

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

Лабораторная работа № 8

Изучение электронной подписи

Студент: _____

Чернякова Валерия, группа 1304

Руководитель: _____

Племянников А.К., доцент каф. ИБ

Цель работы

Повысить компетенции в работе с асимметричными протоколами и шифрами.

Задачи:

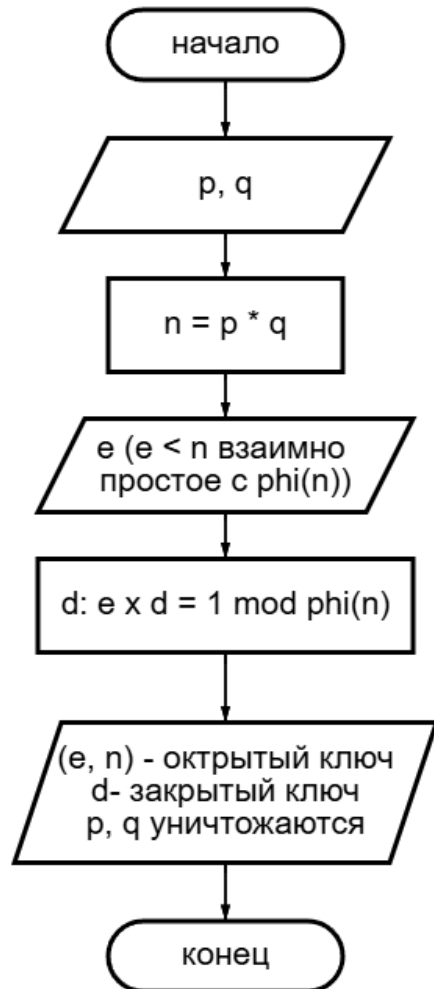
- Изучить генерацию ключевых пар;
- Изучить процесс создания и проверки электронной подписи

Задание

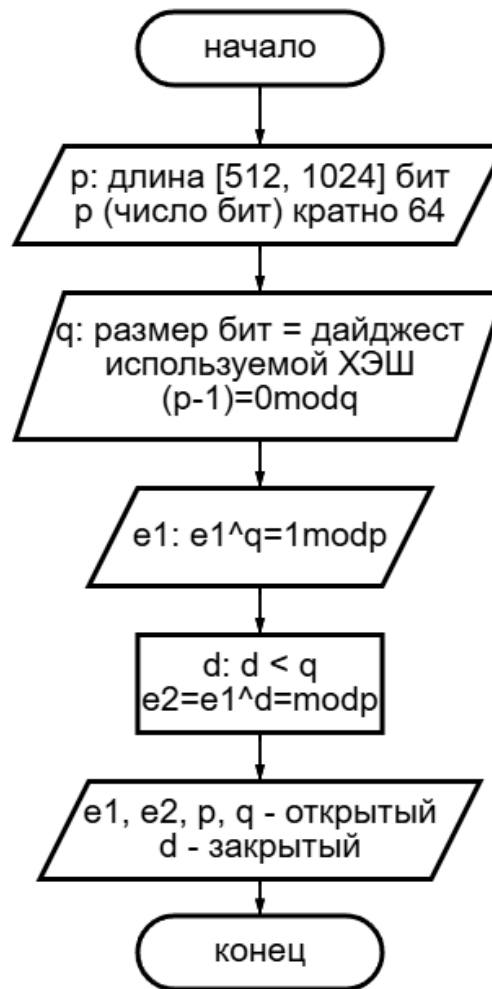
1. Перейти к утилите «Digital Signatures/PKI → PKI/Generate...».
2. Сгенерировать ключевые пары по алгоритмам RSA-2048, DSA-2048, EC-239. Зафиксировать время генерации в таблице.
3. С помощью утилиты «Digital Signatures/PKI → PKI/Display...» вывести сгенерированный открытый ключ и сохранить соответствующий скриншот.

Алгоритм генерации ключевых пар

RSA



DSA



ECDSA



Генерация ключевых пар. RSA

Generation of an 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: Chernyakova

First name: Valeria

Key identifier (optional):

PIN: XXXXX

PIN verification: XXXXX

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

CrypTool

The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[Chernyakova][Valeria][RSA-1024][1733666864]'.

Elapsed time while creating key pair: 1.022 seconds.

OK

Public Parameters of: Valeria Chernyakova

Modulus: 178636806761320471859292538851742342214005153736943291081379878358869241355964997266756741808610558727829932572188941859600436170472428021129076016263372659582638761674275675984695

Exponent: 65537

Base for presentation of numbers
☐ Octal ☒ Decimal ☐ Hexadecimal

Back

Генерация ключевых пар. DSA

Generation of an 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: Chernyakova

First name: Valeria

Key identifier (optional):

PIN: XXXXX

PIN verification: XXXXX

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

CrypTool

The parameters chosen by you and the new key pair have been successfully saved.

The assigned key identifier is '[Chernyakova][Valeria][DSA-1024][1733667071]'.

Elapsed time while creating key pair: 0.238 seconds.

OK

Certificate Data

Version: 2 (X.509v3-1996)

SubjectName: CN=Valeria Chernyakova [1733667071], DC=

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

SerialNumber: 82:70:AE:F4:52:A4:05:9B

Validity - NotBefore: Sun Dec 08 17:11:11 2024 (241208141111Z)

NotAfter: Mon Dec 08 17:11:11 2025 (251208141111Z)

Public Key Fingerprint: 23A0 8D45 6422 52CD 848B 58A5 61F2 B5E9

SubjectKey: Algorithm NIST-DSA (OID 1.3.14.3.2.12),

DSA prime p (no. of bits = 1024):

0 FFD1CEFB 3220F1F1 9A81CE22 63BBC6DD

10 33315BEB C2822134 64C2B280 B76556EF

20 63801FBB 0C996689 17B5BCE8 353C1913

30 9D3B11B6 9ED12FD6 A5F33077 C13BDFD6

40 FF03ADDE 9C523D24 564A5350 C5A959A0

50 C48A7928 DA17AE68 1BDFD137 761DFBC4

60 2C56D1BC 50A94E11 9CF264AB E771428E

70 3060FAFB 0CE9B998 D67B8500 06498BC7

DSA prime q (no. of bits = 160):

Close

Генерация ключевых пар. ECDSA

Generation of an Asymmetric Key Pair

× CrypTool

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:

Chernyakova

First name:

Valeria

Key identifier (optional):

PIN:

PIN verification:

The parameters chosen by you and the new key pair have been successfully saved.

The assigned key identifier is '[Chernyakova][Valeria][EC-prime239v1][1733667127]'.

Elapsed time while creating key pair: 0.010 seconds.

OK

Domain parameters of elliptic curve '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):		

Base for presentation of numbers

☐ Octal

☒ Decimal

☐ Hexadecimal

Generate new key pair...

PKCS #12 Import

Show key pair...

Close

Public Key (Asymmetric)

×

Key owner:

Valeria Chernyakova

Key type:

EC-prime239v1

Date key created:

08.12.2024 17:12:07

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:

x = 269070066235439691230581132778799167444280065264266540853702160361218749

238

y = 748859366878338124498551739275891661625586571986978976878218309222386028

239

Base for presentation of numbers

☐ Octal

☒ Decimal

☐ Hexadecimal

Back

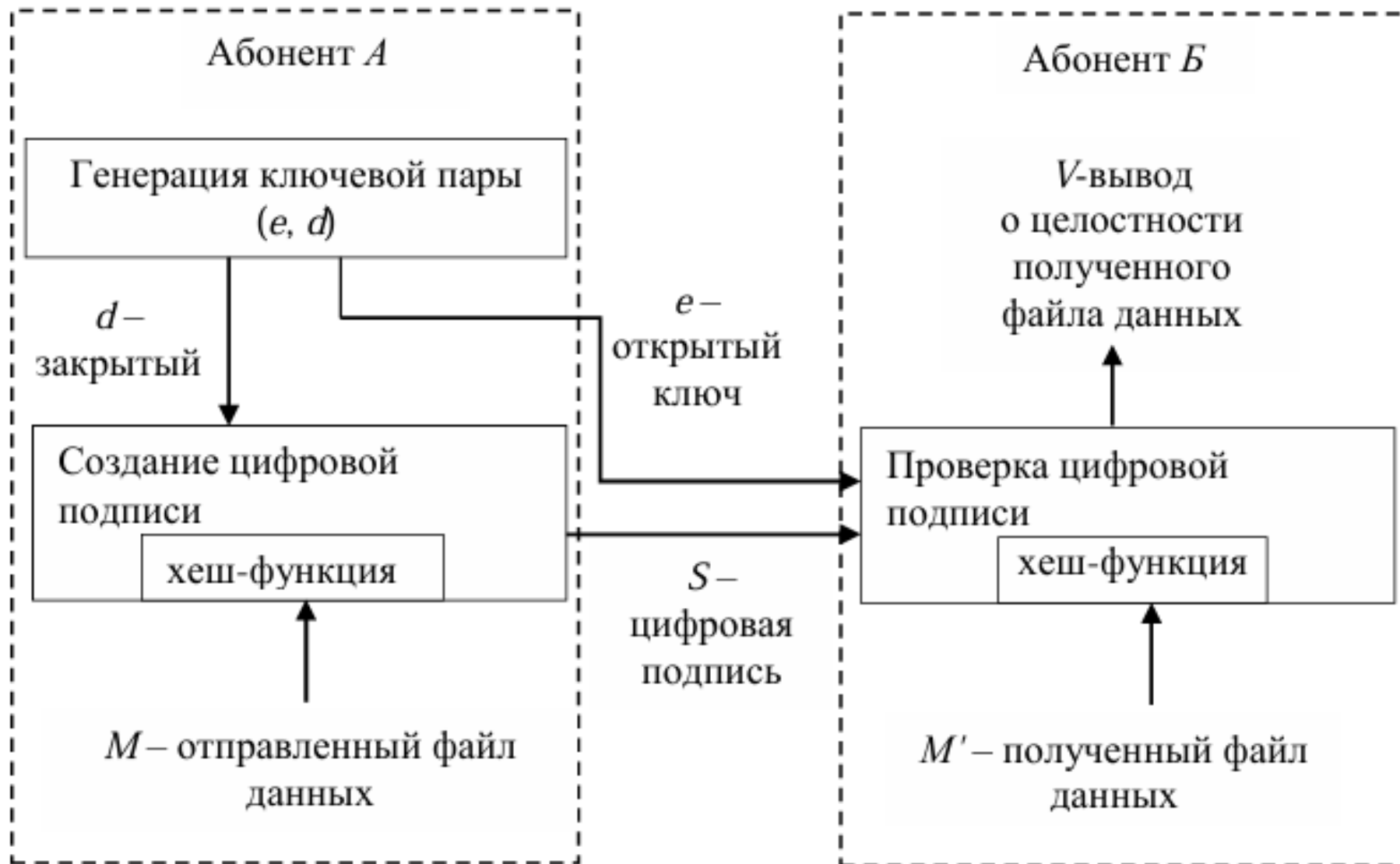
Генерация ключевых пар.

Алгоритм	Время, секунды
RSA-2048	1.022
DSA-2048	0.238
ECDSA-239	0.010


Задание

1. Открыть текст не менее 5000 знаков. Перейти к приложению Digital Signatures/PKI → Sign Document...
2. Задать хеш-функцию и другие параметры электронной подписи.
3. Создать подписи, используя закрытые ключи, сгенерированные в предыдущем задании. Зафиксировать время создания электронной подписи для каждого ключа (опция Display signature time должна быть включена)
4. Сохранить скриншот любой электронной подписи с помощью приложения Digital Signatures/PKI → Extract Signature.
5. Выполнить процедуру проверки любой подписи Digital Signatures/ PKI → Verify Signature для случаев сохранения и нарушения целостности исходного текста. Сохранить скриншоты результатов.


Создание и проверка подписи



Электронная подпись. RSA

**Correct signature!**
Duration of signature verification: 0.000 seconds.

OK

**Signature generation time: 0.000 seconds.**

OK

Signer:Valeria Chernyakova

Used key:RSA-1024; created 08.12.2024 17:07:44


Signature algorithm:RSA with hash function SHA-1

Signature:

00000 F7 CC 37 DD 91 8A 90 D1 89 EF 3A 84 A2 2F 4M73...C.n:..ÿ/
0000E 96 45 BC 8E D6 02 46 44 49 A3 4C 9E BC 3B .Ej.Ц.FDIJL.j;
0001C 25 FD 97 8D 88 8A 42 FB 03 C0 6B 43 E0 6B %e...Bsr.AkCak
0002A 36 25 E8 60 D8 61 1D 18 A5 F9 84 A2 B0 16 6%и'Ша..Гм.ÿ*.
00038 00 8E D5 E2 E9 D1 ED 4C 2A D6 A2 4F 3A 0C ..ХайСнL*ЦÿO:..
00046 1D AF AD 93 4B 42 B8 83 4E E6 EB 5C 9A 17 .İ-.KBë.Nxn\...
00054 02 E8 E0 7A D5 2E C7 99 66 D0 0F ED 32 F3 .iazX.S.fP.n2y
00062 7D 1A D0 D7 D0 20 9A 72 C4 A3 82 E0 23 ED }.P4P.rдJ.a#н

Length of signature: 1024 bits

Options for presentation of signature

Numbers: ☐ Octal ☐ Decimal ☐ Hexadecimal Hex dump (hexadecimal and ASCII): 

Signed message:

00000 54 68 65 20 63 61 74 65 72 69 6E 67 20 69 The catering i
0000E 6E 64 75 73 74 72 79 20 61 6E 64 20 74 68 ndustry and th
0001C 65 20 72 65 73 74 61 75 72 61 6E 74 20 69 e restaurant i
0002A 6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E ndustry are on
00038 20 74 68 65 20 76 65 72 67 65 20 6F 66 20 the verge of
00046 74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61 tremendous tra
00054 6E 73 66 6F 72 6D 61 74 69 6F 6E 73 2C 20 nsformations,
00062 61 73 73 6F 63 69 61 74 65 64 20 70 72 69 associated pri

Length of message: 5615 bytes

Verify

Close

Choose hash function

Algorithm:Output length

☐ MD2128 bits

☐ MD5128 bits

☐ RIPEMD-160160 bits

☐ SHA160 bits

☒ SHA-1160 bits

Choose signature algorithm

Factorization based algorithms

☒ RSA

Discrete logarithm based algorithms

☐ DSA

Elliptic curve based algorithms

☐ ECSP-DSA

☐ ECSP-NR

Presentation format

☐ Affine coordinates

☒ Projective coordinates

00000070ED 32 F3 7D 1A D0 D7 D0 20 9A 72 C4 A3 82 E0 23 .2.)....x....#
00000080ED 25 51 2E 3E AC 05 CF 28 56 26 CC BB 87 7A 05 .%Q.>...(Va....
00000090B0 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000000A020 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000000B020 53 69 67 6E 61 74 75 72 65 20 6C 65 6E 67 74
000000C068 3A 20 20 31 30 32 34 20 20 20 20 20 20 20 20
000000D020 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000000E020 20 20 20 41 6C 67 6F 72 69 74 68 6D 3A 20 20
000000F020 20 20 20 52 53 41 20 20 20 20 20 20 20 20 20
0000010020 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0000011020 20 20 20 48 61 73 68 20 66 75 6E 63 74 69 6F
000001206E 3A 20 20 20 53 48 41 2D 31 20 20 20 20 20 20
0000013020 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0000014020 20 20 20 20 20 4B 65 79 3A 20 20 20 20 20 5B
0000015043 68 65 72 6E 79 61 6B 6F 76 61 5D 5B 56 61 6C
0000016065 72 69 61 5D 5B 52 53 41 2D 31 30 32 34 5D 5B
0000017031 37 33 33 36 36 36 38 36 34 5D 20 20 20 20 20
0000018020 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0000019065 73 73 61 67 65 3A 20 20 20 20 20 20 54 68 65
000001A020 63 61 74 65 72 69 6E 67 20 69 6E 64 75 73 74
000001B072 79 20 61 6E 64 20 74 68 65 20 72 65 73 74 61
000001C075 72 61 6E 74 20 69 6E 64 75 73 74 72 79 20 61
000001D072 65 20 6F 6E 20 74 68 65 20 76 65 72 67 65 20
000001E06F 66 20 74 72 65 6D 65 6E 64 6F 75 73 20 74 72
000001F061 6E 73 66 6F 72 6D 61 74 69 6F 6E 73 2C 20 61
0000020073 73 6F 63 69 61 74 65 64 20 70 72 69 6D 61 72
0000021069 6C 79 20 77 69 74 68 20 74 68 65 20 61 64 76
0000022065 6E 74 20 6F 66 20 6E 65 77 20 66 6F 6F 64 20
0000023070 72 6F 64 75 63 74 69 6F 6E 20 74 65 63 68 6E
0000024061 6E 6F 67 69 65 73 20 61 6E 64 20 69 6E 6E 6F
0000025076 61 74 69 76 65 20 73 6F 6C 75 74 69 6F 6E 73
0000026020 69 6E 20 74 68 65 20 64 65 73 69 67 6E 20 6F
0000027066 20 74 65 63 68 6E 6F 6C 6F 67 69 63 61 6C 20
0000028065 71 75 69 70 6D 65 6E 74 2E 20 52 70 65 61 6B
0000029069 6E 67 20 61 62 6F 75 74 20 74 68 65 20 71 75
000002A061 6C 69 74 79 20 6F 66 20 73 65 72 76 69 63 65
000002B020 70 72 6F 76 69 73 69 6F 6E 20 74 6F 64 61 79
000002C02C 20 66 69 72 73 74 20 6F 66 20 61 6C 6C 2C 20
000002D06F 6F 65 20 73 68 6F 75 6C 64 20 6B 65 65 70 20

Электронная подпись. DSA

Correct signature!
Duration of signature verification: 0.002 seconds.

Signature generation time: 0.000 seconds.

OK

OK

Extracted Signature

Signer: Valeria Chernyakova

Used key: DSA-1024; created 08.12.2024 17:11:11

Signature algorithm: DSA with hash function SHA-1

Signature:

00000	30 2D 02 14 10 3C 37 77 40 53 C4 C0 A9 A7	0-...<7w@SДА@S
0000E	5D 84 98 4E D8 78 1D A2 4B 5A 02 15 00 C8]...Nllx.ŸKZ...И
0001C	B9 EB 38 6F 66 8C 21 1D F2 E7 91 64 63 7C	Мл8of.!.тэ.dcl
0002A	1E 9C 52 0F 64	..R.d

Length of signature: 376 bits

Options for presentation of signature
Numbers: ☐ Octal ☐ Decimal ☐ Hexadecimal ☒ Hex dump (hexadecimal and ASCII):

Signed message:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra
00054	6E 73 66 6F 72 6D 61 74 69 6F 6E 73 2C 20	nsformations,
00062	61 73 73 6F 63 69 61 74 65 64 20 70 72 69	associated pri

Length of message: 5615 bytes

Choose hash function

Algorithm:	Output length
<input type="radio"/> MD2	128 bits
<input type="radio"/> MD5	128 bits

Choose signature algorithm

Factorization based algorithms

☐ RSA


Discrete logarithm based algorithms

☒ DSA


DSA (SHA1) signature of <5000_symbols.txt>

00000000	53 69 67 6E 61 74 75 72 65 3A 20	Signature:
0000000B	20 20 20 20 20 20 30 2D 02 14 10	0-...
00000016	3C 37 77 40 53 C4 C0 A9 A7 5D 84	<7w@S....].
00000021	98 4E D8 78 1D A2 4B 5A 02 15 00	.N.x..KZ...
0000002C	C8 B9 EB 38 6F 66 8C 21 1D F2 E7	...8of.!....
00000037	91 64 63 7C 1E 9C 52 0F 64 20 20	.dcl..R.d
00000042	20 20 20 20 20 20 20 20 20 20 20	
0000004D	20 20 20 20 20 53 69 67 6E 61 74 75	Signature
00000058	72 65 20 6C 65 6E 67 74 68 3A 20	re length:
00000063	20 33 37 36 20 20 20 20 20 20 20	376
0000006E	20 20 20 20 20 20 20 20 20 20 20	
00000079	20 20 20 20 20 20 20 20 20 20 20	
00000084	41 6C 67 6F 72 69 74 68 6D 3A 20	Algorithm:
0000008F	20 20 20 20 20 20 44 53 41 20 20 20	DSA
0000009A	20 20 20 20 20 20 20 20 20 20 20	
000000A5	20 20 20 20 20 20 20 20 20 20 20	
000000B0	20 20 20 20 20 48 61 73 68 20 66 75	Hash fu
000000BB	6E 63 74 69 6F 6E 3A 20 20 20 53	nction: S
000000C6	48 41 2D 31 20 20 20 20 20 20 20	HA-1
000000D1	20 20 20 20 20 20 20 20 20 20 20	
000000DC	20 20 20 20 20 20 20 20 20 4B 65	Ke
000000E7	79 3A 20 20 20 20 20 20 5B 43 68	y: [Ch
000000F2	65 72 6E 79 61 6B 6F 76 61 5D 5B	ernyakova][
000000FD	56 61 6C 65 72 69 61 5D 5B 44 53	Valeria][DS
00000108	41 2D 31 30 32 34 5D 5B 31 37 33	A-1024][173
00000113	33 36 36 37 30 37 31 5D 20 20 20	3667071]
0000011E	20 20 20 20 20 20 20 20 20 20 20	
00000129	20 20 20 20 20 20 20 4D 65 73 73 61	Message: Th
00000134	67 65 3A 20 20 20 20 20 20 54 68	e catering
0000013F	65 20 63 61 74 65 72 69 6E 67 20	industry and
0000014A	69 6E 64 75 73 74 72 79 20 61 6E	d the resta
00000155	64 20 74 68 65 20 72 65 73 74 61	urant indus
00000160	75 72 61 6E 74 20 69 6E 64 75 73	try are on
0000016B	74 72 79 20 61 72 65 20 6F 6E 20	the verge o
00000176	74 68 65 20 76 65 72 67 65 20 6F	f tremendu
00000181	66 20 74 72 65 6D 65 6E 64 6F 75	

Электронная подпись. ECDSA

**Signature generation time: 0.000 seconds.**

OK

**Correct signature!**
Duration of signature verification: 0.002 seconds.

OK

Signer:Valeria Chernyakova

Used key:EC-prime239v1; created 08.12.2024 17:12:07

Signature algorithm:ECSP-DSA with hash function SHA-1

Signature:

```
c = 52085005903166884712392134307815116773826478672099609678159668879479610;  
d = 77173435991932743297975348595679355913618099601259512936755344317248378;
```

Length of signature: 478 bits

Options for presentation of signature:
Numbers: ☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Hex dump (hexadecimal and ASCII):

Signed message:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra
00054	6E 73 66 6F 72 6D 61 74 69 6F 6E 73 2C 20	nsformations,
00062	61 73 73 6F 63 69 61 74 65 64 20 70 72 69	associated pri

Length of message: 5615 bytes

Verify

Close

Choose hash function

Algorithm:	Output length
<input type="radio"/> MD2	128 bits
<input type="radio"/> MD5	128 bits
<input type="radio"/> RIPEMD-160	160 bits
<input type="radio"/> SHA	160 bits
<input checked="" type="radio"/> SHA-1	160 bits

Choose signature algorithm

Factorization based algorithms
☐ RSA

Discrete logarithm based algorithms
☐ DSA

Elliptic curve based algorithms
☒ ECSP-DSA
☐ ECSP-NR

Extracted Signature

Signer:Valeria Chernyakova
Used key:EC-prime239v1; created 08.12.2024 17:12:07
Signature algorithm:ECSP-DSA with hash function SHA-1
Signature:

```
c = 52085005903166884712392134307815116773826478672099609678159668879479610;  
d = 77173435991932743297975348595679355913618099601259512936755344317248378;
```

Length of signature: 478 bits

Options for presentation of signature:
Numbers: ☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Hex dump (hexadecimal and ASCII):

Signed message:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra
00054	6E 73 66 6F 72 6D 61 74 69 6F 6E 73 2C 20	nsformations,
00062	61 73 73 6F 63 69 61 74 65 64 20 70 72 69	associated pri

Length of message: 5615 bytes

Verify

Close

Электронная подпись.

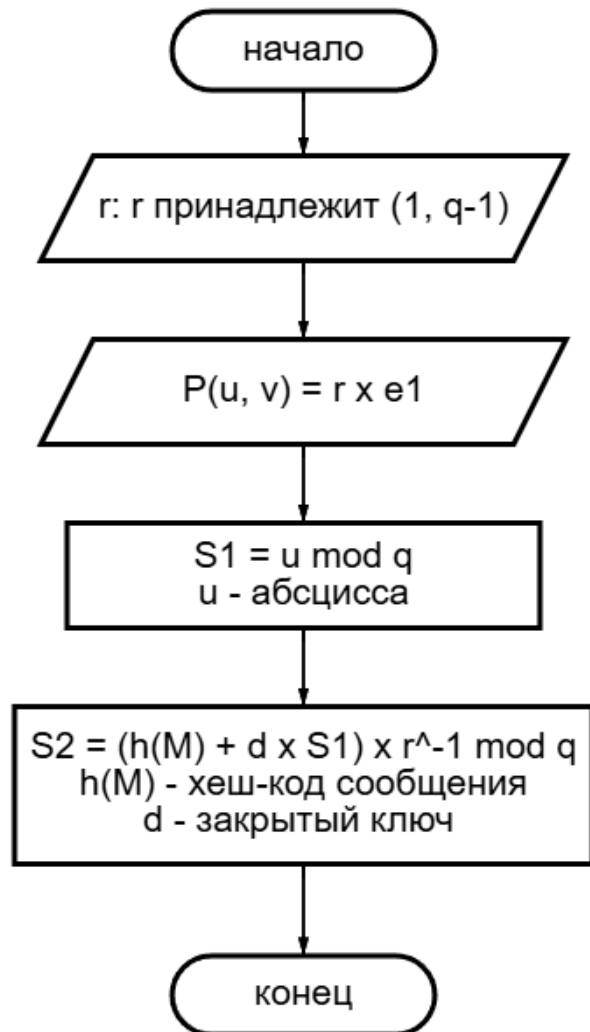
Алгоритм	Время, секунды
RSA-2048	0.000
DSA-2048	0.002
ECDSA-239	0.002

Задание

1. Выполнить процедуру создания подписи Digital Signatures/PKI → Sign Document... алгоритмом ECSP-DSA в пошаговом режиме (Display inter. results = ON). Зафиксировать скриншоты последовательности шагов.
2. Выполнить процедуру проверки подписи ECSP-DSA для случаев сохранения и нарушения целостности исходного текста. Сохранить скриншоты результатов.
3. Проверить лекционный материал по ECDSA, создав и проверив подпись сообщения M (принять $M = h(M)$) приложением Indiv.Procedures → Number Theory... → Point Addition on EC.

Алгоритм формирования и проверки подписи ECDSA

Формирование



Подписание



Выполнение ECDSA. Создание подписи

Signature Generation - Step By Step

Message M to be signed:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra
00054	6E 73 66 6F 72 6D 61 74 69 6F 6E 73 2C 20	nsformations,
00062	61 73 73 6F 63 69 61 74 65 64 20 70 72 69	associated pri

Step-by-step signature generation:

Signature originator: Valeria Chernyakova

Domain parameters to be used 'EC-prime239v1':

a = 8834235323891921647916487503603088853144765972529603627924508;
b = 7385252174069924173485960880387817241648609717970989718912404;
Gx = 1102820037495488564763485335411862045779050615048812422401495;
Gy = 8690784074355093787473518737930588685002103849460406946513687;
k = 1
r = 8834235323891921647916487503603088848075503416916277522753454;

Secret key s of the signature originator:

s = 8316803642024931035992173469288214479292721767258821696718389'

Step 0 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

Signature Generation - Step By Step

Message M to be signed:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra
00054	6E 73 66 6F 72 6D 61 74 69 6F 6E 73 2C 20	nsformations,
00062	61 73 73 6F 63 69 61 74 65 64 20 70 72 69	associated pri

Step-by-step signature generation:

s = 8316803642024931035992173469288214479292721767258821696718389'

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

Size of message M to be signed: 5615 bytes

Continue ...

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

f = 741538877857563602099040643932266114445834453853

Continue ...

Step 1 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

Выполнение ECDSA. Создание подписи

Signature Generation - Step By Step

Message M to be signed:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra
00054	6E	73	66	6F	72	6D	61	74	69	6F	6E	73	2C	20	nsformations,
00062	61	73	73	6F	63	69	61	74	65	64	20	70	72	69	associated pri

Step-by-step signature generation:

$f = 741538877857563602099040643932266114445834453853$

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 elliptic curve

$u = 43059259079578474120401365114774130937887802502695161694020308$
 $V_x = 4235290420475586463578988904442293026617250849506886203436038$
 $V_y = 3651185061107279205474805426831909043006236194378266460635278$

Continue ...

Step 2 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

Signature Generation - Step By Step

Message M to be signed:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra
00054	6E	73	66	6F	72	6D	61	74	69	6F	6E	73	2C	20	nsformations,
00062	61	73	73	6F	63	69	61	74	65	64	20	70	72	69	associated pri

Step-by-step signature generation:

with the domain parameters of 'EC-prime239v1' (V=(Vx,Vy) is a point on the elliptic curve

$u = 43059259079578474120401365114774130937887802502695161694020308$
 $V_x = 4235290420475586463578988904442293026617250849506886203436038$
 $V_y = 3651185061107279205474805426831909043006236194378266460635278$

Continue ...

Convert the group element Vx (x co-ordinates of point V on elliptic curve) to an integer

$i = 4235290420475586463578988904442293026617250849506886203436038$

Continue ...

Step 3 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

Выполнение ECDSA. Создание подписи

Signature Generation - Step By Step

Message M to be signed:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra
00054	6E	73	66	6F	72	6D	61	74	69	6F	6E	73	2C	20	nsformations,
00062	61	73	73	6F	63	69	61	74	65	64	20	70	72	69	associated pri

Step-by-step signature generation:

Continue ...

Convert the group element V_x (x co-ordinates of point V on elliptic curve) to integer i :

$i = 4235290420475586463578988904442293026617250849506886203436038$

Continue ...

Calculate the number $c = i \bmod r$ (c not equal to 0):

$c = 4235290420475586463578988904442293026617250849506886203436038$

Continue ...

Step 4 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

Signature Generation - Step By Step

Message M to be signed:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra
00054	6E	73	66	6F	72	6D	61	74	69	6F	6E	73	2C	20	nsformations,
00062	61	73	73	6F	63	69	61	74	65	64	20	70	72	69	associated pri

Step-by-step signature generation:

Continue ...

Calculate the number $c = i \bmod r$ (c not equal to 0):

$c = 4235290420475586463578988904442293026617250849506886203436038$

Continue ...

Calculate the number $d = u^{(-1)} * (f + s * c) \bmod r$ (d not equal to 0):

$d = 6599326242878186008268722183783724421360711753308363804401221$

Continue ...

Step 5 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

Выполнение ECDSA. Создание подписи

Signature Generation - Step By Step

Message M to be signed:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra
00054	6E	73	66	6F	72	6D	61	74	69	6F	6E	73	2C	20	nsformations,
00062	61	73	73	6F	63	69	61	74	65	64	20	70	72	69	associated pri

Step-by-step signature generation:

Calculate the number $c = i \bmod r$ (c not equal to 0):
 $c = 4235290420475586463578988904442293026617250849506886203436038:$
Continue ...

Calculate the number $d = u^{(-1)} * (f + s * c) \bmod r$ (d not equal to 0):
 $d = 6599326242878186008268722183783724421360711753308363804401221:$
Continue ...

Signature generation finished.
The signature consists of the two numbers c and d.

Step 6 out of a maximum of 6 steps.

Output signature data

Cancel

Continue >

ECSP-DSA (SHA-1) signature of <5000_symbols.txt>

00000150	6E	3A	20	20	20	53	48	41	2D	31	20	20	20	20	n: SH
0000015E	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0000016C	20	20	20	20	20	20	20	20	20	4B	65	79	3A	20	
0000017A	20	20	20	20	20	5B	43	68	65	72	6E	79	61	6B	[C
00000188	6F	76	61	5D	5B	56	61	6C	65	72	69	61	5D	5B	oval[Va
00000196	45	43	2D	70	72	69	6D	65	32	33	39	76	31	5D	EC-prim
000001A4	5B	31	37	33	33	36	36	37	31	32	37	5D	20	20	[173366
000001B2	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
000001C0	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
000001CE	20	4D	65	73	73	61	67	65	3A	20	20	20	20	20	Message
000001DC	20	54	68	65	20	63	61	74	65	72	69	6E	67	20	The ca
000001EA	69	6E	64	75	73	74	72	79	20	61	6E	64	20	74	industr
000001F8	68	65	20	72	65	73	74	61	75	72	61	6E	74	20	he rest
00000206	69	6E	64	75	73	74	72	79	20	61	72	65	20	6F	industr
00000214	6E	20	74	68	65	20	76	65	72	67	65	20	6F	66	n the v
00000222	20	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	tremen
00000230	61	6E	73	66	6F	72	6D	61	74	69	6F	6E	73	2C	ansform
0000023E	20	61	73	73	6F	63	69	61	74	65	64	20	70	72	associ
0000024C	69	6D	61	72	69	6C	79	20	77	69	74	68	20	74	imarily
0000025A	68	65	20	61	64	76	65	6E	74	20	6F	66	20	6E	he adve
00000268	65	77	20	66	6F	6F	64	20	70	72	6F	64	75	63	ew food
00000276	74	69	6F	6E	20	74	65	63	68	6E	6F	6C	6F	67	tion te
00000284	69	65	73	20	61	6E	64	20	69	6E	6E	6F	76	61	ies and
00000292	74	69	76	65	20	73	6F	6C	75	74	69	6F	6E	73	tive so
000002A0	20	69	6E	20	74	68	65	20	64	65	73	69	67	6E	in the
000002AE	20	6F	66	20	74	65	63	68	6E	6F	6C	6F	67	69	of tec
000002BC	63	61	6C	20	65	71	75	69	70	6D	65	6E	74	2E	cal equ
000002CA	20	53	70	65	61	6B	69	6E	67	20	61	62	6F	75	Speaki
000002D8	74	20	74	68	65	20	71	75	61	6C	69	74	79	20	t the q
000002E6	6F	66	20	73	65	72	76	69	63	65	20	70	72	6F	of serv
000002F4	76	69	73	69	6F	6E	20	74	6F	64	61	79	2C	20	vision
00000302	66	69	72	73	74	20	6F	66	20	61	6C	6C	2C	20	first o
00000310	6F	6E	65	20	73	68	6F	75	6C	64	20	6B	65	65	one shc
0000031E	70	20	69	6E	20	6D	69	6E	64	20	63	6C	65	61	p in mi
0000032C	72	2C	20	75	6E	64	65	72	73	74	61	6E	64	61	r, unde
0000033A	62	6C	65	2C	20	74	72	61	6E	73	70	61	72	65	ble, tr

Выполнение ECDSA. Проверка подписи

Signature Verification - Step By Step

Signed message:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'
d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

Signature originator: Valeria Chernyakova

Domain parameters to be used 'EC-prime239v1':

a = 88342353238919216479164875036030888531447659725296036279245081
b = 7385252174069924173485960880387817241648609717970989718912404:
Gx = 1102820037495488564763485335411862045779050615048812422401495:
Gy = 8690784074355093787473518737930588685002103849460406946513687:
k = 1
r = 8834235323891921647916487503603088848075503416916277522753454:

Step 0 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

Signature Verification - Step By Step

Signed message:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'
d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

Bit length of c + bit length of d = 474 bits

Continue ...

Calculate a 'hash value' f (message representative) from message M, 1

f = 741538877857563602099040643932266114445834453853

Continue ...

Step 1 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

Выполнение ECDSA. Проверка подписи

Signature Verification - Step By Step

Signed message:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'

d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

c and d fall within the required interval $[1, r-1]$.

Continue ...

Calculate the number $h = d^{(-1)} \bmod r$:

h = 3413213073754882572536149560753928734292351563362405799711476'

Continue ...

Step 3 out of a maximum of 10 steps.

End dialog Cancel Continue >

Signature Verification - Step By Step

Signed message:

00000	54	68	65	20	63	61	74	65	72	69	6E	67	20	69	The catering i
0000E	6E	64	75	73	74	72	79	20	61	6E	64	20	74	68	ndustry and th
0001C	65	20	72	65	73	74	61	75	72	61	6E	74	20	69	e restaurant i
0002A	6E	64	75	73	74	72	79	20	61	72	65	20	6F	6E	ndustry are on
00038	20	74	68	65	20	76	65	72	67	65	20	6F	66	20	the verge of
00046	74	72	65	6D	65	6E	64	6F	75	73	20	74	72	61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'

d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

f = 741538877857563602099040643932266114445834453853

Continue ...

If c or d does not fall within the interval $[1, r-1]$ then the signature is invalid.
c and d fall within the required interval $[1, r-1]$.

Continue ...

Step 2 out of a maximum of 10 steps.

End dialog Cancel Continue >

Выполнение ECDSA. Проверка подписи

Signature Verification - Step By Step

Signed message:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'
d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

h1 = 7176661840243318160190629791224466448928689494250475139487141!
Continue ...
Calculate the number h2 = c*h mod r:
h2 = 7501409784741656795097477592053620016319852746922705363749305!
Continue ...

Step 5 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

Signature Verification - Step By Step

Signed message:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'
d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

h = 3413213073754882572536149560753928734292351563362405799711476'
Continue ...
Calculate the number h1 = f*h mod r:
h1 = 7176661840243318160190629791224466448928689494250475139487141!
Continue ...

Step 4 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

Выполнение ECDSA. Проверка подписи

Signature Verification - Step By Step

Signed message:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'
d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

Py = 1430979997554930505255706023961040987257167661430934812035537;
Continue ...
Convert the group element Px (x co-ordinates of point P on elliptic curve)
i = 3599490696855950185443208968463515975167257083945013296284053;
Continue ...

Step 7 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

Signature Verification - Step By Step

Signed message:

00000	54 68 65 20 63 61 74 65 72 69 6E 67 20 69	The catering i
0000E	6E 64 75 73 74 72 79 20 61 6E 64 20 74 68	ndustry and th
0001C	65 20 72 65 73 74 61 75 72 61 6E 74 20 69	e restaurant i
0002A	6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E	ndustry are on
00038	20 74 68 65 20 76 65 72 67 65 20 6F 66 20	the verge of
00046	74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61	tremendous tra

Signature:

c = 3599490696855950185443208968463515975167257083945013296284053982'
d = 8401792538568924708309320484205641758174657425332912990628114488'

Base for presentation of signature
☐ Octal ☒ Decimal ☐ Hexadecimal ☐ Octets

Step-by-step signature verification:

Continue ...
Calculate the elliptic curve point $P = h_1 G + h_2 W$
(If $P = (P_x, P_y) = (\text{inf}, \text{inf})$ then the signature is invalid):
 $P_x = 3599490696855950185443208968463515975167257083945013296284053$
 $P_y = 1430979997554930505255706023961040987257167661430934812035537$
Continue ...

Step 6 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

Выполнение ECDSA. Проверка подписи

Signature Verification - Step By Step

Signed message:

```
00000 54 68 65 20 63 61 74 65 72 69 6E 67 20 69 The
0000E 6E 64 75 73 74 72 79 20 61 6E 64 20 74 68 ndus
0001C 65 20 72 65 73 74 61 75 72 61 6E 74 20 69 e re
0002A 6E 64 75 73 74 72 79 20 61 72 65 20 6F 6E ndus
00038 20 74 68 65 20 76 65 72 67 65 20 6F 66 20 the
00046 74 72 65 6D 65 6E 64 6F 75 73 20 74 72 61 trem
```

Signature:

```
c = 359949069685595018544320896846351597516725708394501
d = 8401792538568924708309320484205641758174657425332912990628114488'
```

Step-by-step signature verification:

```
i = 3599490696855950185443208968463515975167257083945013296284053'
Continue ...
Calculate the number  $c' = i \bmod r$ :
c' = 3599490696855950185443208968463515975167257083945013296284053'
Continue ...
```

Step 8 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

CrypTool



Correct signature!
Duration of signature verification: 87.372 seconds.

OK



Invalid signature!
Duration of signature verification: 0.002 seconds.

OK

Signature Verification - Step By Step

```
20 63 61 74 65 72 69 6E 67 20 69 The catering i
73 74 72 79 20 61 6E 64 20 74 68 ndustry and th
65 73 74 61 75 72 61 6E 74 20 69 e restaurant i
73 74 72 79 20 61 72 65 20 6F 6E ndustry are on
65 20 76 65 72 67 65 20 6F 66 20 the verge of
6D 65 6E 64 6F 75 73 20 74 72 61 tremendous tra
```

```
55950185443208968463515975167257083945013296284053982'
```

```
d = 8401792538568924708309320484205641758174657425332912990628114488'
```

Step-by-step signature verification:

```
Continue ...
Calculate the number  $c' = i \bmod r$ :
c' = 3599490696855950185443208968463515975167257083945013296284053'
Continue ...
If  $c' = c$  then the signature is correct; otherwise the signature is :
```

Step 9 out of a maximum of 10 steps.

End dialog

Cancel

Continue >

ECDSA. Проверка лекционного материала

Задание

1. Запустить демонстрационную утилиту «Digital Signatures/PKI → Signature Demonstration...».
2. Получить сертификат ключа проверки электронной подписи (открытого ключа) на ранее сгенерированную ключевую пару RSA-2048.
3. Выполнить и сохранить скриншоты всех этапов создания электронной подписи документа.
4. Сохранить скриншот полученного сертификата ключа проверки этой электронной подписи.

Структура сертификата

Version: 2 (X.509v3-1996)
SubjectName: CN=Valeria Chernyakova [1733672135],
DC=cryptool, DC=org
IssuerName: CN=CrypTool CA 2, DC=cryptool, DC=org
SerialNumber: 53:D1:67:35:20:3F:6D:34
Validity - NotBefore: Sun Dec 08 18:35:36 2024
(241208153536Z)
NotAfter: Mon Dec 08 18:35:36 2025
(251208153536Z)
Public Key Fingerprint: 1FCB 9830 4E82 25D0 3F82 0FFC 90C4
F268
SubjectKey: Algorithm rsa (OID 2.5.8.1.1), Keysize
= 2048

Public modulus (no. of bits = 2048):

```
0 FEB68903 F37A94B2 BEAF0079 8EE249DA
10 1C06BC96 57EABA65 671A9B03 67865E31
20 D12FFD0D 9B92EEAF C263B485 C6D04A5D
30 4C665FB9 9F53DB9C CF9DD475 D43EA44F
40 E9EBB00A 34C245E0 4BB78FF2 2C4F0634
50 679B6538 6D12AE9D E6042DCC 10B67DF3
60 542AF980 21E0C12A C8C984B8 292B65F4
70 52AB78C2 4E3F2301 3C40FB30 E44EAE1F
80 831D0890 08BC3F1B 346C491F 84D68EB0
90 9B911A3E BC7A96AA 51D84A5A 2FE8BE5F
A0 E31E243B 262F68AD B452D35D C69E2773
B0 9ED9A846 D2F95FE9 83BFB577 EFEE1616
C0 2576BE63 2EBDA44F 04FEA909 E29725BF
D0 4358B881 666E70CC 27FEEC0D 0A3051CF
E0 3AFD4FC7 B818B855 60BF8923 71433885
F0 04C2853C 60A12CCC 43D005AB 01439581
```

Public exponent (no. of bits = 17):

```
0 010001
```

Certificate extensions:

Private extensions:

OID 2.206.5.4.3.2:

PrintableString:

```
| [Chernyakova] [Valeria] [RSA-2048] |
| [1733672135] |
```

SHA1 digest of DER code of ToBeSigned:

```
0 0A1FC787 0FCD9741 83E13F4A F18CFCD1
10 EC832924
```

Signature:

Algorithm sha1WithRSASignature (OID

1.3.14.3.2.29), NULL

```
0 8E55412D A10C30BC 3C8F717F E5FBF1A9
10 5BB9B8DC 7B1B2005 EDCF0B5A 856754F1
20 184FB9DF 08F03E90 4840022A 9F104C5A
30 C49ADF24 5FE2676D 2265DCFB EA5BCB39
40 9CE0C192 C91714EF 94F8127A 7A24623E
50 4CB46B1B CBACA786 11E29428 12DC5095
60 E1EDA1E5 9D0AB379 966838D4 A6A815B0
70 87E402D6 FC9ACB5E F096C1B9 A80B062A
80 1C756DCF 35980636 D00BF2F7 B94D005F
90 2B7CB995 26DA7733 FC64EA59 31299DCE
A0 AE938223 CB1E9F16 941EE5F3 C8D88900
B0 DB24F21F E73C662B 8DD04577 CBD420E8
C0 70E3EAB9 721FCC6E F1222478 ACEAC887
D0 2A5BF430 FB9F308C 5C890F08 04EA2D1D
E0 137F5052 C0681CA1 E35D773E 9ABF7BDE
F0 B730A35F D85FA4D2 625C7794 BCD7504F
```

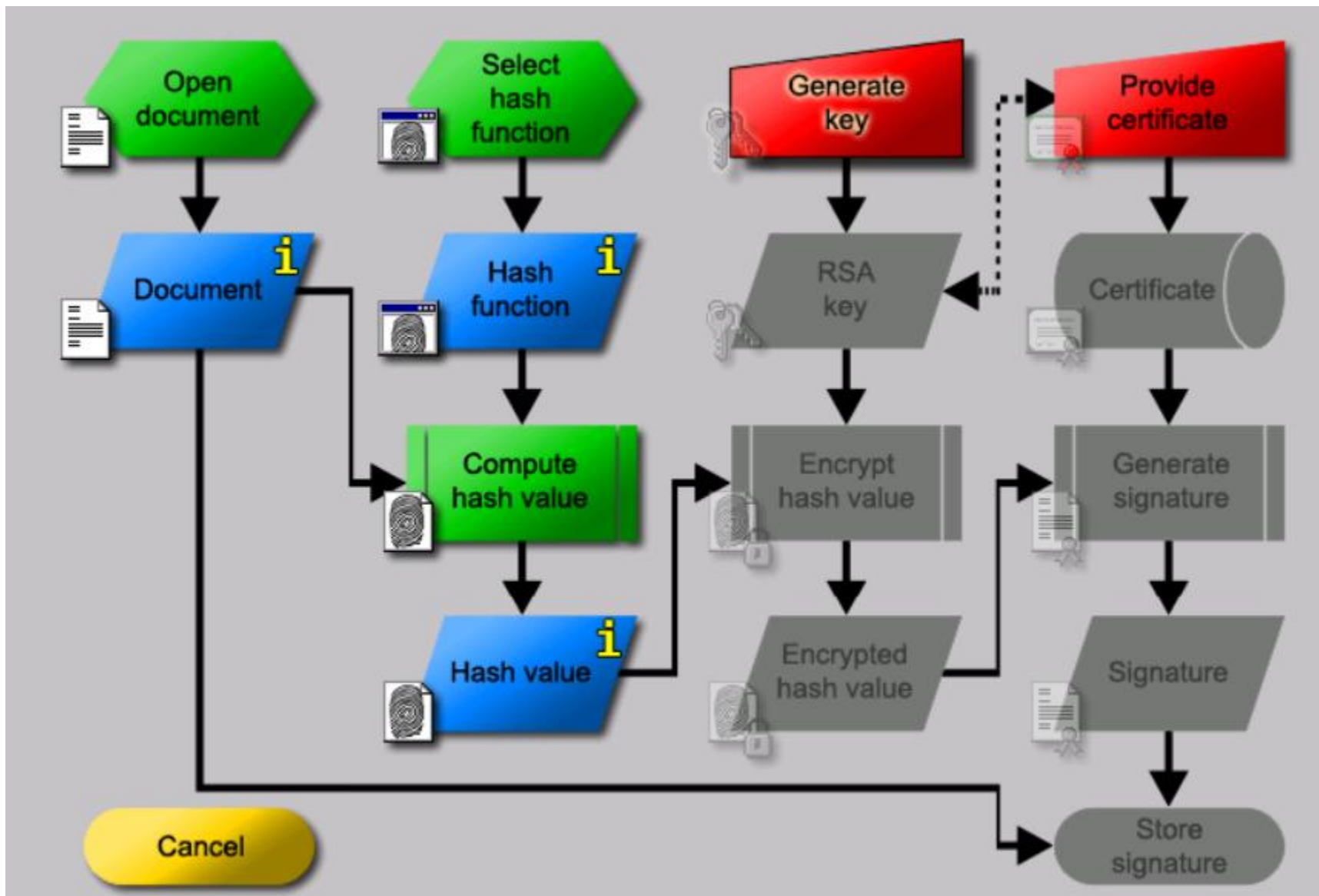
Certificate Fingerprint (MD5):

4C:A7:E6:87:02:7A:8F:85:32:33:2F:62:3D:E2:38:24

Certificate Fingerprint (SHA-1): 6A48 91E9 C751 76A2 D93C 8A87 205C

2BEE 6848 1D35

Схема процедуры подписания



Задание

1. Сконвертировать отчет в формат pdf.
2. Экспортировать ранее созданный сертификат ключевой пары RSA Digital Signatures/PKI → PKI/Generate... → Export PSE(#PKCS12).
3. Открыть pdf-версию отчета и попытаться подписать с использованием этого сертификата.
4. Создать собственный самоподписанный сертификат в среде Adobe Reader и использовать его для подписи отчета.
5. Сохранить скриншоты свойств подписи и сертификата.
6. Внести изменения (маркеры, комментарии) в отчет и проверить подпись.

Заключение

- Исследован протокол согласования ключей Диффи-Хеллмана. Рассмотрена и проведена атака протокола "посредником" для случая, когда только одна уполномоченная сторона создает параметры открытого ключа. Были получены одинаковые значения ключа для стороны отправителя и посредника, а также посредника и получателя.
- Исследован алгоритм асимметричного шифрования RSA. Средствами CrypTool2 была составлена схема атаки коротким сообщением. Атака успешно сработала, были найдены верные значения исходного текста и его зашифрованного.
- Исследован протокол асимметричного шифрования RSA. Средствами CrypTool2 была составлена схема атаки протокола «посредником». Атака успешно сработала, значение зашифрованного текста, найденного посредником, совпала с тем, что было у получателя.
- Изучена атака факторизацией модуля на шифр RSA. Она заключается в разложении модуля n на простые множители p и q , что позволяет вычислить приватный ключ и взломать шифр.
- Была проведена атака на гибридную систему, основанная на том, что злоумышленник перехватывает цифровой конверт с зашифрованным сообщением и зашифрованным секретным ключом. Модифицируя полученные данные и анализируя ответы сервера, можно побитово восстановить целиком секретный ключ.