

Санкт-Петербургский государственный электротехнический
университет «ЛЭТИ» им. В.И. Ульянова (Ленина)

Лабораторная работа № 8

Изучение и исследование алгоритмов создания и проверки
электронной подписи

Студентка: Усачева Дарья, группа 1384

Руководитель: Племянников А.К., доцент каф. ИБ

Санкт-Петербург, 2024

Цель работы и задачи

Цель: Повысить свою компетенцию в области алгоритмов создания и проверки электронной подписи и в криптографии в целом.

Задачи:

1. Изучить генерацию ключевых пар для алгоритмов RSA, DSA, и ECDSA.
2. Изучить процессы создания и проверки электронных подписей.
3. Создать и проверить электронную подпись на основе эллиптических кривых.
4. Продемонстрировать процесс подписи в среде PKI.
5. Подписать свой отчет.

Изучение генерации ключевых пар для алгоритмов RSA, DSA, и ECDSA

Описание алгоритмов генерации ключевых пар

Генерация ключевых пар для алгоритма RSA (с использованием двух больших простых чисел p и q , которые хранятся в секрете) включает следующие шаги:

1. Вычисление $n = p \times q$.
2. Выбор произвольного числа e ($e < n$), которое является взаимно простым с $\phi(n)$.
3. Определение d , удовлетворяющего уравнению $e \times d = 1 \bmod \phi(n)$.
4. Пара (e, n) формирует открытый ключ, а d — закрытый ключ; значения p и q подлежат уничтожению.

Генерация ключевых пар для алгоритма DSA включает следующие этапы:

1. Выбор числа p с длиной 512 - 1024 бит, при этом длина p должна быть кратна 64.
2. Выбор числа q , которое имеет такой же размер в битах, как и размер дайджеста используемой хеш-функции (160 бит для SHA-1), и удовлетворяет условию $p - 1 = 0 \bmod q$.
3. Выбор e_1 , для которого выполняется $e_1^q = 1 \bmod p$.
4. Выбор целого числа $d < q$ и вычисление e_2 , для которого выполняется $e_2 = e_1^d \bmod p$.
5. Числа (e_1, e_2, p, q) образует открытый ключ, а d — закрытый ключ.

Описание алгоритмов генерации ключевых пар

Генерация ключевых пар для алгоритма ECDSA включает следующие этапы:

1. Выбор эллиптической кривой $E_p(a, b)$, где p - простое числом.
2. Выбор точки на кривой $e_1 = (x_1, y_1)$.
3. Выбор простого числа q - порядка одной из циклических подгрупп группы точек эллиптической кривой, удовлетворяющего условию $q \times (x_1, y_1) = 0$.
4. Выбор закрытого ключа d .
5. Вычисление точки на кривой $e_2 = d \times e_1$.
6. Открытый ключ (a, b, q, p, e_1, e_2) .

Значения открытых ключей

Public Parameters of: DARIA USACHEVA

Modulus: 314989511258995491407470819058197066555357323022733414699175267835748872740081418943722084716770900095119200840474247512899226963477285773180897298075869086354524529437835152674083

Exponent: 65537

Base for presentation of numbers

☐ Octal ☒ Decimal ☐ Hexadecimal

Back

Version: 2 (X.509v3-1996)

SubjectName: CN=DARIA USACHEVA [1734899877], DC=crypt

IssuerName: CN=CrypTool CA 2, DC=cryptool, DC=org

SerialNumber: 4F:C4:F2:4B:46:65:C6:4E

Validity - NotBefore: Sun Dec 22 23:38:00 2024 (241222203800Z)

NotAfter: Mon Dec 22 23:38:00 2025 (251222203800Z)

Public Key Fingerprint: CE10 9E02 D07D 928A C252 3CC1 7424 A0EE

SubjectKey: Algorithm NIST-DSA (OID 1.3.14.3.2.12),
DSA prime p (no. of bits = 2048):
0 FFE14748 7B11477C E83D623C CD554917
10 9E3AB5DE 9047DA93 AC06370E 78A272A6
20 1BACE618 28D5CD0D AA21BD34 95A2A0C1
30 375B89D6 6BDE9A99 8D6088D0 DE033C57
40 1D0ADB5A 06464ADC 044ABD15 6CA7A74C
50 16A5E071 80FADA01 85BC4EA5 74FB441D
60 50BA8C62 51D6BF26 7B091871 093DB800
70 C5F880BF 62CFD4C4 3D84B157 1F0A4FC5
80 CCF0B981 F1BB1594 C1F2AF19 676FE39E

Close

Key owner: DARIA USACHEVA

Key type: EC-prime239v1

Date key created: 22.12.2024 23:38:38

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 = 869161134724625083650792092946599662886500338531307119889860040692556051		239
y = 705058440132343763482574834743210890306224135155610961574785343153628129		239

Base for presentation of numbers

☐ Octal ☒ Decimal ☐ Hexadecimal

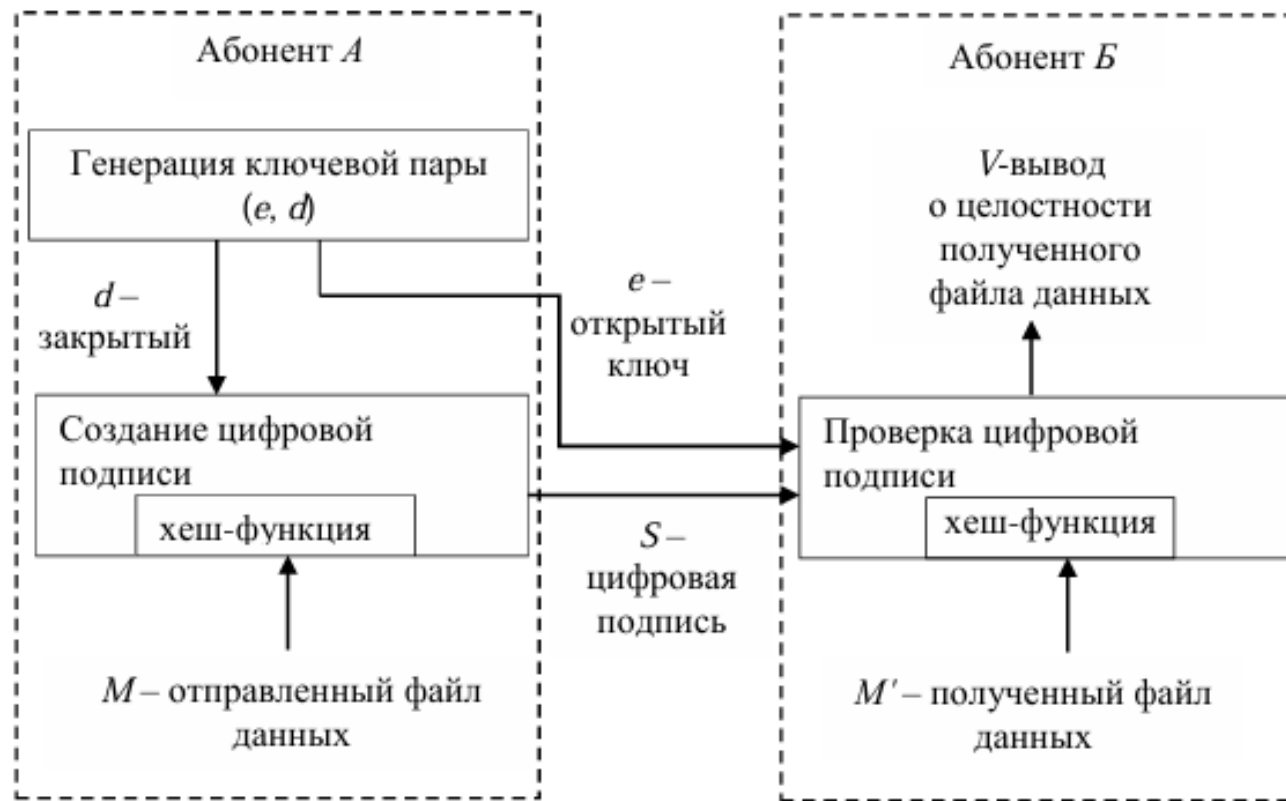
Back

Фактическое время генерации ключевых пар

Алгоритм	Время генерации
RSA-2048	2,861 сек
DSA-2048	3,061 сек
EC-239	0,014 сек

Изучение процессов создания и проверки электронных подписей

Схема, поясняющая работу протокола подписания документа и проверки электронной подписи



Фактическое время генерации электронной подписи

Алгоритм	Время генерации
RSA-2048	0,008 сек
DSA-2048	0,002 сек
EC-239	0,000 сек

Значение электронной подписи и результат ее проверки

Extracted Signature

Signer:

DARIA USACHEVA

Used key:

RSA-2048; created 22.12.2024 23:35:15

Signature algorithm:

RSA with hash function SHA-1

Signature:

00000	77 6A D6 62 F6 20 9F 04 E6 AD C9 6F 5C F9	wjЦbu ..ж-Йo\м
0000E	DA 28 AB 91 3F 40 04 79 C0 0E DD FD C0 2A	Ъ(«.?.yA.3sA*
0001C	1F 95 90 AB 5C 60 3B B7 75 05 A1 3D DD 65	...«\';-u.Ÿ=3e
0002A	E6 8E 18 6E 2F FB CA F5 6D D6 EB 7F 01 EC	ж...n/ыKgmЦл...м
00038	32 F3 A2 4C 68 51 8C E0 7A 58 CA 56 F9 08	2yŸLhQ.azXKVм.
00046	07 F9 52 C3 0E 80 95 AD CF 0F 85 B4 FD 6D	.mRT...-П...rem
00054	16 7A B9 84 D5 A1 5C CD 32 BC D2 42 EF D8	.zŸ.XŸ\H2jTBmIII
00062	80 36 C9 2B 38 C9 AE 52 C2 AD BF 5A 67 06	.6Й+8Й0RB-iZg.

Length of signature: 2048 bits

Options for presentation of signature

Numbers: ☐ Octal ☐ Decimal ☐ Hexadecimal

Hex dump (hexadecimal and ASCII): ☒

Signed message:

00000	0D 0A 31 2E 31 2E 20 48 75 6D 61 6E 69 74	..l.l. Humanit
0000E	79 20 73 74 61 6E 64 73 20 61 74 20 61 20	y stands at a
0001C	64 65 66 69 6E 69 6E 67 20 6D 6F 6D 65 6E	defining momen
0002A	74 20 69 6E 20 68 69 73 74 6F 72 79 2E 20	t in history.
00038	57 65 20 61 72 65 20 63 6F 6E 66 72 6F 6E	We are confron
00046	74 65 64 20 77 69 74 68 20 61 20 70 65 72	ted with a per
00054	70 65 74 75 61 74 69 6F 6E 20 0D 0A 6F 66	petuation ..of
00062	20 64 69 73 70 61 72 69 74 69 65 73 20 62	disparities b

Length of message: 7562 bytes

Verify

Close

CrypTool

Correct signature!

Duration of signature verification: 0.000 seconds.

OK

CrypTool

Invalid signature!

Duration of signature verification: 0.000 seconds.

OK

Создание и проверка электронной подписи на основе эллиптических кривых

Алгоритмы создания и проверки электронной подписи ECDSA

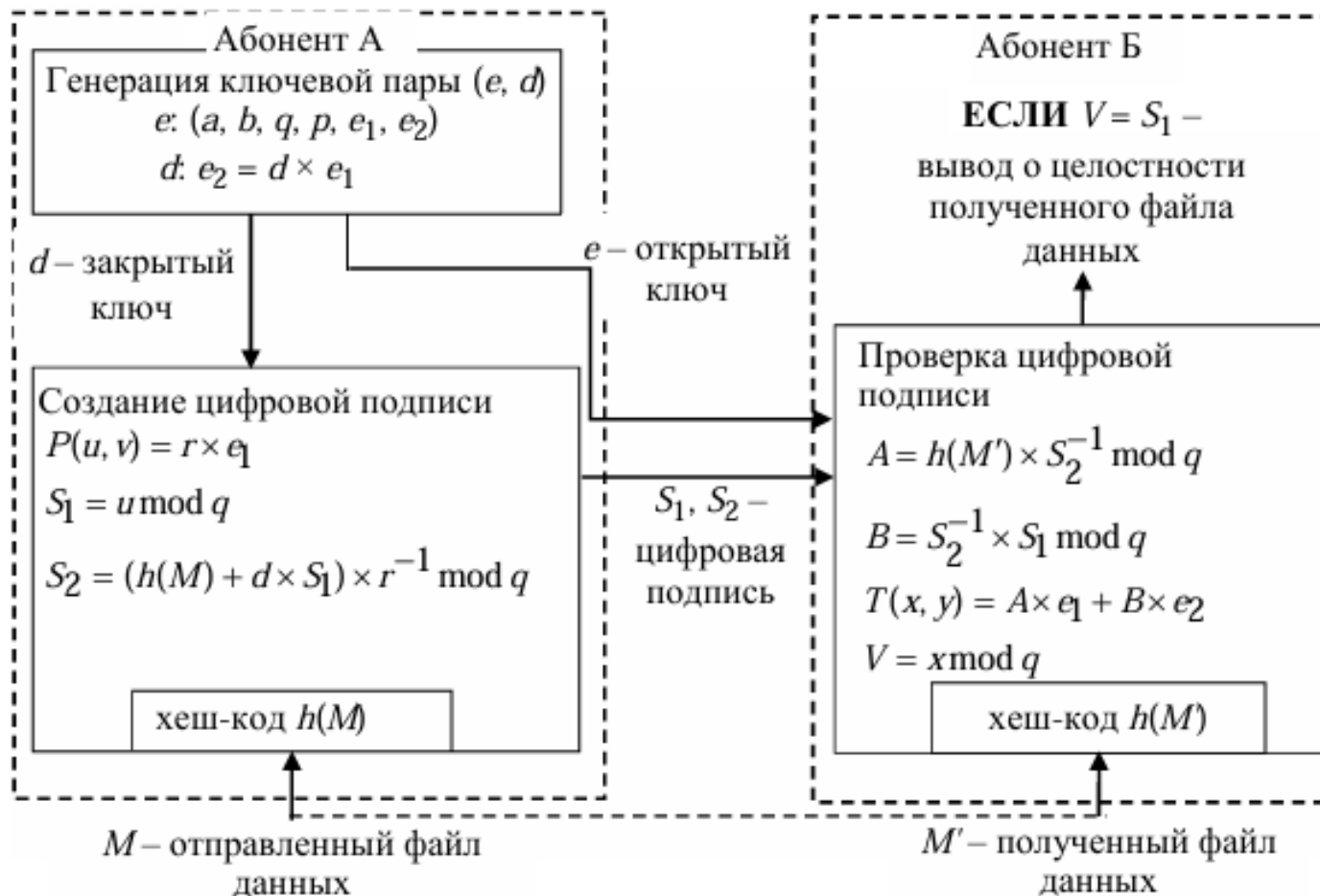
Алгоритм создания электронной подписи ECDSA

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 u — абсцисса.
4. Вычисляется вторая часть подписи по формуле:
$$S_2 = (h(M) + d \times S_1) \times r^{-1} \bmod q,$$
где $h(M)$ — хеш-код сообщения; d — закрытый ключ.

Алгоритм проверки электронной подписи ECDSA

1. Вычисляются промежуточные результаты A и B :
$$A = h(M) \times S_2^{-1} \bmod q,$$
$$B = S_2^{-1} \times S_1 \bmod q.$$
2. Восстанавливается третья точка:
$$T(x, y) = A \times e_1 + B \times e_2.$$
Верификатор $V = x \bmod q$ сравнивается с первой частью подписи S_1 .

Подписание документа и верификация подписи



Последовательность шагов создания подписи

Message M to be signed:

00000 6D 65 6F 77

meow

Step-by-step signature generation:

Signature originator: DARIA USACHEVA

Domain parameters to be used 'EC-prime239v1':

```
a = 88342353238919216479164875036030888531447659725296036279245081
b = 73852521740699241734859608803878172416486097179709897189124041
Gx = 11028200374954885647634853354118620457790506150488124224014951
Gy = 86907840743550937874735187379305886850021038494604069465136871
k = 1
r = 88342353238919216479164875036030888480755034169162775227534541
```

Secret key s of the signature originator:

```
s = 29150367485000442713237211996478299038756914117055334117019811
```

Step 0 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

Step-by-step signature generation:

```
s = 29150367485000442713237211996478299038756914117055334117019811
```

Chosen signature algorithm: ECSP-DSA with hash function SHA-1

Size of message M to be signed: 4 bytes

Continue ...

Calculate a 'hash value' f (message representative) from message M, ...

```
f = 715679189069181012862657191738191532500000735025
```

Continue ...

Step 1 out of a maximum of 6 steps.

Step-by-step signature generation:

```
f = 715679189069181012862657191738191532500000735025
```

Continue ...

Create a random one-time key pair (secret key, public key) = (u,V) with the domain parameters of 'EC-prime239v1' (V=(Vx,Vy) is a point on the curve)

```
u = 50716748525959755513826183749724949378700162542693502136193111
Vx = 6730505914931207341002609671744548717026099910946475396907831
Vy = 5567321228873950613597649967034883259668510280419585287825511
```

Continue ...

Step 2 out of a maximum of 6 steps.

Последовательность шагов создания подписи

Step-by-step signature generation:

```
with the domain parameters of 'EC-prime239v1' (V=(Vx,Vy) is a point on the elliptic curve)
u = 4596299103454599495084631723209311662536445802888187494925514:
Vx = 4330281343362892978064747494779038494414506652205817690935221:
Vy = 560008800154351338425267528898070975226680271039049008483920:
Continue ...
Convert the group element Vx (x co-ordinates of point V on elliptic curve) to integer i
i = 4330281343362892978064747494779038494414506652205817690935221:
Continue ...
```

Step 3 out of a maximum of 6 steps.

Step-by-step signature generation:

```
Continue ...
Calculate the number c = i mod r (c not equal to 0):
c = 4330281343362892978064747494779038494414506652205817690935221:
Continue ...
Calculate the number d = u^(-1)*(f + s*c) mod r (d not equal to 0):
d = 5385019037545927529247700116865247394078540382682988046809183:
Continue ...
```

Step 5 out of a maximum of 6 steps.

Step-by-step signature generation:

```
Continue ...
Convert the group element Vx (x co-ordinates of point V on elliptic curve) to integer i
i = 4330281343362892978064747494779038494414506652205817690935221:
Continue ...
Calculate the number c = i mod r (c not equal to 0):
c = 4330281343362892978064747494779038494414506652205817690935221:
Continue ...
```

Step 4 out of a maximum of 6 steps.

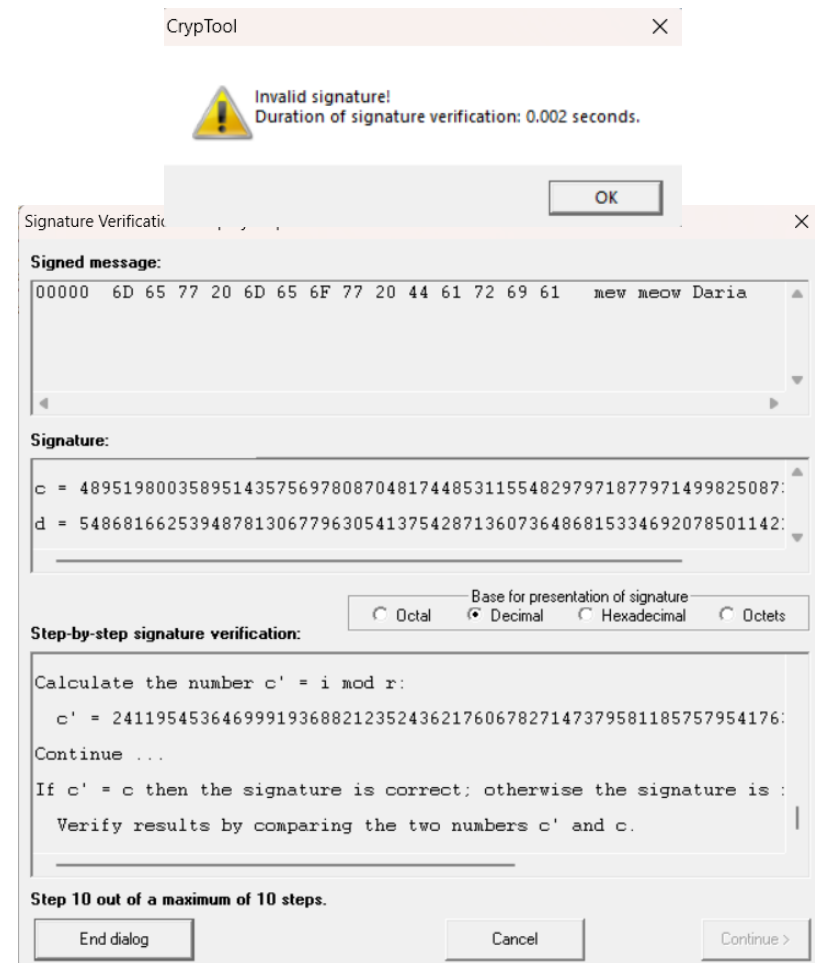
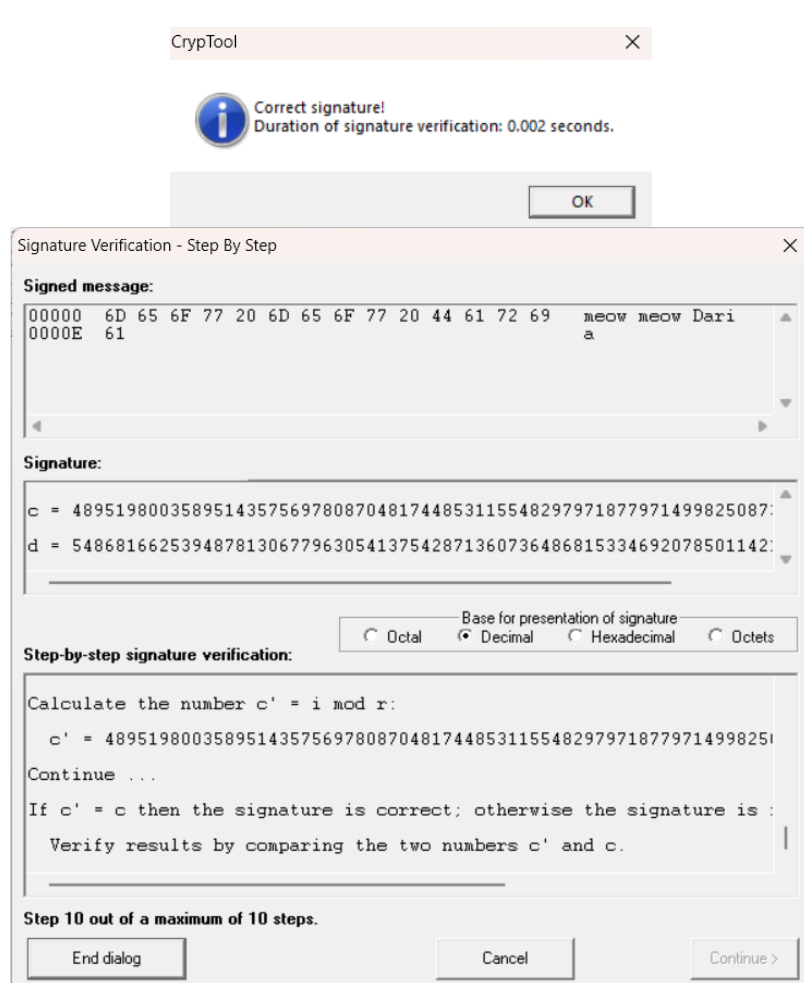
Step-by-step signature generation:

```
Calculate the number c = i mod r (c not equal to 0):
c = 4330281343362892978064747494779038494414506652205817690935221:
Continue ...
Calculate the number d = u^(-1)*(f + s*c) mod r (d not equal to 0):
d = 5385019037545927529247700116865247394078540382682988046809183:
Continue ...
Signature generation finished.
The signature consists of the two numbers c and d.
```

Step 6 out of a maximum of 6 steps.

Результат проверки электронной подписи

Результат проверки для случаев сохранения и нарушения целостности исходного текста



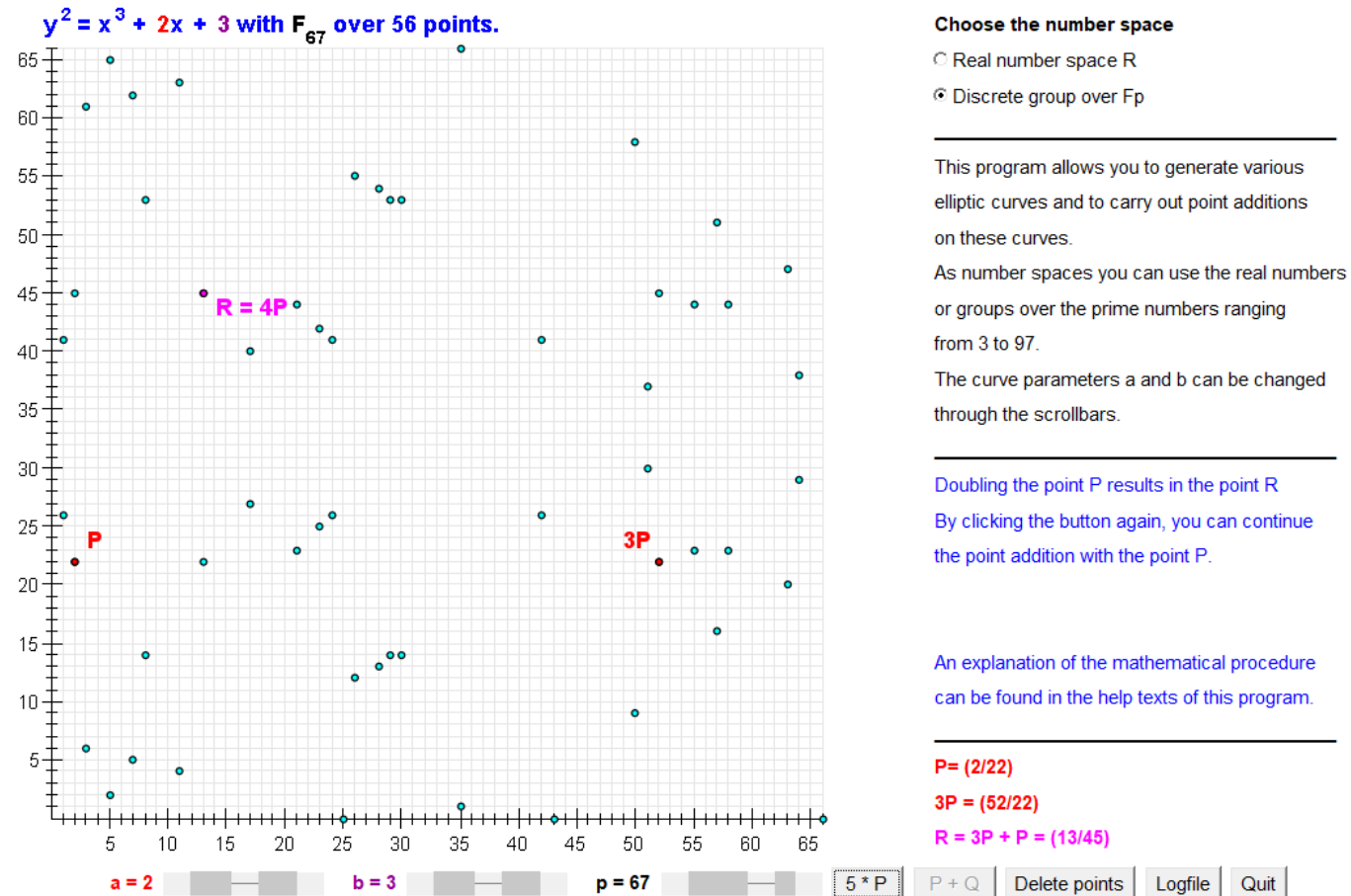
Проверка лекционного материала по ECDSA

Шифр Эль-Гамала на эллиптических кривых

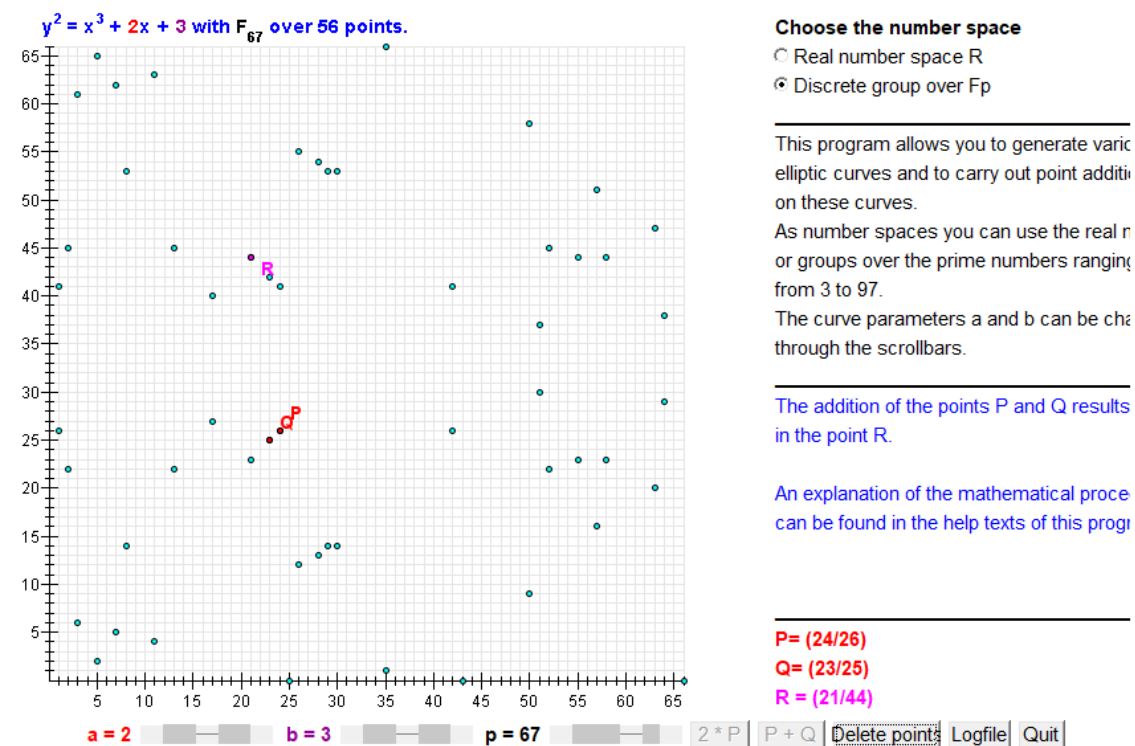
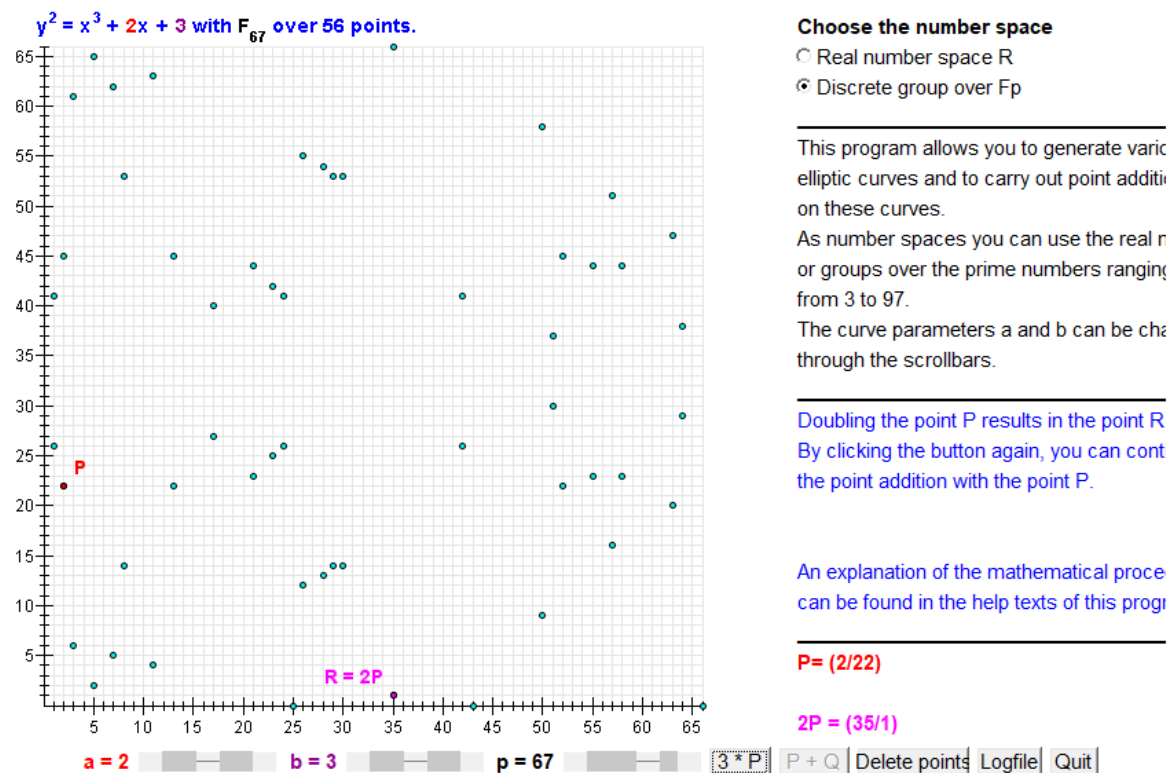
1. Выбираем эллиптическую кривую $E_{67}(2, 3)$, где p - простое число.
2. Выбираем точку на кривой $e_1 = (2, 22)$.
3. Выбираем закрытый ключ $d = 4$.
4. Вычисление точки на кривой $e_2 = d \times e_1 = 4 \times (2, 22) = (13, 45)$.
6. Открытый ключ $(2, 3, 67, (2, 22), (13, 45))$.

7. Выбираем точку для сопоставления открытому тексту $P = (24, 26)$ на кривой.
8. Выбираем секретное случайное число $r = 2$:
 $r \in (1, q-1)$.
9. Создаем шифровку C_1, C_2 :
 $C_1 = r \times e_1 = 2 \times (2, 22) = (35, 1)$
 $C_2 = P + r \times e_2 = (24, 26) + 2 \times (13, 45) = (24, 26) + (23, 25) = (21, 44)$
10. Получатель выполняет расшифровку:
 $C_2 - (d \times C_1) = P + r \times d \times e_1 - d \times r \times e_1 = P$
 $(21, 44) - (4 \times (35, 1)) = (21, 44) + (23, 42) = (24, 26)$
 - $(4 \times (35, 1)) = -(23, 25) = (23, 42)$

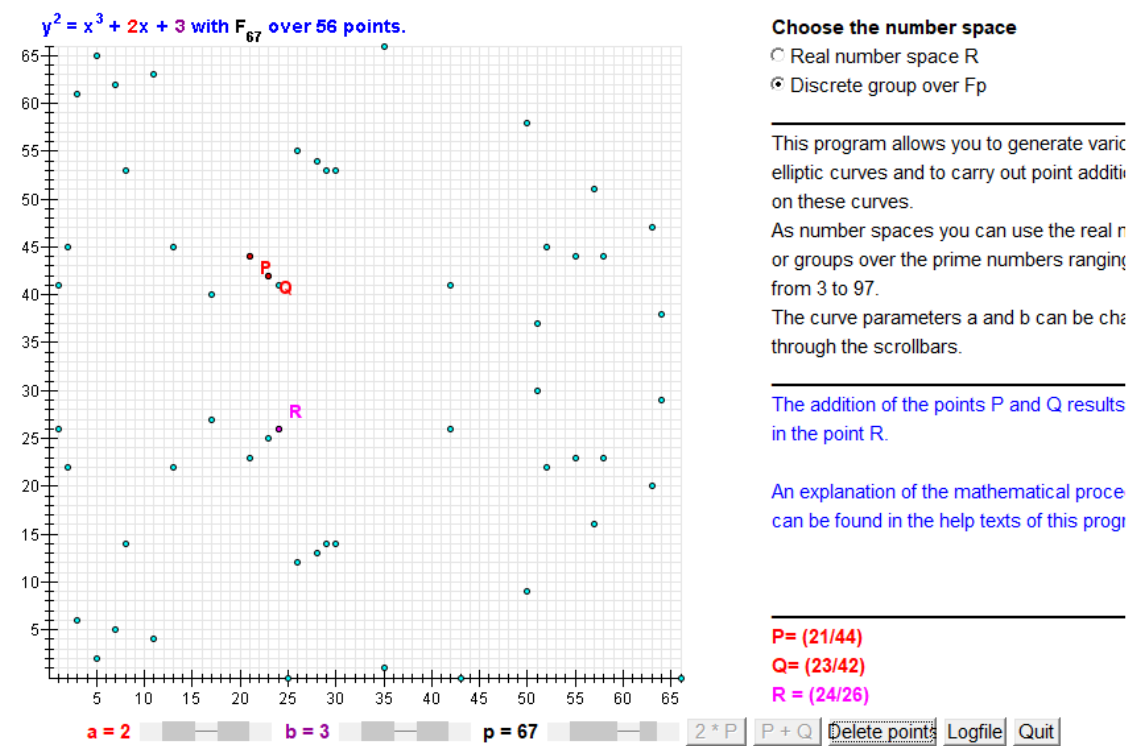
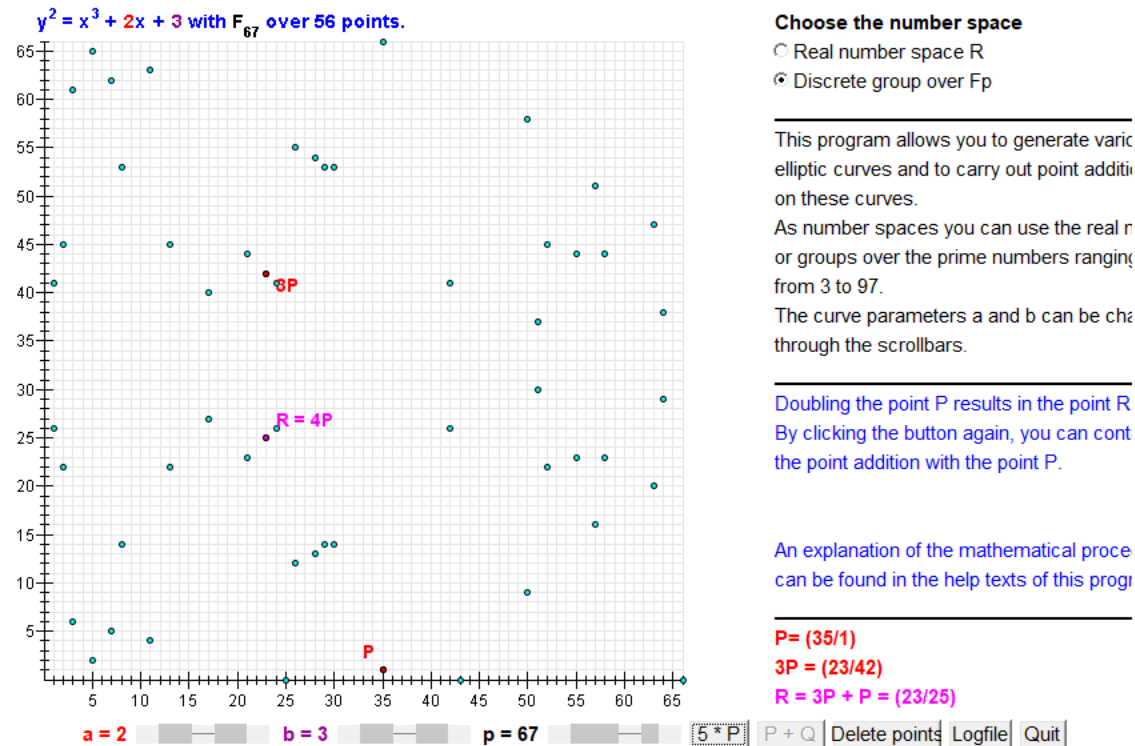
Проверка лекционного материала по ECDSA. Генерация ключа



Проверка лекционного материала по ECDSA. Зашифрование



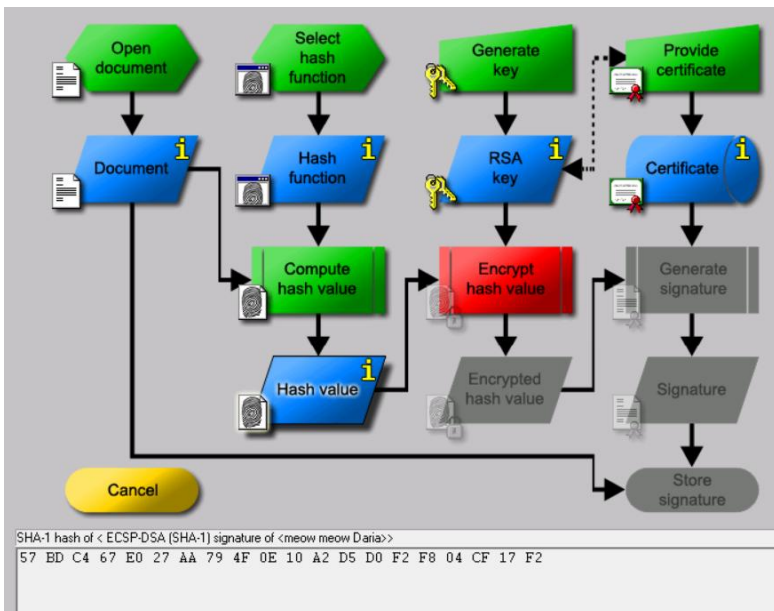
Проверка лекционного материала по ECDSA. Расшифрование



Демонстрация процесса подписи в среде PKI

Демонстрация этапов создания электронной подписи в среде РКИ

Вычисление дайджеста файла



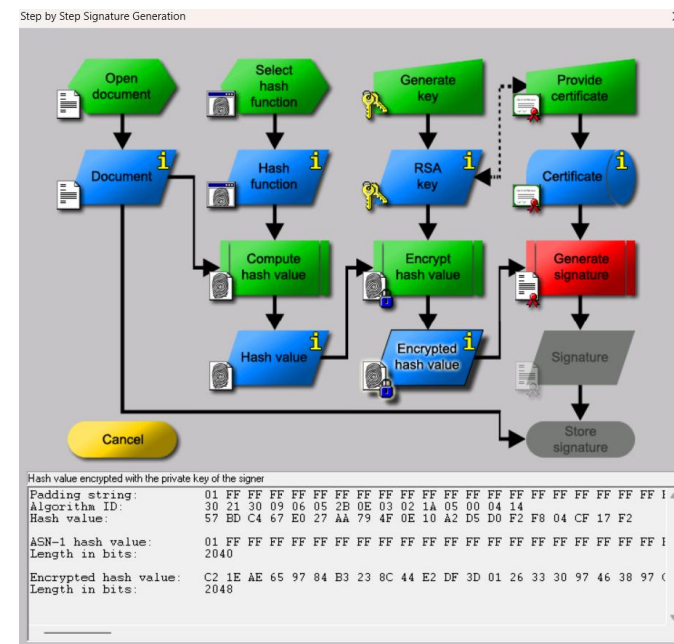
Импортирование сгенерированной ранее ключевой пары RSA-2048

The 'Create Certificate and PSE' dialog box is shown. It contains the following fields and options:

- Public RSA parameter:**
 - Bit length: 2048 bit
 - RSA modulus N: 314989511258995491407470819058197066555357323022733414699175
 - Public key e: 65537
- Personal data for the certificate:**
 - Name: USACHEVA
 - First name: DARIA
 - Key identifier: (optional)
 - PIN: [blank]
 - PIN verification: [blank]
- Generated names for PSE and certificate:**
 - User Key ID: [USACHEVA][DARIA][RSA-2048][1734899715]
 - Distinguished Name: CN=DARIA USACHEVA [1734899715], DC=cryptool, DC=org

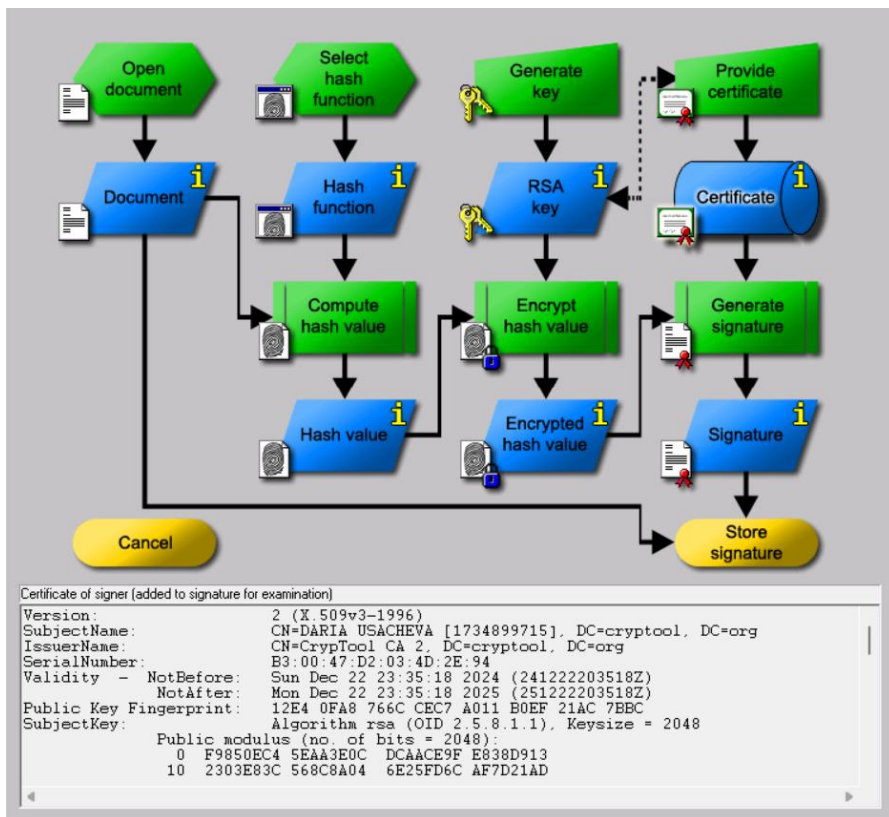
Buttons at the bottom: 'Create Certificate and PSE', 'Import certificate and key', and 'Cancel'.

Шифрование ключа функцией диверсификации

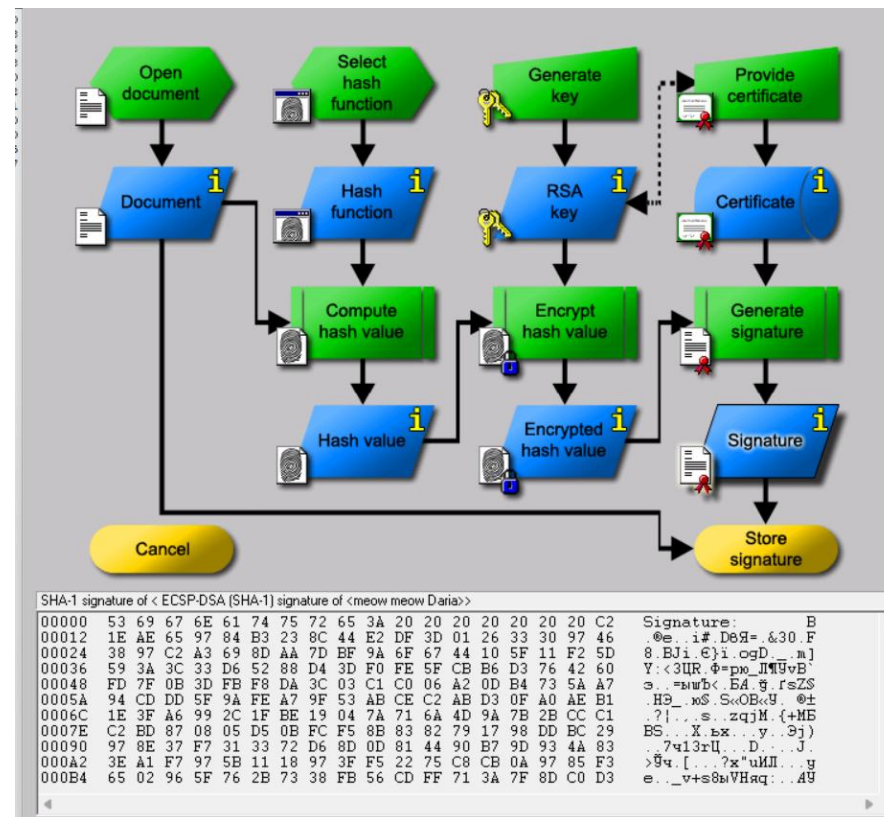


Демонстрация этапов создания электронной подписи в среде РКІ

Сертификат



Создание подписи документа



Структура сертификата

Подписание своего отчета

Заключение