) Создана подпись

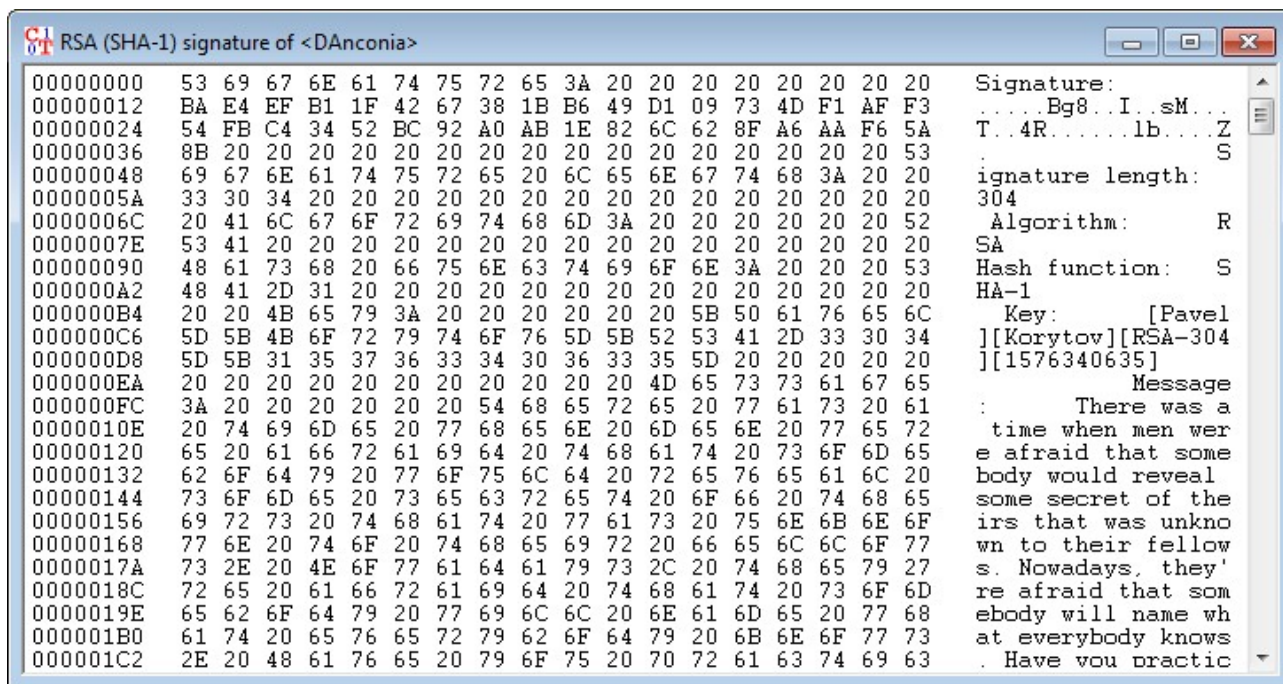


Рисунок 12. Подписанное сообщение

5. Подписание своего отчёта

5.1. Формулировка задания

1. Сконвертируйте отчёт в формат pdf
2. Экпортируйте ранее созданный сертификат ключевой пары RSA Digital Signatures/PKI->PKI/Generate...->Export PSE (#PKCS12).
3. Откройте pdf-версию отчета и попытайтесь подписать с использованием этого сертификата.
4. Создайте собственный самоподписанный сертификат в среде Adobe Reader и используйте его для подписи отчета.
5. Сохраните скриншоты свойств подписи и сертификата
6. Внесите изменения (маркеры, комментарии) в отчёт и проверьте подпись.

5.2. Ход работы

1. Текущая версия отчёта скомпилирована в pdf.
2. Созданный сертификат экспортирован в формат p12.

3. Т.к. на Linux нет Adobe Acrobat, установлена программа Portable Signer. Произведено подписание документа.

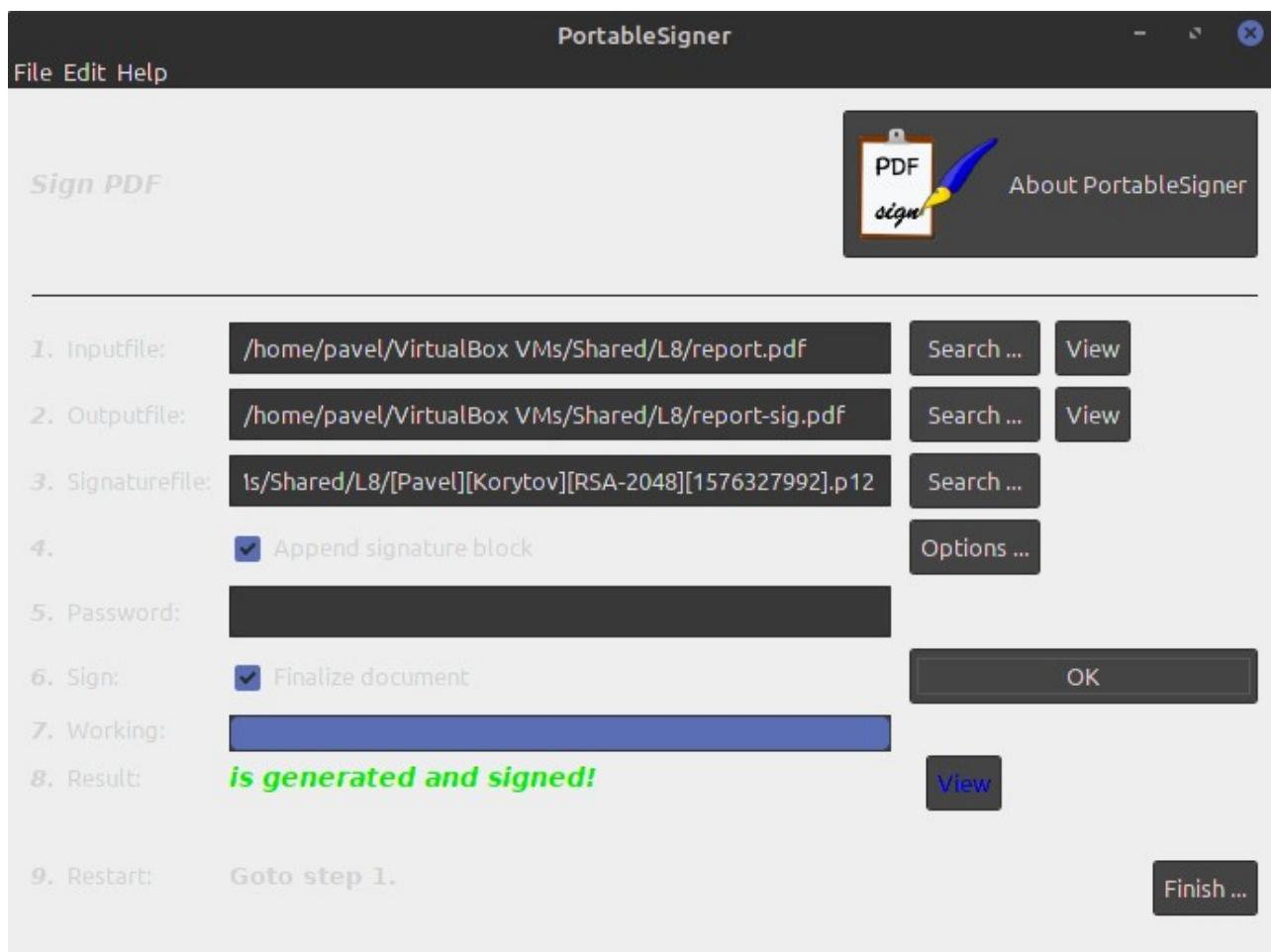


Рисунок 13. Интерфейс программы

4. С помощью утилиты pdfsig проведена проверка подписи



Рисунок 14. Знак подписи

```

/bin/bash
~/VirtualBox VMs/Shared/L8
> pdfsig report-sig.pdf
Digital Signature Info of: report-sig.pdf
Signature #1:
- Signer Certificate Common Name: Korytov Pavel [1576327992]
- Signer full Distinguished Name: CN=Korytov Pavel [1576327992],DC=cryptool,DC=org
- Signing Time: Dec 14 2019 20:53:02
- Signing Hash Algorithm: SHA1
- Signature Type: adbe.pkcs7.sha1
- Signed Ranges: [0 - 1169715], [1174151 - 1179633]
- Total document signed
- Signature Validation: Signature is Valid.
- Certificate Validation: Certificate issuer isn't Trusted.
~/VirtualBox VMs/Shared/L8
> pdfsig report.pdf
File 'report.pdf' does not contain any signatures
~/VirtualBox VMs/Shared/L8
2 >

```

Рисунок 15. Проверка подписи

Сертификат верен.

5. Проведена модификация pdf-файла.



Рисунок 16. Модифицированный файл

6. Проведена проверка дайджеста

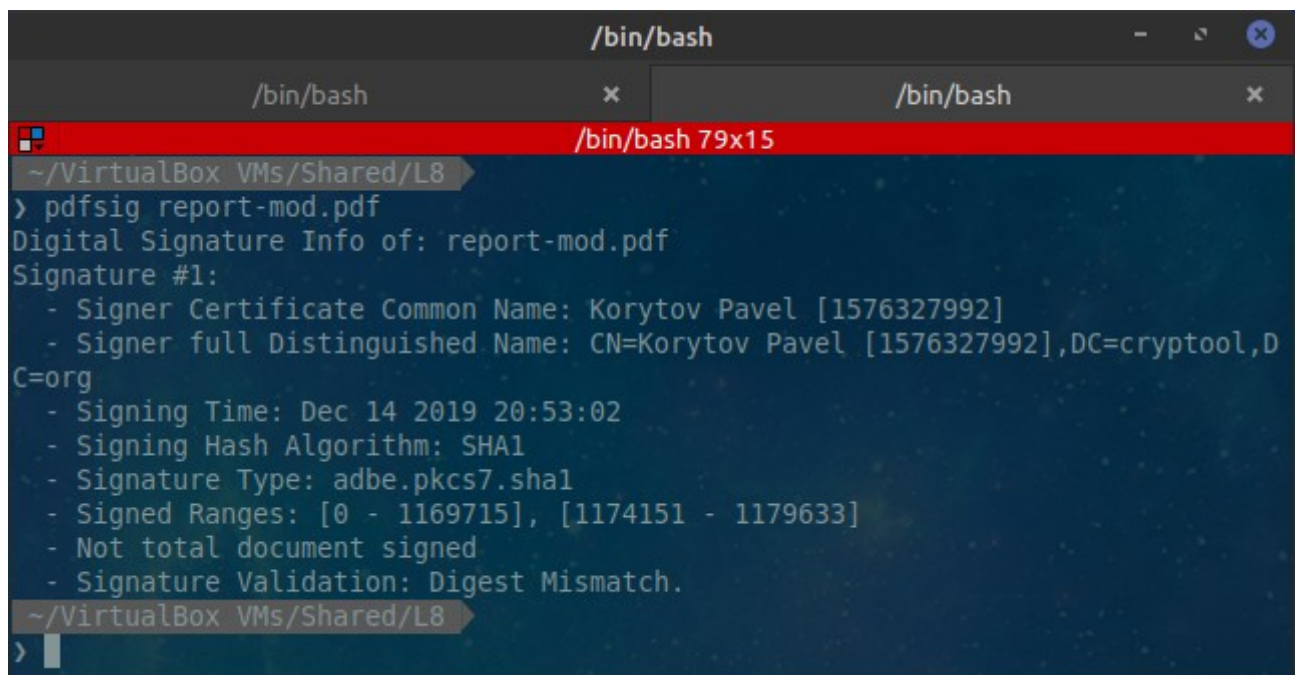


Рисунок 17. Проверка подписи модифицированного файла

Изменение обнаружено.

6. Выводы

Исследованы алгоритмы создания и проверки цифровой подписи, алгоритмы генерации ключевых пар RSA, DSA, ECDSA. Изучена работа с ними в CrypTool 1.

Алгоритм RSA основывается на задаче факторизации, DSA — на задаче дискретного логарифмирования. ECDSA — модификация DSA, работающая не в кольце целых чисел, но в группе точек эллиптической кривой.


Цифровая подпись — результат криптографической-хэш функции от документа. Цифровая подпись создается секретно (с помощью закрытого ключа), но может быть публично проверена (с помощью открытого ключа).

Сертификат открытого ключа содержит:

- Открытый ключ владельца сертификата
- Срок действия
- Имя выдающего
- Имя владельца сертификата
- Цифровой подписи

Сертификат выдается центром сертификации, открытый ключ центра общеизвестен. Любой, имеющий сертификат, может проверить подлинность сертификата, как следствие — подлинность открытого ключа владельца. Таким образом, можно проверить подлинность подписи документа.

This document is signed by

| | | |
|---|---------------------------|---|
|  | Signatory | CN=Korytov Pavel [1576327992], DC=cryptool, DC=org |
| | Date/Time | Sat Dec 14 21:16:36 MSK 2019 |
| | Issuer-Certificate | CN=CrypTool CA 2, DC=cryptool, DC=org |
| | Serial-No. | 6150972613640014763 |
| | Method | urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature) |
| Note | Pavel Korytov | |