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

ОТЧЕТ

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

Студент гр. 9303 _____ Ефимов М.Ю.

Преподаватель _____ Племянников А.К.

Санкт-Петербург
2022

Цель работы.

Исследовать алгоритмы создания и проверки цифровой подписи, алгоритмы генерации ключевых пар для алгоритмов цифрой подписи RSA, DSA, ECDSA и получить практические навыки работы с ними, в том числе с использованием приложения Cryptool 1 и 2.

Генераторы ключевых пар.

Описание алгоритмов генерации.

Генерация ключевых пар для алгоритма RSA:

Генерация двух больших простых чисел p и q (p и q держаться в секрете).

1. Вычисление n = p * q

2. Вычисление n = p · q.

3. Выбирается произвольное e (e < n), взаимно простое с (p-1)·(q-1) = φ(n)

4. Вычисление d: e · d = 1 mod φ(n).

5. Числа (e, n) – открытый ключ, d – закрытый ключ, p и q уничтожаются.

DSA генерация ключей:

1. Выбирается простое число p, длиной между 512 и 1024 битами. Число битов в p должно быть кратно 64

2. Выбирается другое простое число q, которое имеет тот же самый размер дайджеста 160 бит, такое, что: (p - 1) = 0 mod φ(n).

3. Выбирается e1: e1^q = 1 mod p путём вычисления e1 = e0^(p-1/q1) e0 ϵ Zp (теорема Ферма).

4. Выбирается целое d < q и вычисляется e = e d2

5. Объявляется открытый ключ (e1, e2, p, q).

6. Назначается закрытый ключ d.

Генерация ключевых пар для алгоритма ECDSA

1. Выбирается эллиптическая кривая $Ep(a, b)$, p − простое число.

2. Выбирается точка на кривой $e1 = (x1, y1)$

3. Выбирается простое число q – порядок одной из циклических подгрупп группы точек эллиптической кривой: $q \times (x1, y1) = O$.

4. Выбирается закрытый ключ d.

5. Вычисляется точка на кривой $e2 = d \times e1$.

6. Открытый ключ - $(a, b, q, p, e1, e2)$.

Таблица с фактическим временем генерации ключевых пар.

Алгоритм	Время генерации, с
RSA-2048	1.659
DSA-2048	1.293
EC-239	0.033

Скриншоты со значениями открытых ключей.

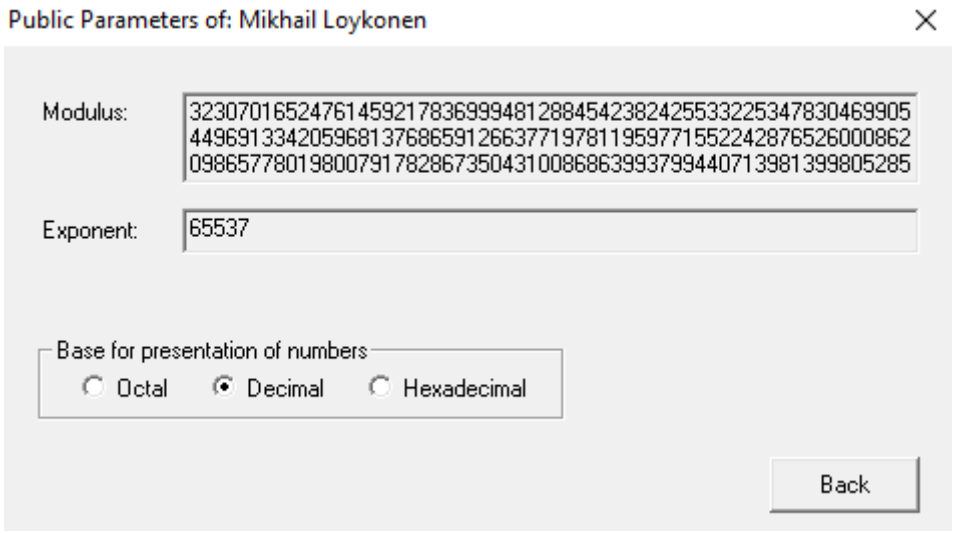


Рисунок 1 - Открытый ключ RSA-2048

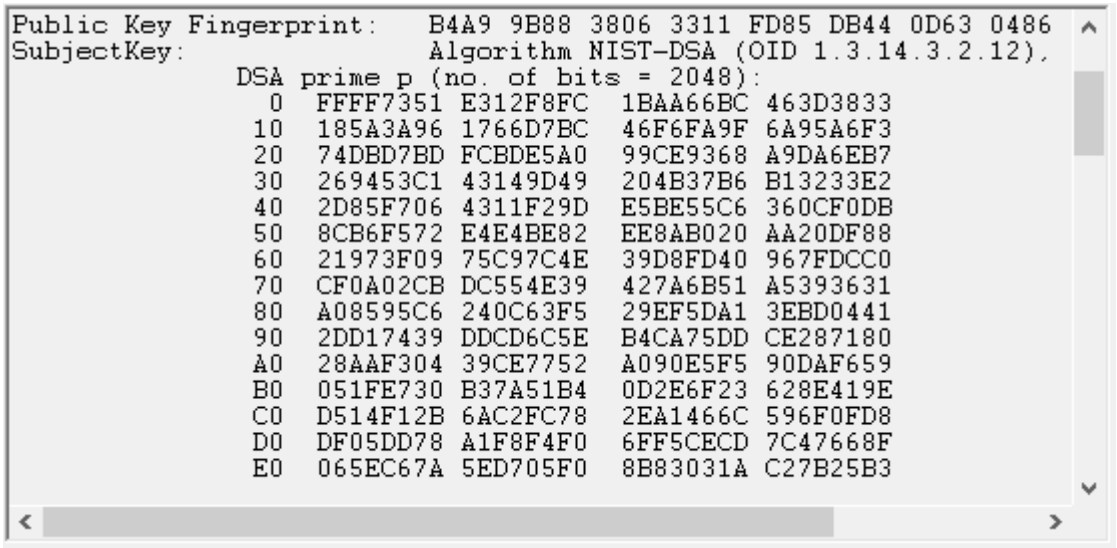


Рисунок 2 - Открытый ключ DSA-2048 (1)

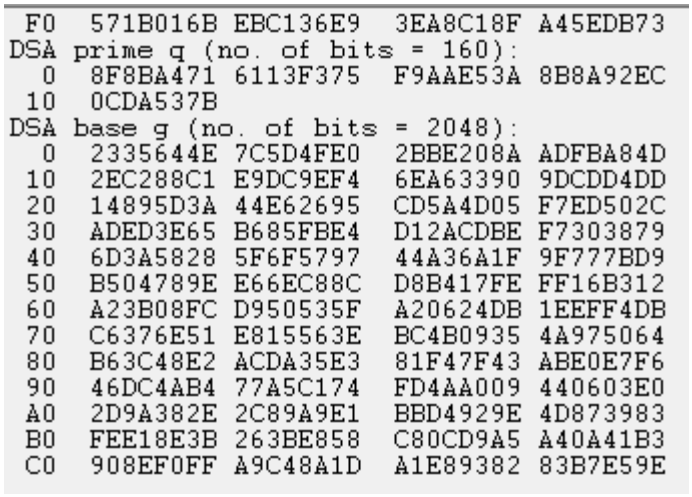


Рисунок 3 - Открытый ключ DSA-2048 (2)

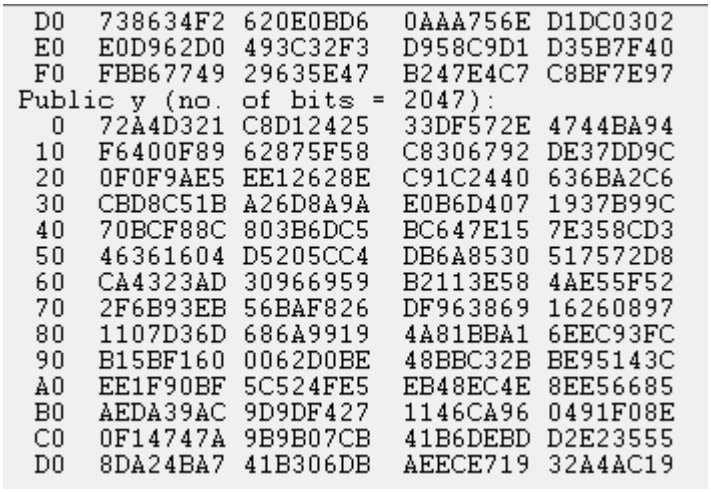


Рисунок 4 - Открытый ключ DSA-2048 (3)

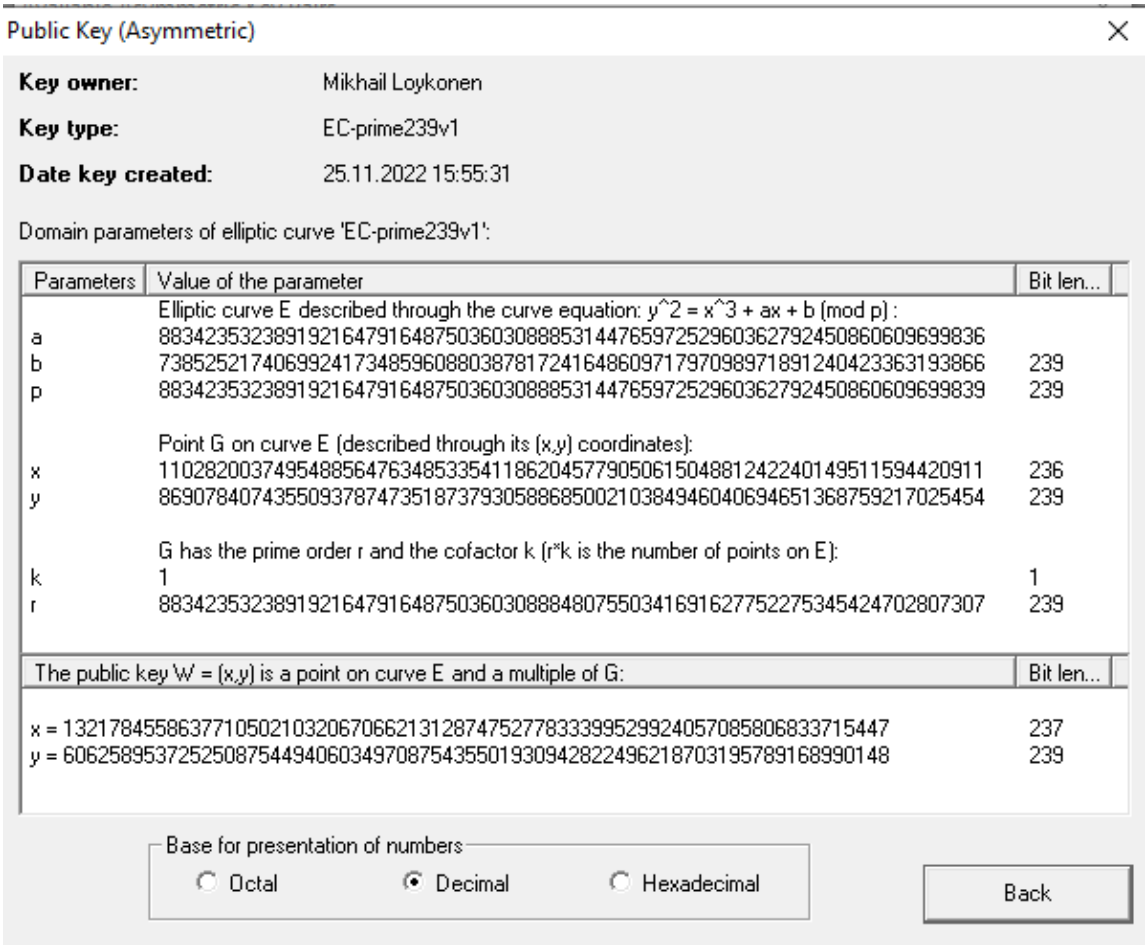


Рисунок 5 - Открытый ключ EC-239

Процессы создания и проверки цифровой подписи.

Обобщенная схема создания и проверки цифровой подписи.

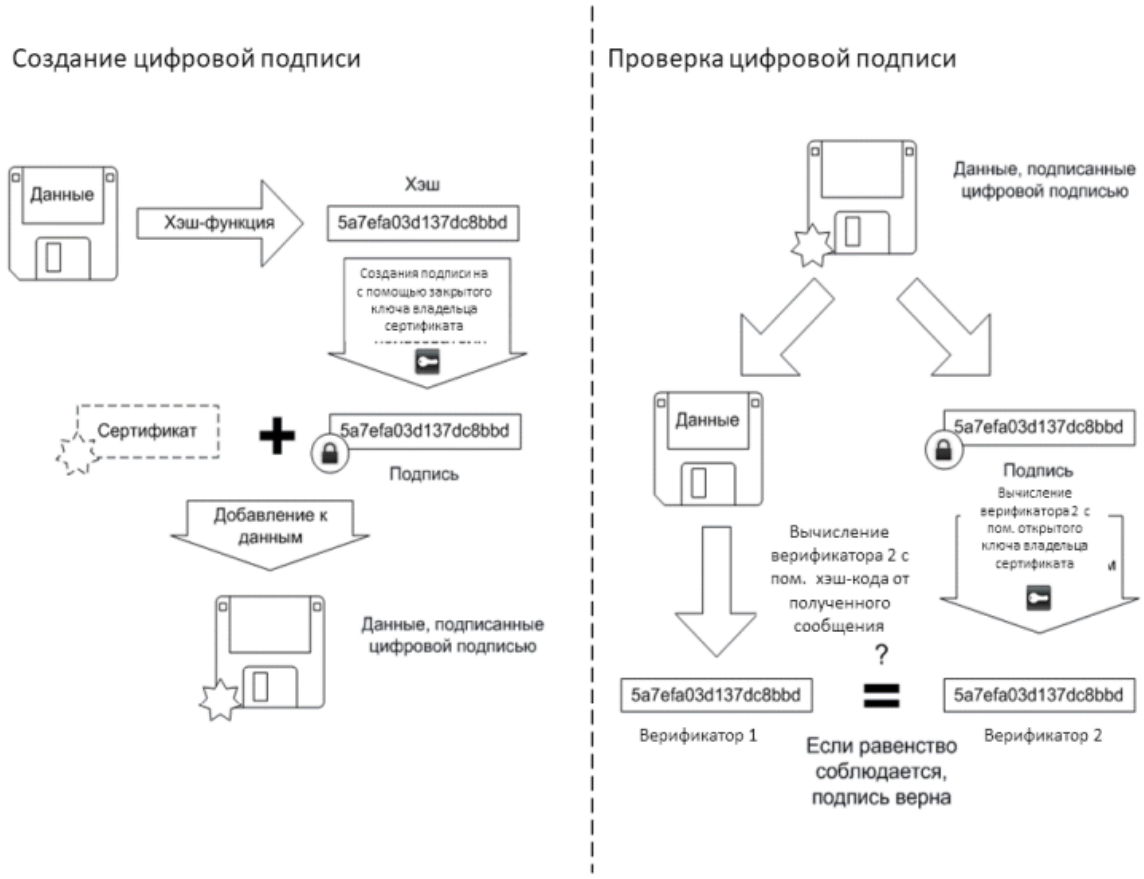


Таблица с фактическим временем генерации цифровой подписи.

Ключ	Время генерации, с
RSA-2048	0.008
DSA-2048	0.002
EC-239	0.002

Скриншоты со значениями цифровой подписи.

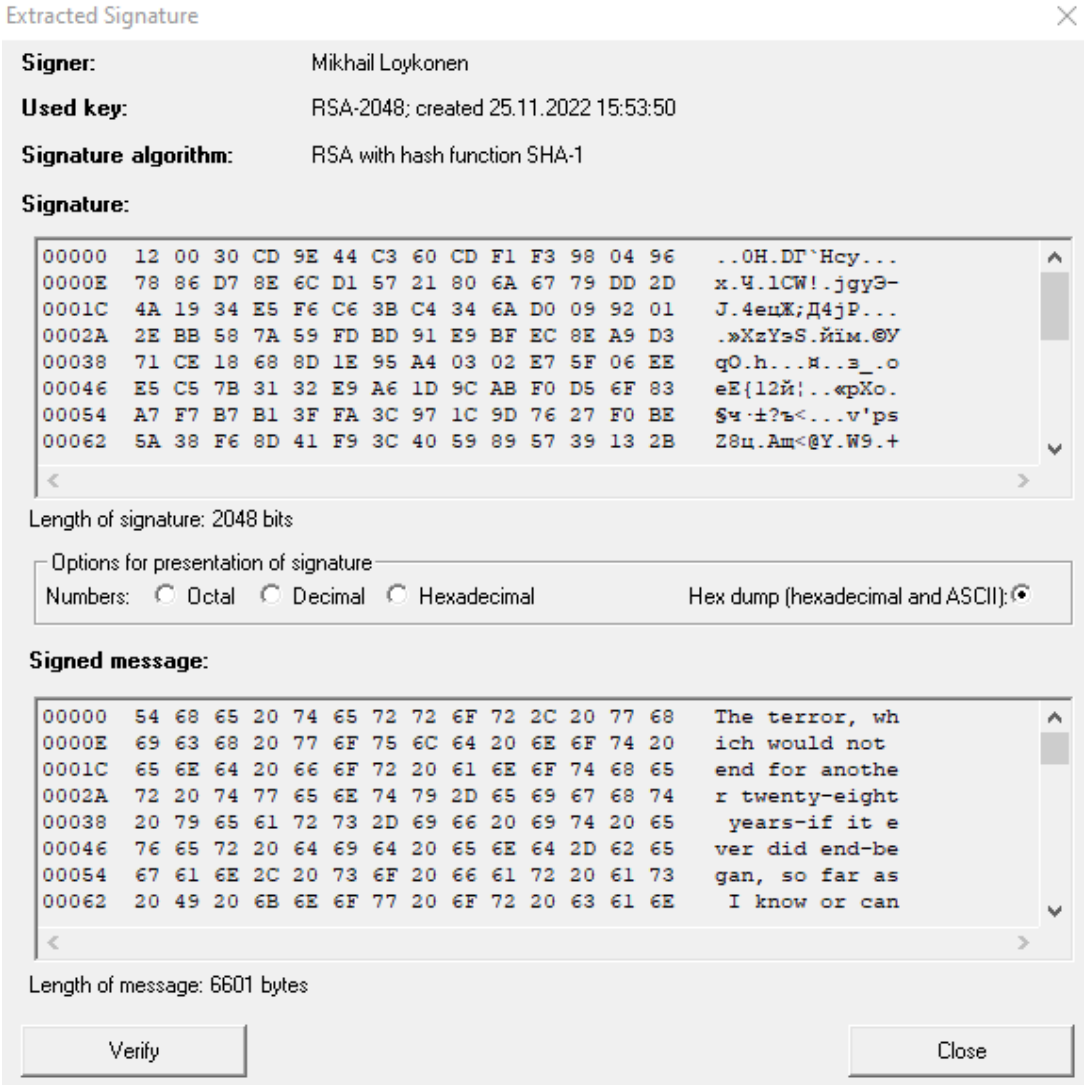


Рисунок 6 - Значение цифровой подписи для ключа RSA-2048

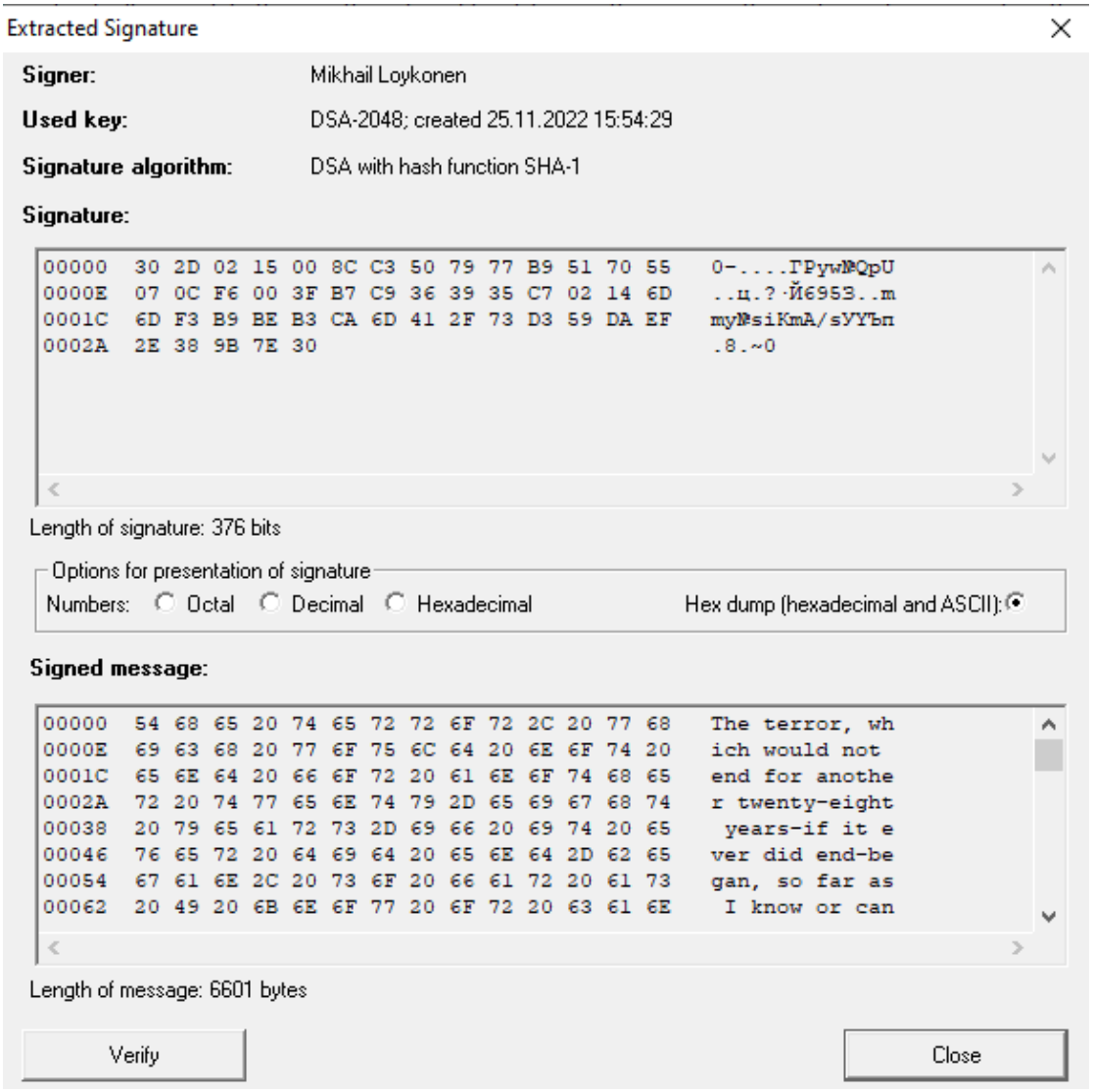


Рисунок 7 - Значение цифровой подписи для ключа DSA-2048

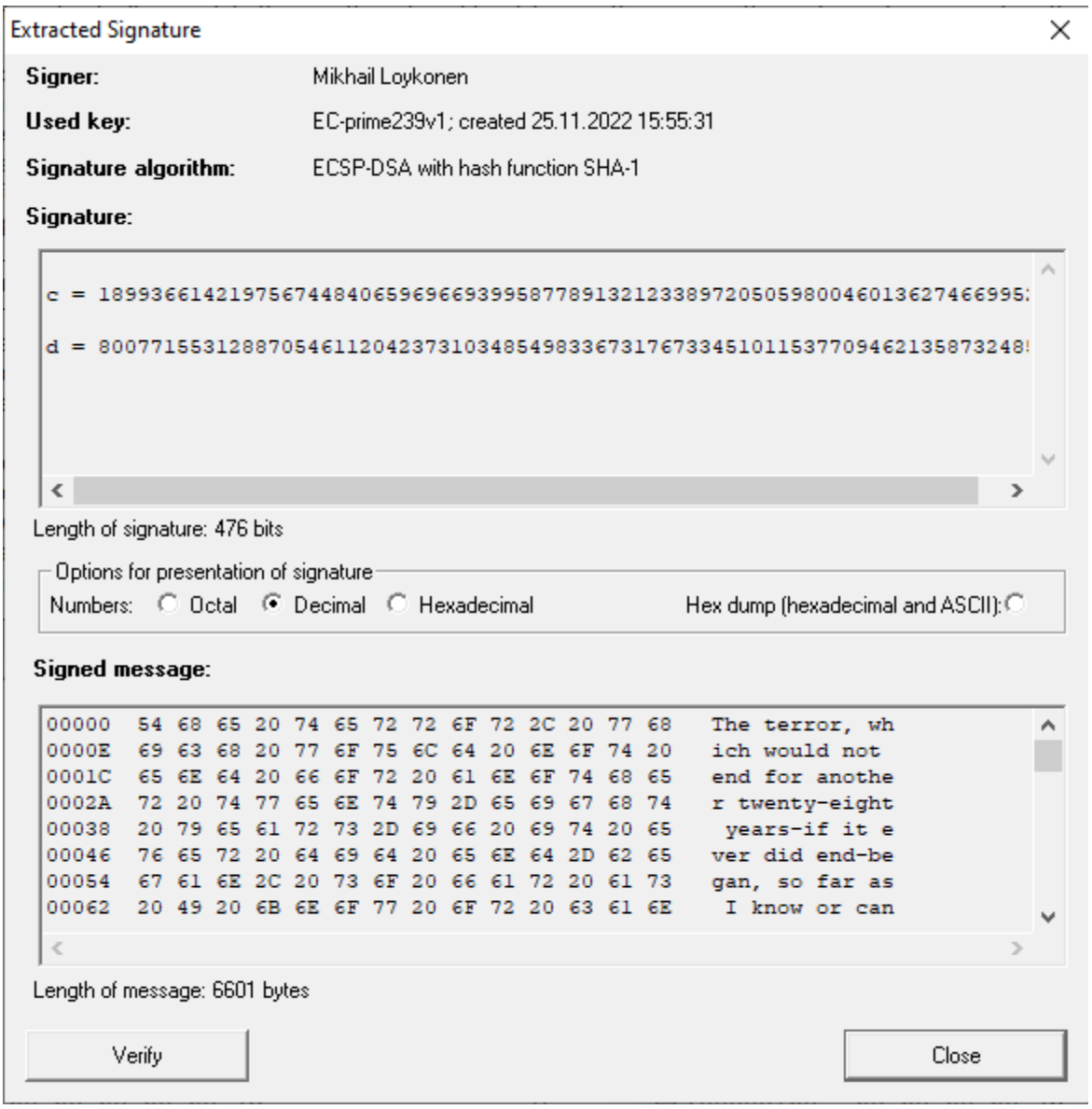


Рисунок 8 - Значение цифровой подписи для ключа EC-239

Скриншоты с результатами проверки цифрой подписи.

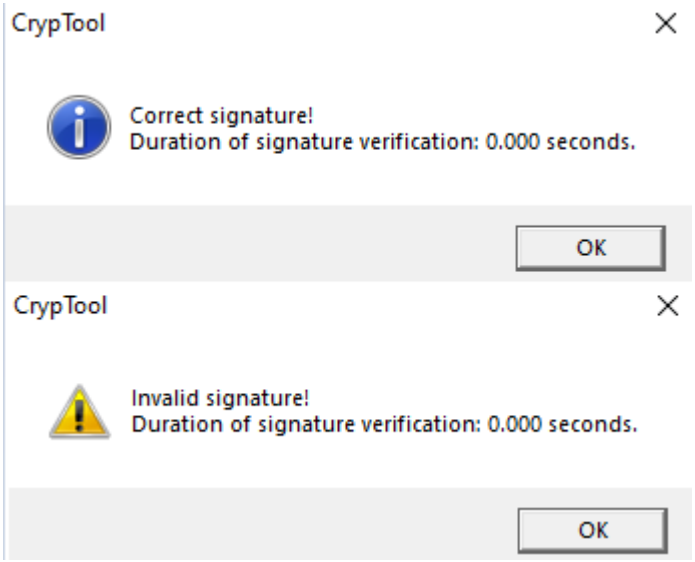


Рисунок 9 - Проверка RSA

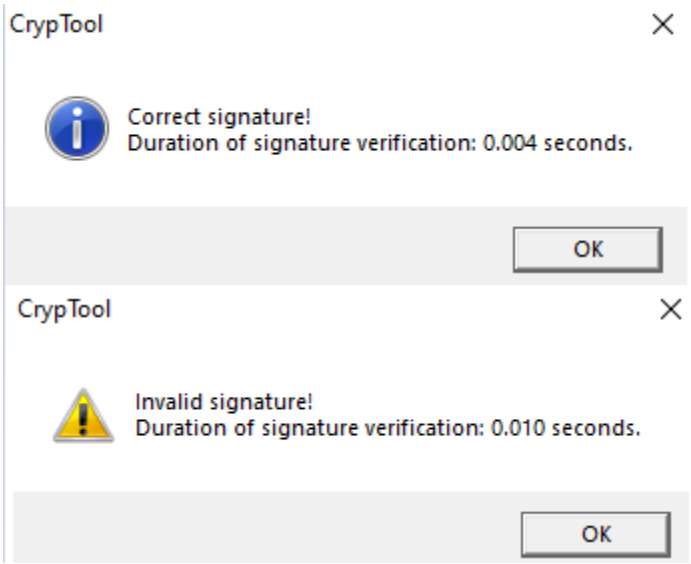


Рисунок 10 - Проверка DSA

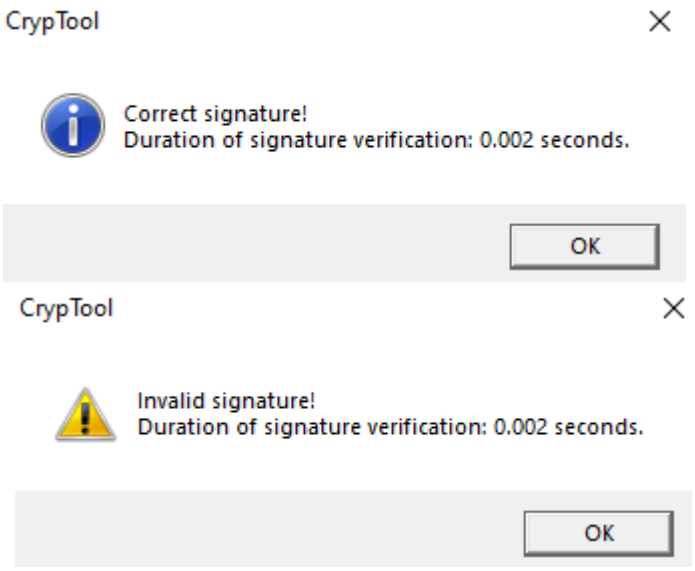
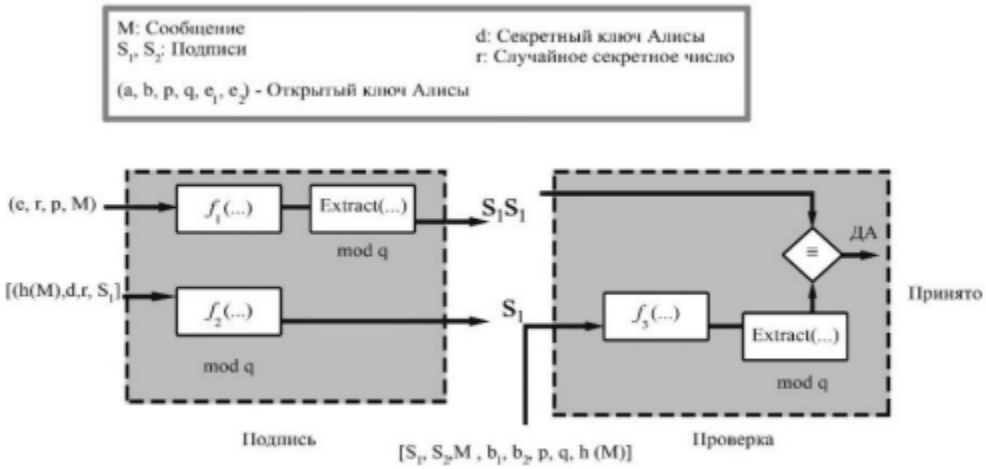


Рисунок 11 - Проверка ЕС

Схемы цифровой подписи на эллиптических кривых.

Описание алгоритма формирования и проверки подписи ECDSA.



Алгоритм подписания ECDSA состоит из следующих операций:

1. Выбирается секретное случайное число r: $r \in (1, q - 1)$

2. Выбирается третья точка на кривой: $P(u, v) = r \times e1$

3. Вычисляется первая часть подписи по формуле: $S1 = u \; mod \; q$, где u- абсцисса.

4. Вычисляется вторая часть подписи по формуле: $S2 = (h(M) + d \times S1) \times r\text{^}(-1) \; mod \; q$, где $h(M)$- дайджест сообщения, d- закрытый ключ

Алгоритм проверки цифровой подписи ECDSA включает следующие операции:

1. Вычисляем промежуточные результаты A и B:

$A = h(M) \times S2\text{^}(-1)\ mod\ q$

$B = S2\text{^}(-1) \times S1\ mod\ q$

2. Восстанавливаем третью точку: $T(x, y) = A \times e1 + B \times e2$

3. Верификатор $V = x\ mod\ q$ сравнивается с первой частью цифровой подписи $S1$.

Результаты (скриншоты) пошагового выполнения ECDSA в CrypTool 1. Сравнение лекционной версии и реализации.

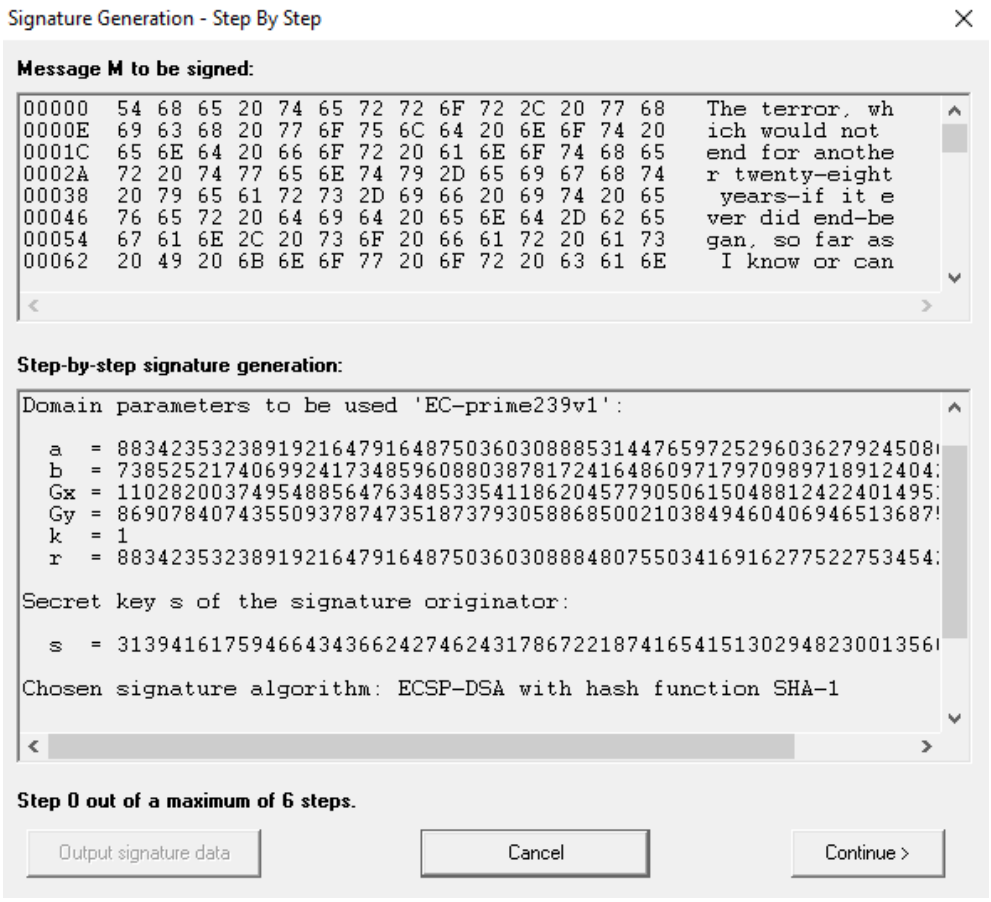


Рисунок 12 - Первый шаг

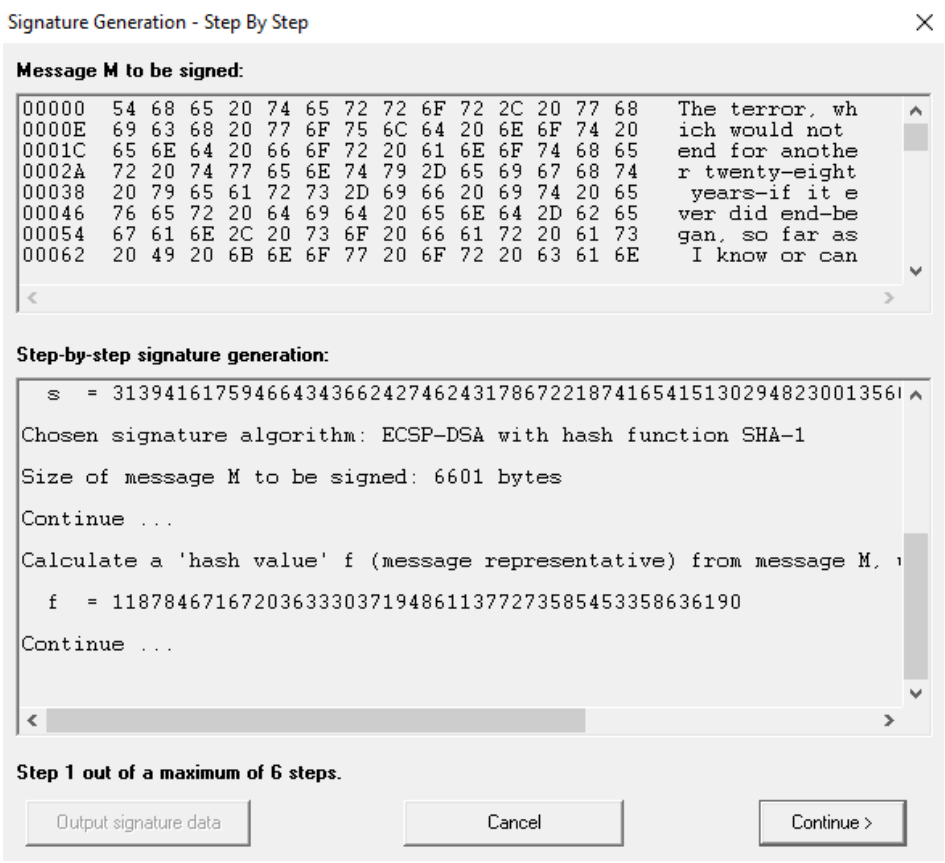


Рисунок 13 - Второй шаг

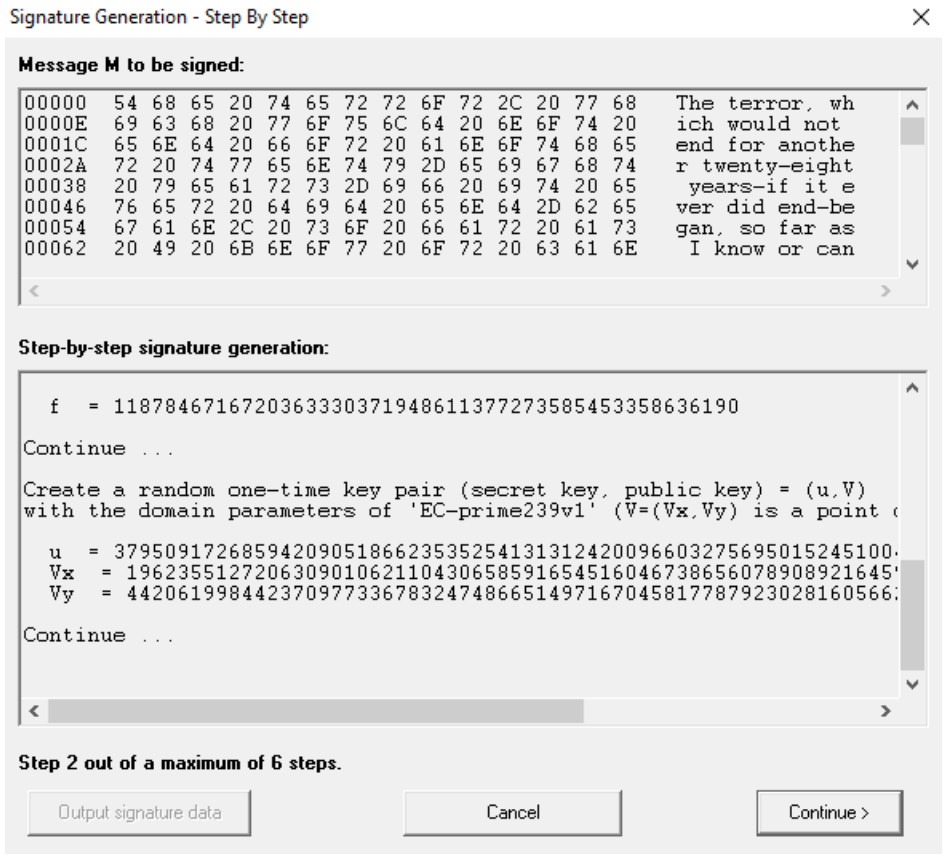


Рисунок 14 - Третий шаг

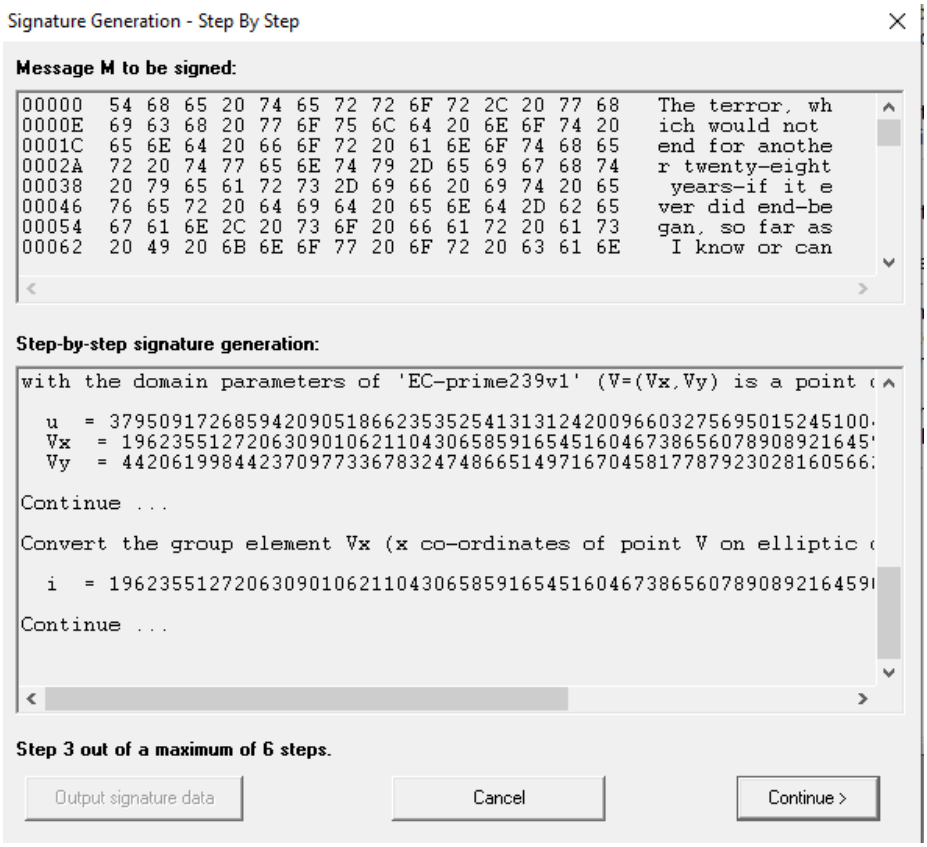


Рисунок 15 - Четвертый шаг

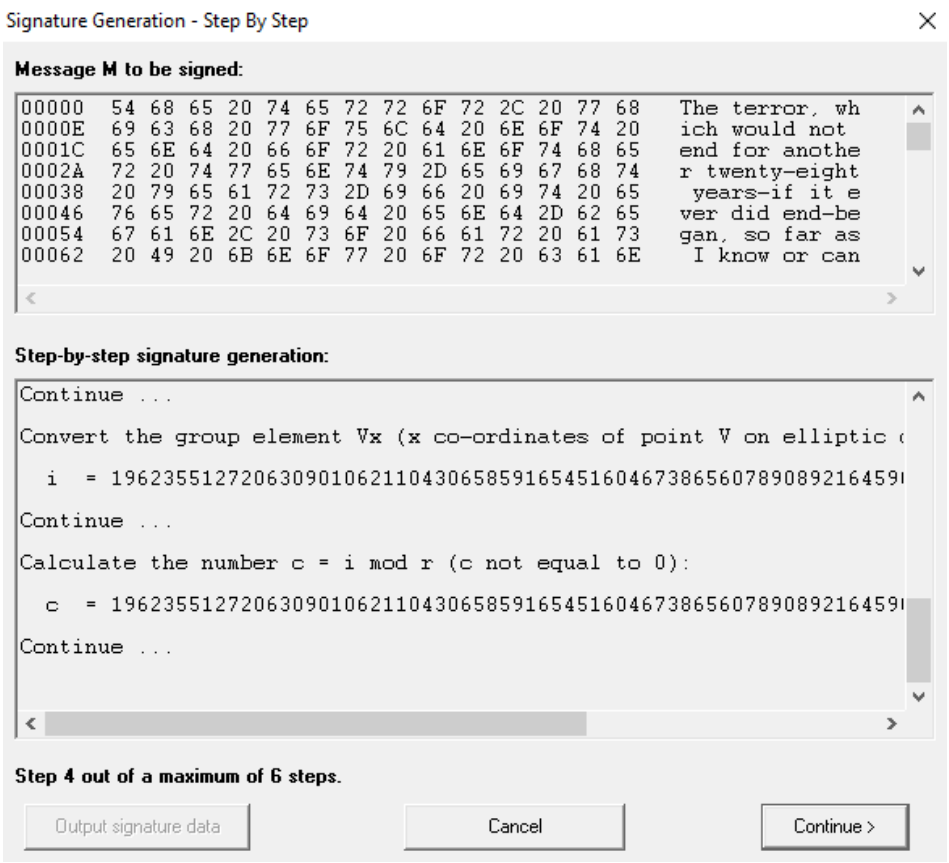


Рисунок 16 - Пятый шаг

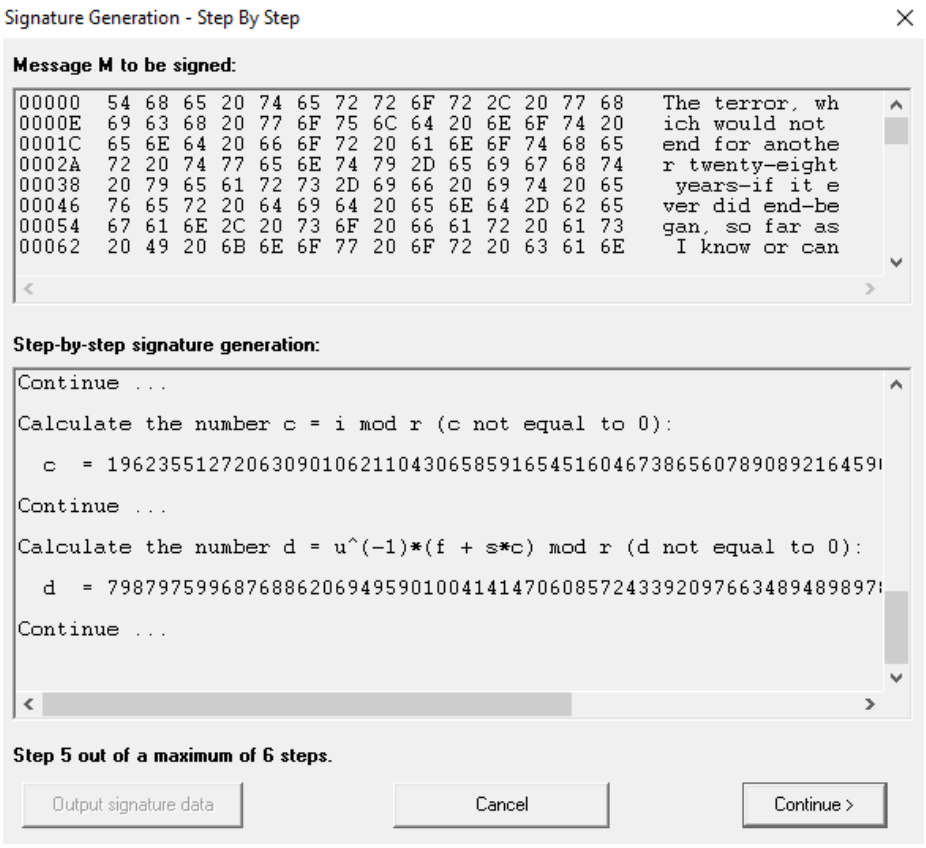


Рисунок 17 - Шестой шаг

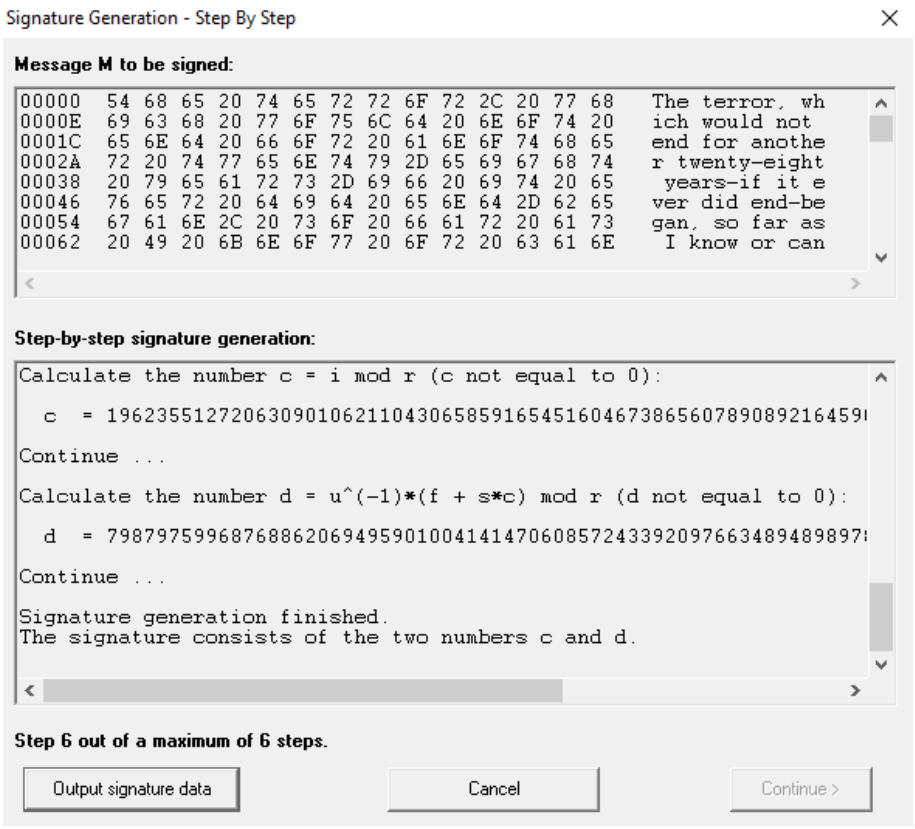


Рисунок 18 - Седьмой шаг

Алгоритм аналогичен лекционному.

Результаты проверки лекционного материала по ECDSA.

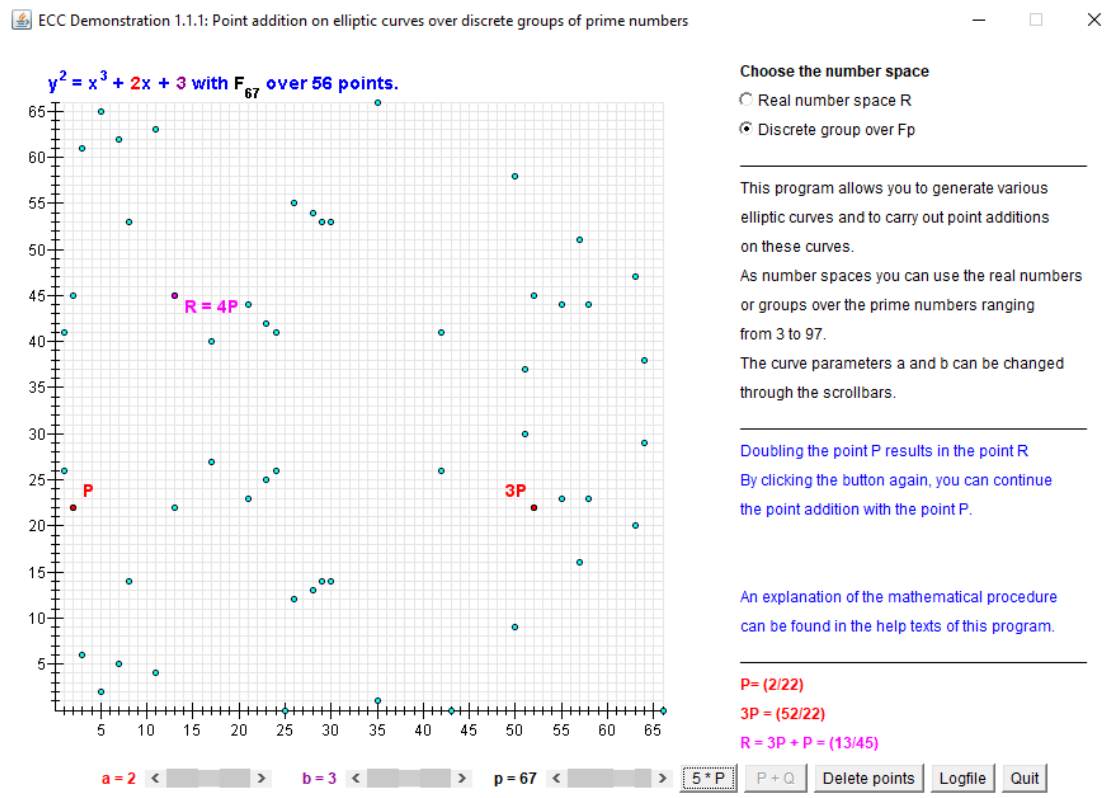


Рисунок 19 - Вычисление e2

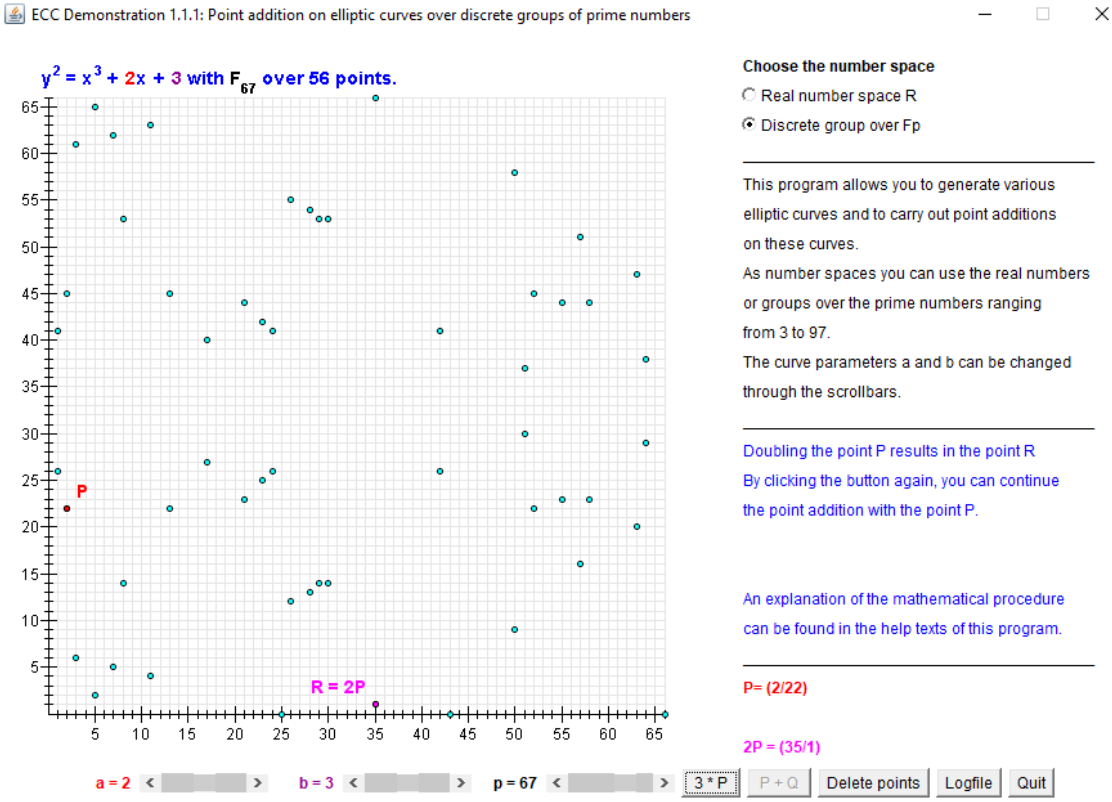


Рисунок 20 - Вычисление C1

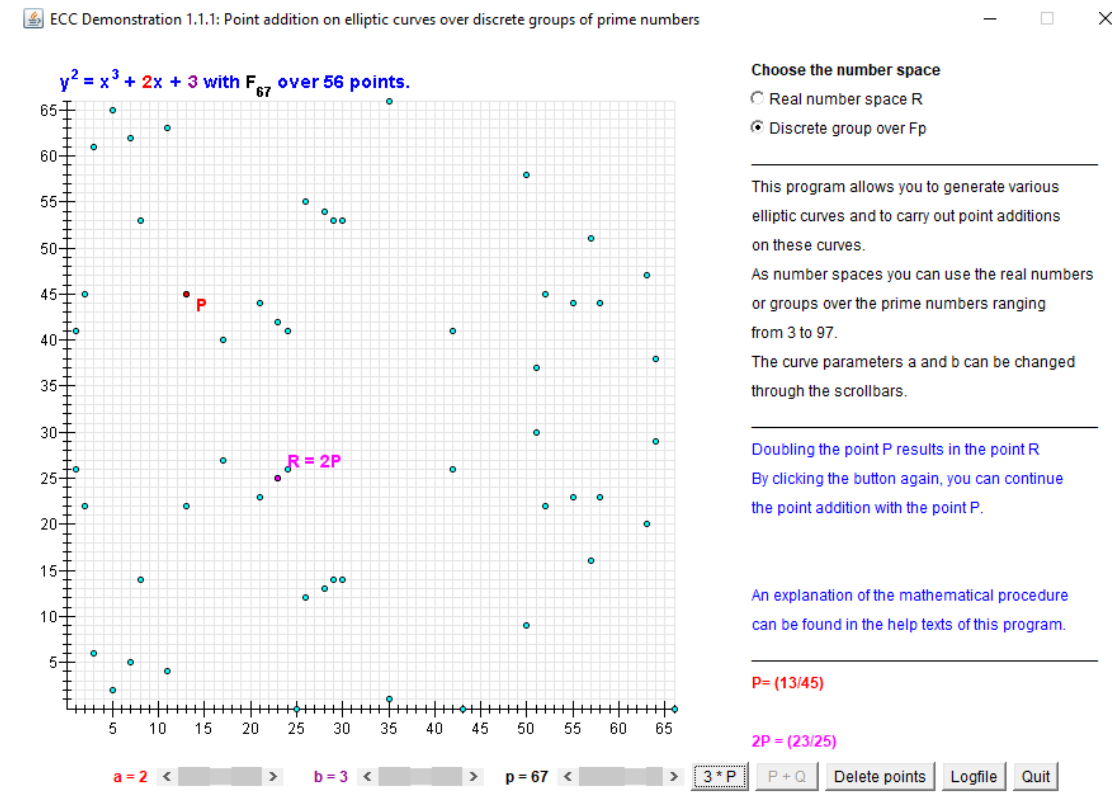


Рисунок 21 - Вычисление r x e2

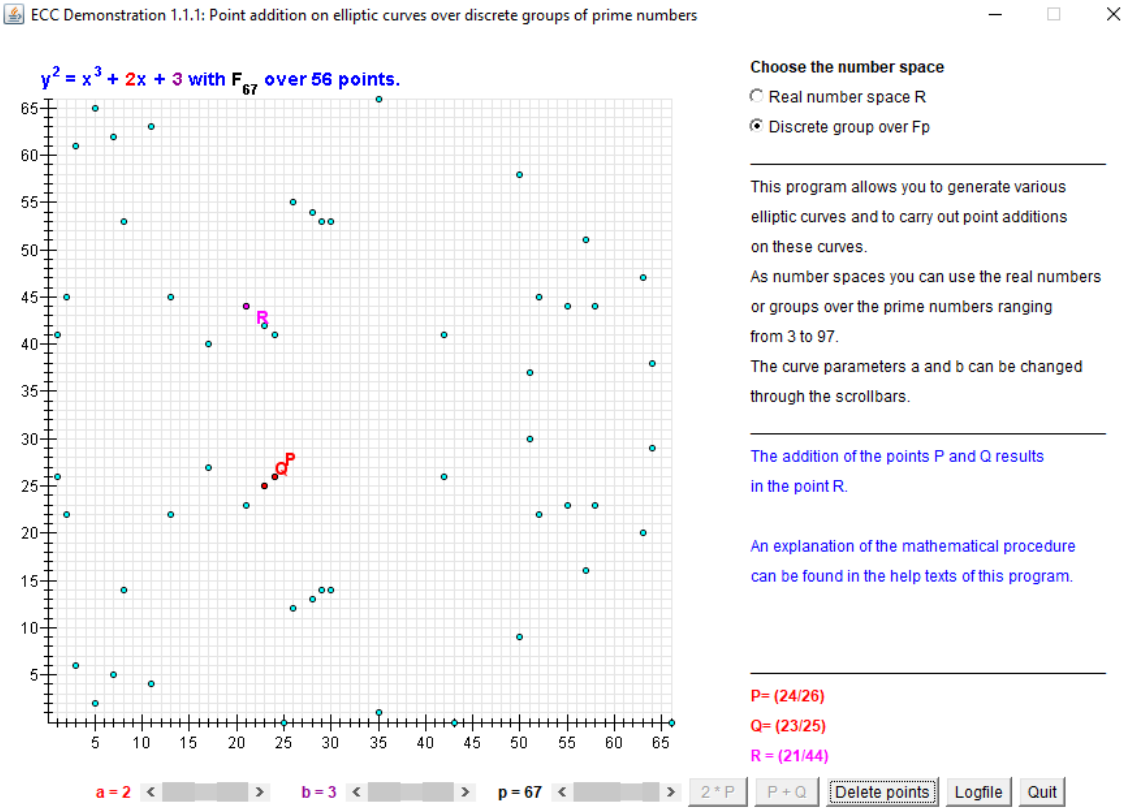


Рисунок 22 - Вычисление C2

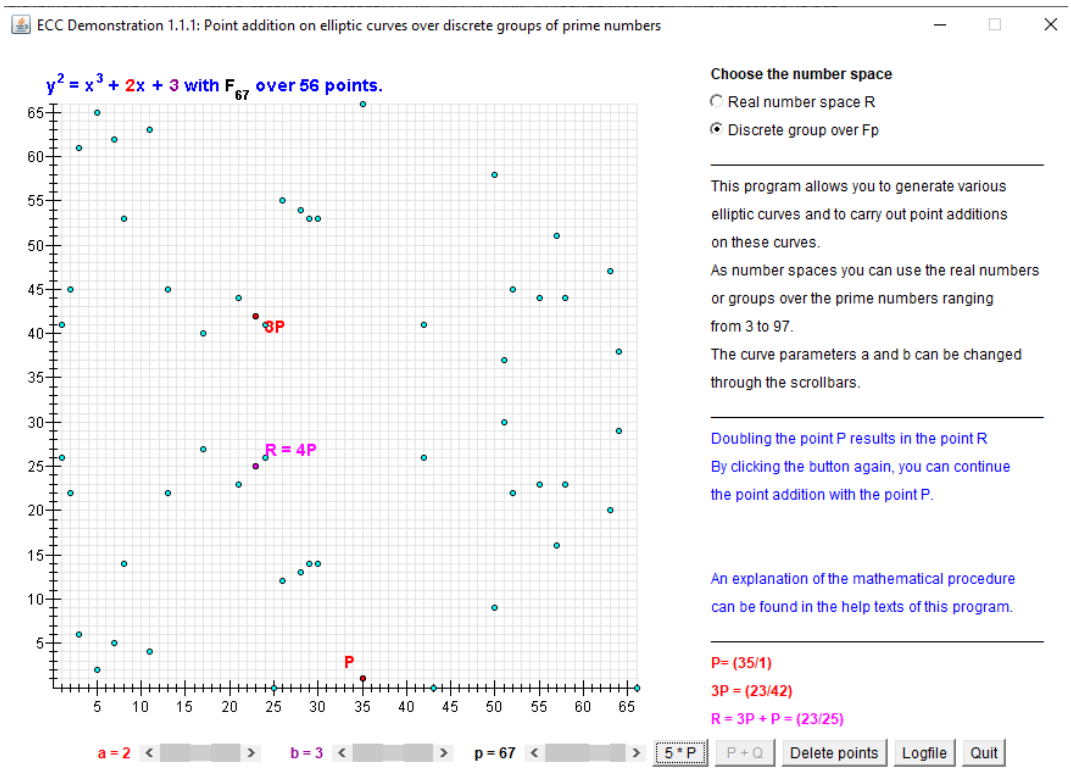


Рисунок 23 - Вычисление d x C1

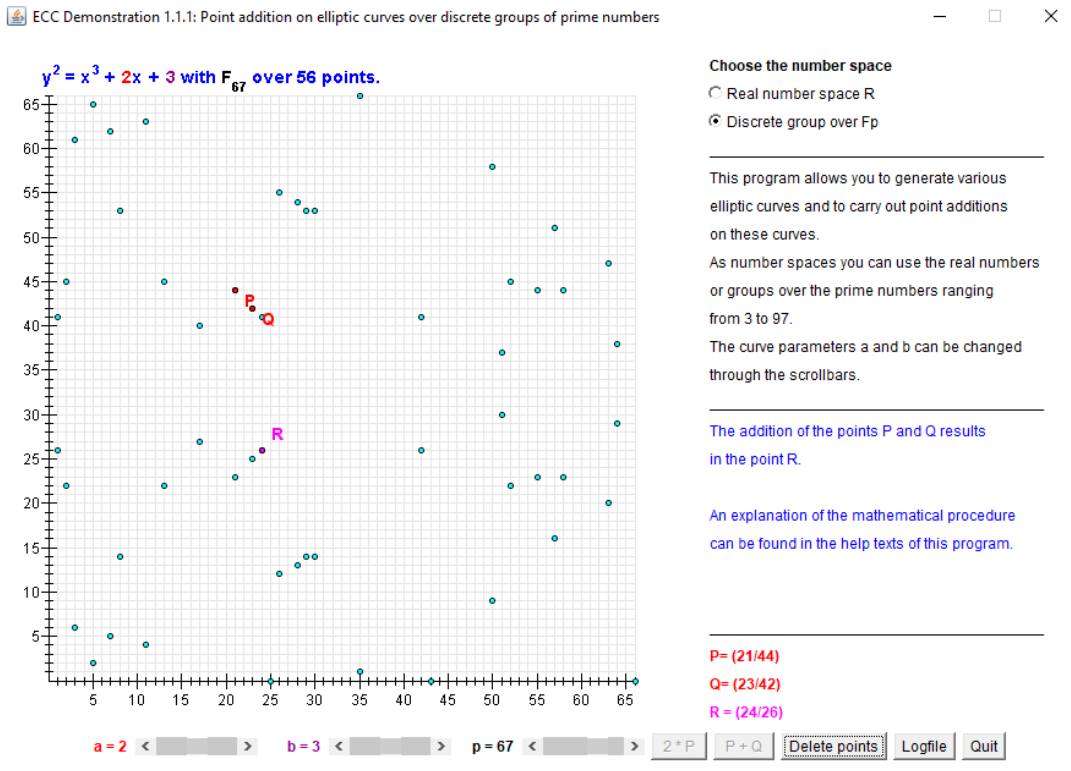


Рисунок 24 - Вычисление P

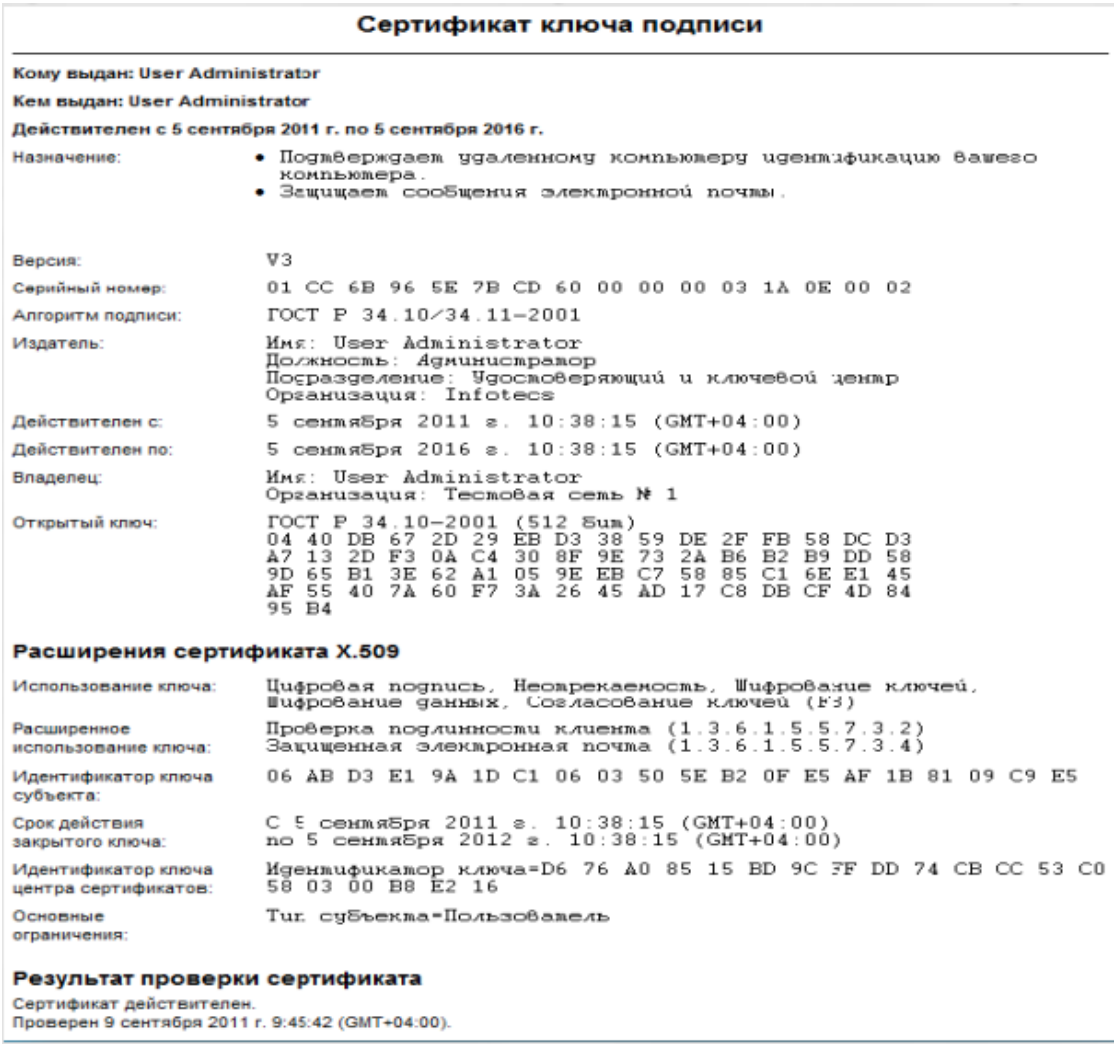
Демонстрация процесса подписи в среде PKI.

Сравнение структуры сертификата (как в лекции) и сертификата из CrypTool 1.0.

```
Version:                2 (X.509v3-1996)
SubjectName:            CN=Loykonen Mikhail [1669557189], DC=cryptool, DC=org
IssuerName:             CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber:           AC:15:10:BA:D0:73:79:FC
Validity  -  NotBefore: Sun Nov 27 16:53:14 2022 (221127135314Z)
             NotAfter:  Mon Nov 27 16:53:14 2023 (231127135314Z)
Public Key Fingerprint: A49D 54FE 00F8 F8AE 145E F0F5 036D 8B70
SubjectKey:             Algorithm rsa (OID 2.5.8.1.1), Keysize = 512
             Public modulus (no. of bits = 302):
               0  32803A25 B09A5F84  66CBB978 AAD45AB2
              10  931502A7 E134D662  FF3E269C FDD51E65
              20  E5E78BF9 5653
             Public exponent (no. of bits = 17):
               0  010001
Certificate extensions:
Private extensions:
    OID 2.206.5.4.3.2:
        PrintableString:
                |C:\Users\\314\350\370\340\AppDat|
                |a\Roaming\CrypTool\PSE/[Mikhail]|
                |[Loykonen][RSA-304][1669557189].|
                |pse                             |

Signature:              Algorithm sha1WithRSASignature (OID 1.3.14.3.2.29), NULL
               0  A725F7BE 565AACBE  11DE6A16 22402DC8
              10  1CB897B3 8735BC64  0A09EFA1 0D47A5F5
              20  54F54FDC 9B6B008F  AC6FD951 7FB8D490
              30  FED2A214 CC4920E0  BDF842D9 A06A2672
              40  7CBFF81E 03CFC3B5  E135CEA9 608F4716
              50  81FF9120 A5924B65  CAA59F57 F9820CFD
              60  01294EB3 BCBD4442  311D440B 5EC5BBE5
              70  30069382 6312039F  D05677C1 41EE8C1F
              80  A90C3A16 554C1C2D  C236CD2D 470A7506
              90  A0EC12E2 442992AD  9EA72AA0 127A22F5
              A0  90067062 A21A8596  A5706827 0204EC45
              B0  8BC3B7F7 C35273C7  48A5EE09 94DED8E9
              C0  A4E1B7F3 E3F864DF  59DC0962 535552F3
              D0  24939B19 04B07965  A3C22C2F 7DA2FF8E
              E0  E5D50DBF 5FC55206  69A61C12 9AA0F67C
              F0  2CCFFB57 C047AD5F  29BFD8D5 2126CE95
Certificate Fingerprint (MD5):    FB:CF:42:F7:A5:D7:21:35:12:24:F0:DD:8B:C9:DB:36
Certificate Fingerprint (SHA-1):  02D5 41B6 D0B5 32E5 5A56 027F 0130 4C22 C026 9B05
```

Рисунок 25 - Сертификат Cryptool



Сертификат ключа подписи

Кому выдан: User Administrator

Кем выдан: User Administrator

Действителен с 5 сентября 2011 г. по 5 сентября 2016 г.

Назначение:
- Подтверждает удаленному компьютеру идентификацию вашего компьютера.
- Защищает сообщения электронной почты.

Версия:	V3
Серийный номер:	01 CC 6B 96 5E 7B CD 60 00 00 00 03 1A 0E 00 02
Алгоритм подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Имя: User Administrator Должность: Администратор Подразделение: Удостоверяющий и ключевой центр Организация: Infotecs
Действителен с:	5 сентября 2011 г. 10:38:15 (GMT+04:00)
Действителен по:	5 сентября 2016 г. 10:38:15 (GMT+04:00)
Владелец:	Имя: User Administrator Организация: Тестовая сеть № 1
Открытый ключ:	ГОСТ Р 34.10-2001 (512 бит) 04 40 DB 67 2D 29 EB D3 38 59 DE 2F FB 58 DC D3 A7 13 2D F3 0A C4 30 8F 9E 73 2A B6 B2 B9 DD 58 9D 65 B1 3E 62 A1 05 9E EB C7 58 85 C1 6E E1 45 AF 55 40 7A 60 F7 3A 26 45 AD 17 C8 DB CF 4D 84 95 B4

Расширения сертификата X.509

Использование ключа:	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F3)
Расширенное использование ключа:	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Идентификатор ключа субъекта:	06 AB D3 E1 9A 1D C1 06 03 50 5E B2 0F E5 AF 1B 81 09 C9 E5
Срок действия закрытого ключа:	С 5 сентября 2011 г. 10:38:15 (GMT+04:00) по 5 сентября 2012 г. 10:38:15 (GMT+04:00)
Идентификатор ключа центра сертификатов:	Идентификатор ключа=D6 76 A0 85 15 BD 9C 7F DD 74 CB CC 53 C0 58 03 00 B8 E2 16
Основные ограничения:	Тип субъекта=Пользователь

Результат проверки сертификата

Сертификат действителен.
Проверен 9 сентября 2011 г. 9:45:42 (GMT+04:00).

Рисунок 26 - Лекционный сертификат

Основные отличия:

- В Cryptool отсутствует поле “назначение”.
- В Cryptool пункт расширения значительно меньше, содержит только идентификатор.
- В Cryptool есть хэш открытого ключа.
- В Cryptool присутствуют дополнительные хэши (MD5 и SHA-1)

Схема процедуры подписания из CrypTool.

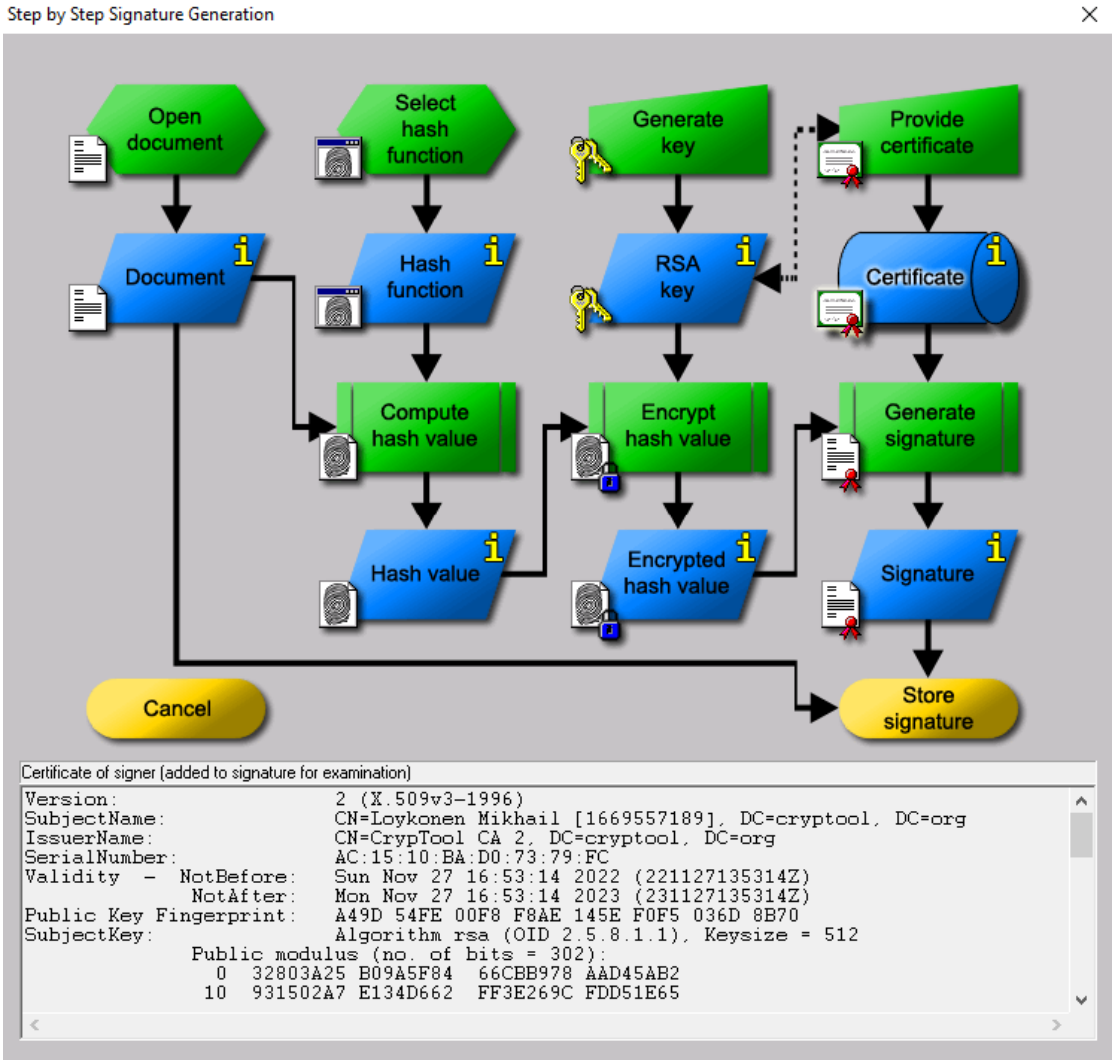


Рисунок 27 - Схема подписания

Подписание своего отчета.

Скриншот титульного листа с цифровой подписью.

Сертификатом, полученным в Cryptool, не удалось подписать отчет, ошибка показана на рис. 28.

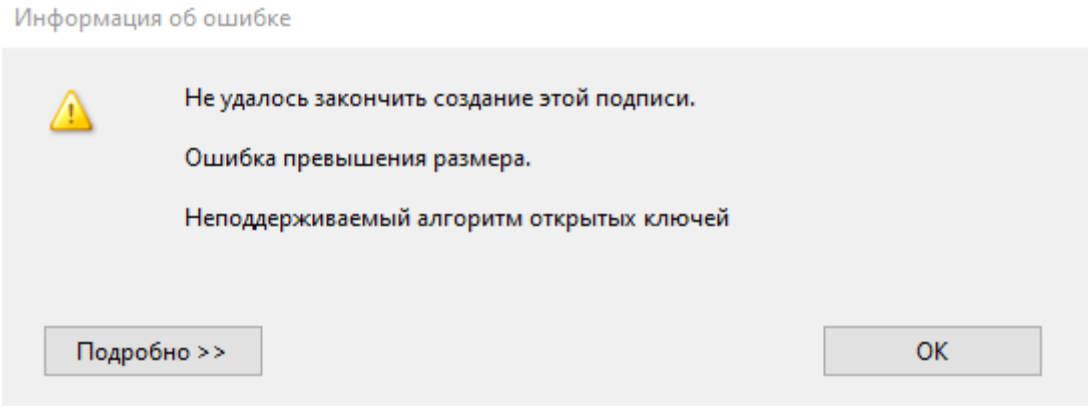


Рисунок 28 - Попытка подписать документ

На рис. 29 показана подпись, сделанная средствами программы Adobe Reader.

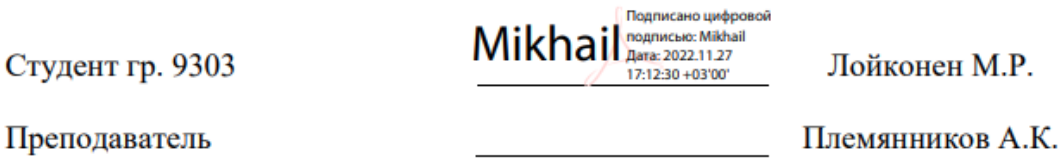


Рисунок 29 - Подпись отчета

Скриншоты свойств подписи и сертификата.

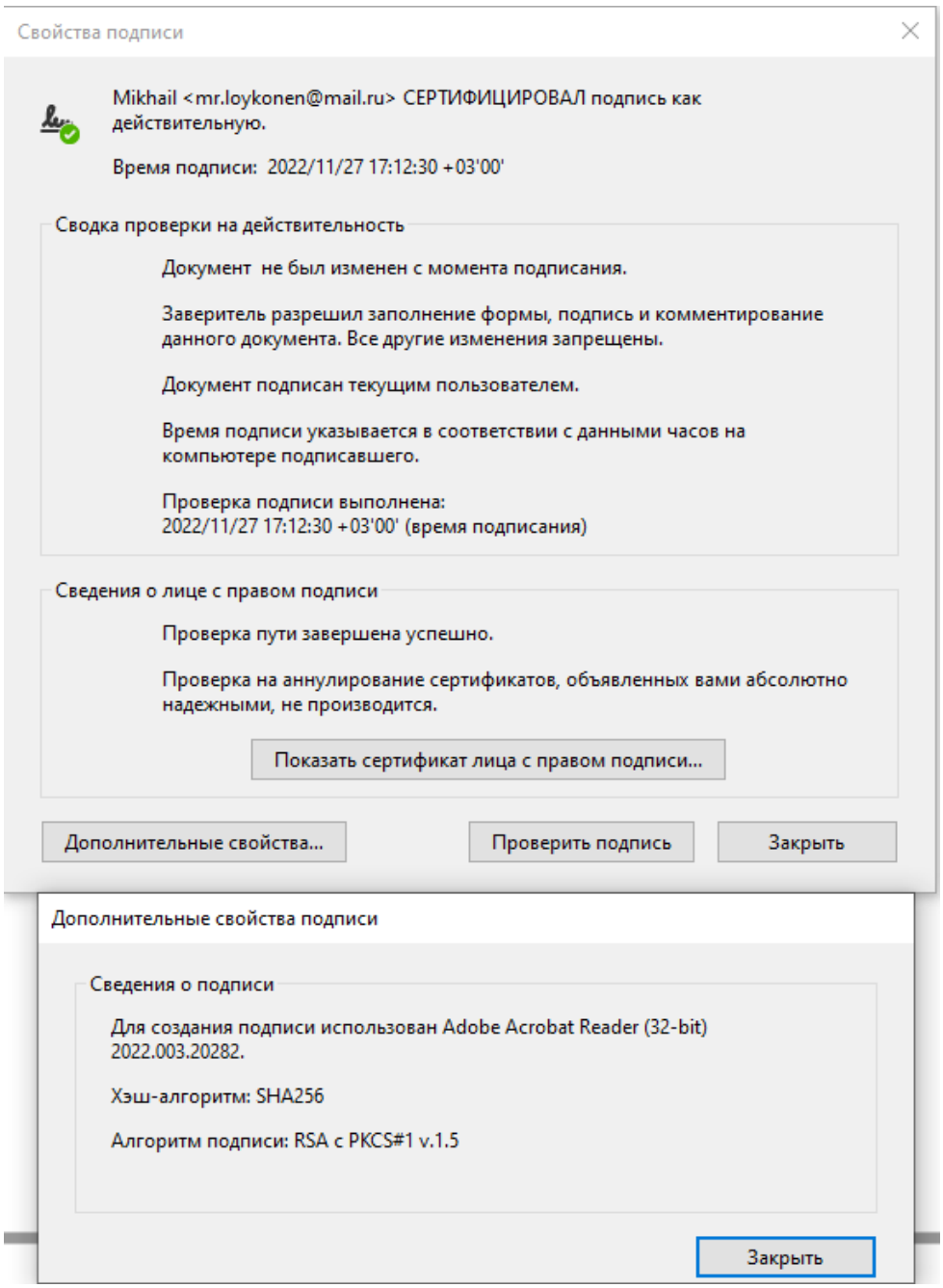


Рисунок 30 - Свойства подписи

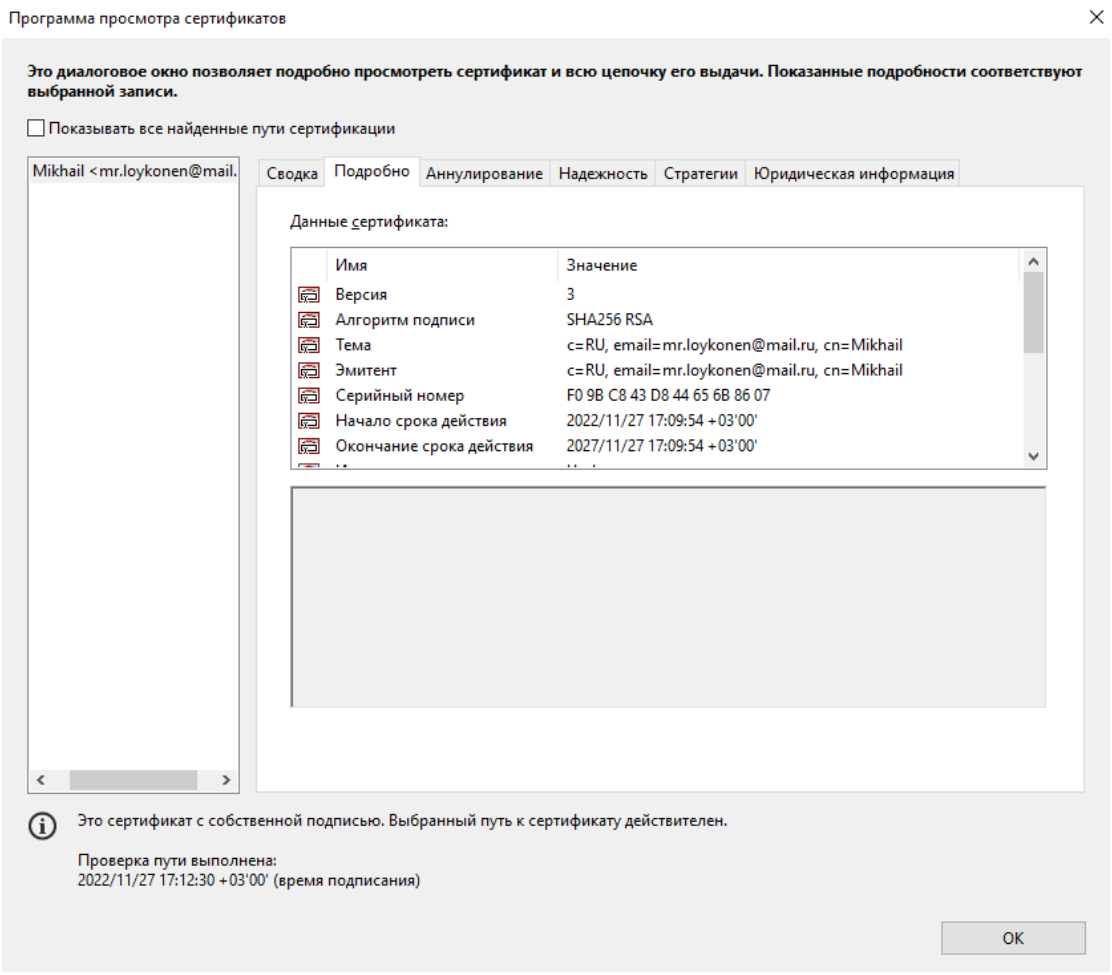


Рисунок 31 - Свойства сертификата

Скриншот результата проверки после внесения изменений в отчет.

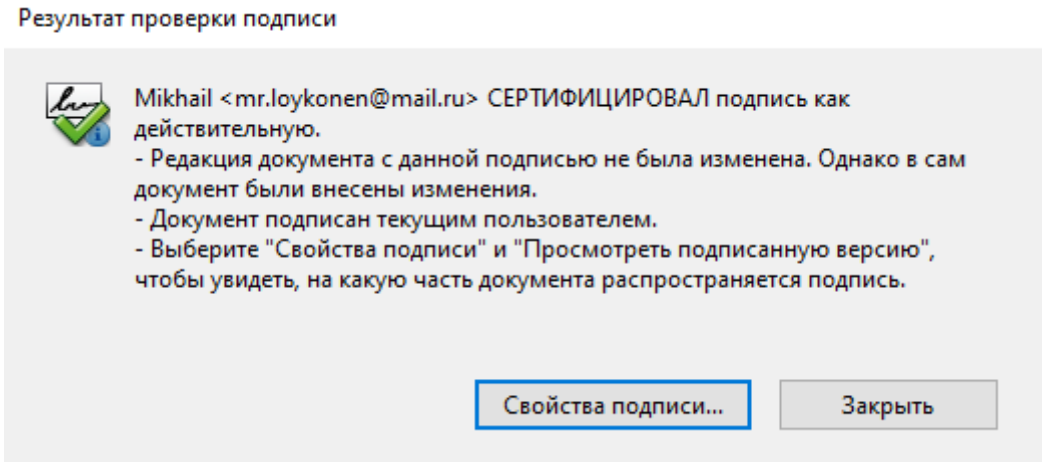


Рисунок 32 - Результаты проверки подписи

Выводы.

1. Были исследованы алгоритмы генерации ключевых пар – RSA, DSA и ECDSA. RSA основан на задаче факторизации, DSA – на задаче дискретного логарифмирования, ECDSA – модификация DSA, работающая в группе точек эллиптической кривой. Установлено, что пары ключей ECDSA генерируются быстрее, чем RSA и DSA.

2. Был изучен процесс создания и проверки цифровой подписи. Создание осуществляется с помощью закрытого ключа владельца сертификата, проверка осуществляется открытым ключом. В цифровой подписи указывается дата создания, владелец, алгоритм хэширования, алгоритм шифрования.

3. Была изучена схема цифровой подписи ECDSA. Открытый ключ представляет из себя набор параметров (a, b, q, p, $\boldsymbol{e_1}$, $\boldsymbol{e_2}$), где a, b, p – значения, определяющие кривую, $\boldsymbol{e_1}$ – точка на кривой, q – такое простое число, что оно является порядком одной из циклических подгрупп группы точек кривой: q x ($\boldsymbol{x_1}$, $\boldsymbol{y_1}$) = 0, $\boldsymbol{e_2}$ – точка на кривой, $\boldsymbol{e_2 = d \times e_1}$, d – закрытый ключ. Алгоритм подписания состоит в вычислении двух частей подписи. Для проверки необходимо вычислить верификатор и сравнить его со второй частью.

4. Был рассмотрен процесс создания подписи в среде PKI и сгенерирован собственный сертификат. Сертификат содержит следующую информацию: информация о владельце и об организации, которая его выдала, срок действия, открытый ключ пользователя, цифровая подпись.

5. Была произведена подпись собственного отчета. При внесении изменений в отчет и последующей проверке подписи, было получено сообщение о том, что в документ внесены изменения.