باسمه تعالی

سارا برادران

تکلیف سری ششم رمزنگاری

9624193

Question 1)

$a = 6 = (110)_2 = d_2d_1d_0$, $B = (5, 9)$

We must compute aB :

step

#0 p = 1 p → initial setting p = (5, 9)

$d_1 = 1$

#1a $p + p = 2p = (10)_2$ p → double

$S = (3 * 5^2 + 1) . 18^{-1} \text{ mod } 11 = 76 * 18^9 \text{ mod } 11 = 10 * 7^9 \text{ mod } 11 = 10 * 5^4 * 7 \text{ mod } 11 = 9 * 10 * 7 \text{ mod } 11 = 3$

$X' = S^2 – X1 – X2 \text{ mod } p = 9 – 5 – 5 \text{ mod } 11 = 10$

$Y' = S(X1 – X') – y1 \text{ mod } 11 = 3(5 – 10) – 9 \text{ mod } 11 = 9$ → 2p = (10, 9)

#2b $2p + p = 3p = (11)_2$ p → add

$S = (9 – 9) . (5 – 10)^{-1} \text{ mod } 11 = 0$

$X' = S^2 – X1 – X2 \text{ mod } p = 0 – 5 – 10 \text{ mod } 11 = 7$

$Y' = S(X1 – X') – y1 \text{ mod } 11 = 0(5 – 7) – 9 \text{ mod } 11 = 2$ → 3p = (7, 2)

$d_0 = 1$

#3a $3p + 3p = 6p = (110)_2$ p → double

$S = (3 * 7^2 + 1) . 4^{-1} \text{ mod } 11 = 5 * 4^9 \text{ mod } 11 = 5 * 5^4 * 4 \text{ mod } 11 = 5 * 9 * 4 \text{ mod } 11 = 4$

$X' = S^2 – X1 – X2 \text{ mod } p = 16 – 7 – 7 \text{ mod } 11 = 2$

$Y' = S(X1 – X') – y1 \text{ mod } 11 = 4(7 – 2) – 2 \text{ mod } 11 = 7$ → 6p = (2, 7)

#3b → No add

Session key = (2, 7)

Question 2)

$$y^2 = x^3 + 2x + 2 \mod 17$$

2.1

Elliptic curve equation : $y^2 = x^3 + ax + b \mod p \rightarrow a = 2 , b = 2 , p = 17$

$4a^3 + 27b^2 \mod p \neq 0 \rightarrow 4 (2)^3 + 27(2)^2 \mod 17 = 15 + 6 \mod 17 = 4 \neq 0$

2.2

(2, 7) + (5, 2) = (x' , y')

$M = \frac{y2-y1}{x2-x1} = \frac{2-7}{5-2} \mod 17 = 12 . 3^{-1} \mod 17 = 12 . 3^{15} \mod 17 = 12 . (3^5)^3 \mod 17 =$

$12 . 5^3 \mod 17 = 4 = s$

$X' = s^2 - x1 - x2 \mod p = 16 - 2 - 5 \mod 17 = 9$

$Y' = s(x1 - x') - y1 \mod p = 4(2 - 9) - 7 \mod 17 = 16$

(x' , y') = (9, 16)

2.3

Hasse's theorem :

$P + 1 - 2\sqrt{p} \leq \#E \leq P + 1 + 2\sqrt{p}$

$\#E = 19 , p = 17 \rightarrow 17 + 1 - 2\sqrt{17} = 9.75 , \ 17 + 1 + 2\sqrt{17} = 26.24$

$9.75 \leq 19 \leq 26.24$ true

2.4

Because #E = 19 is a prime number and If we have a cyclic group with |G| elements where |G| is a prime number then all the members of this group are primitive elements (generators) .

Question 3)

P = 31 , $\alpha = 3$ *and* $\beta = 6$

3.1

Received message = x = 10

First signature = (17, 5) → r = 17, s = 5

t = $\beta^r . r^s$ mod p = $6^{17} . 17^5$ mod 31 = 26.26 mod 31 = 25 , α^x mod p = 3^{10} mod 31 = 25 signature is valid

second signature = (13, 5) → r = 13, s = 5

t = $\beta^r . r^s$ mod p = $6^{13} . 13^5$ mod 31 = 6.6 mod 31 = 5 , α^x mod p = 3^{31} mod 31 = 25 signature is not valid

3.2

there is only one signature for every KE which select from {0, 1, … , p – 2}

t = $\beta^r . r^s$ mod p = α^x mod p

(α^d)^r . (α^{kE})^s = $\alpha^{dr + skE}$ mod p

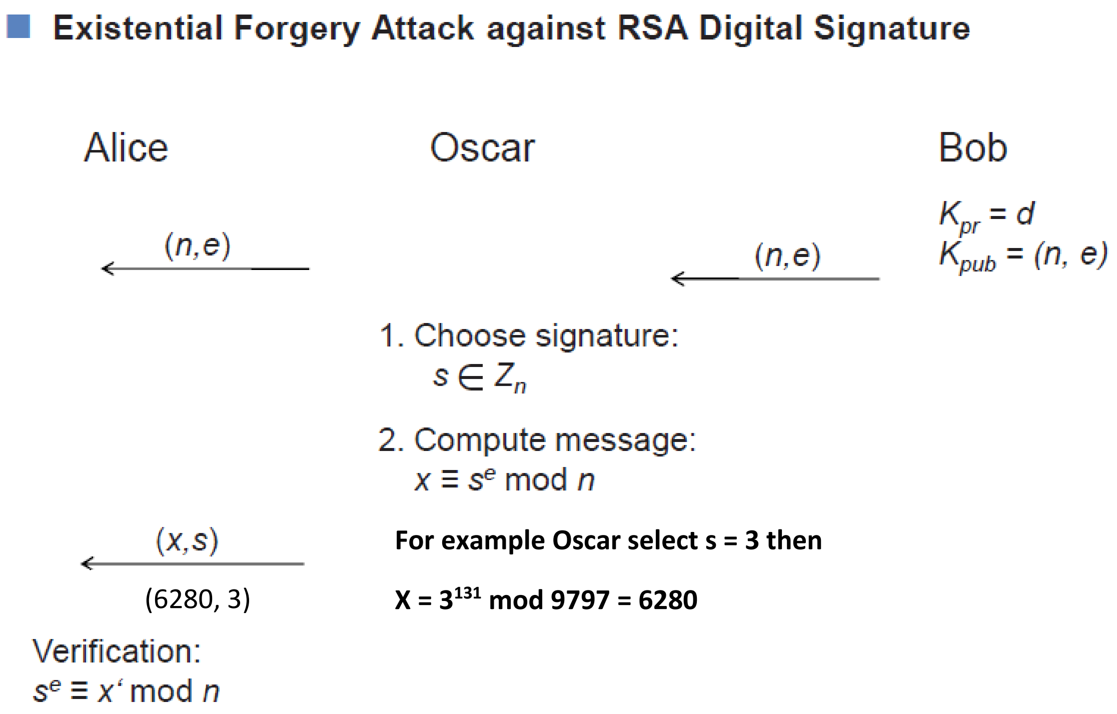
s = (x - dr) kE^{-1} mod p – 1 → s.kE = x – dr mod p – 1 → x = s.kE + dr mod p – 1

→ $\alpha^{dr + skE}$ mod p

P = 31 so we can choose kE form {0, 1, … , 29} → $|S_{kE}|$ = 30

So there are 30 valid signature for every x (message)

Question 4)



Existential Forgery Attack against RSA Digital Signature

1. Choose signature:
   $s \in Z_n$
2. Compute message:
   $x \equiv s^e \bmod n$

(x,s)

(6280, 3)

For example Oscar select s = 3 then

X = 3^{131} mod 9797 = 6280

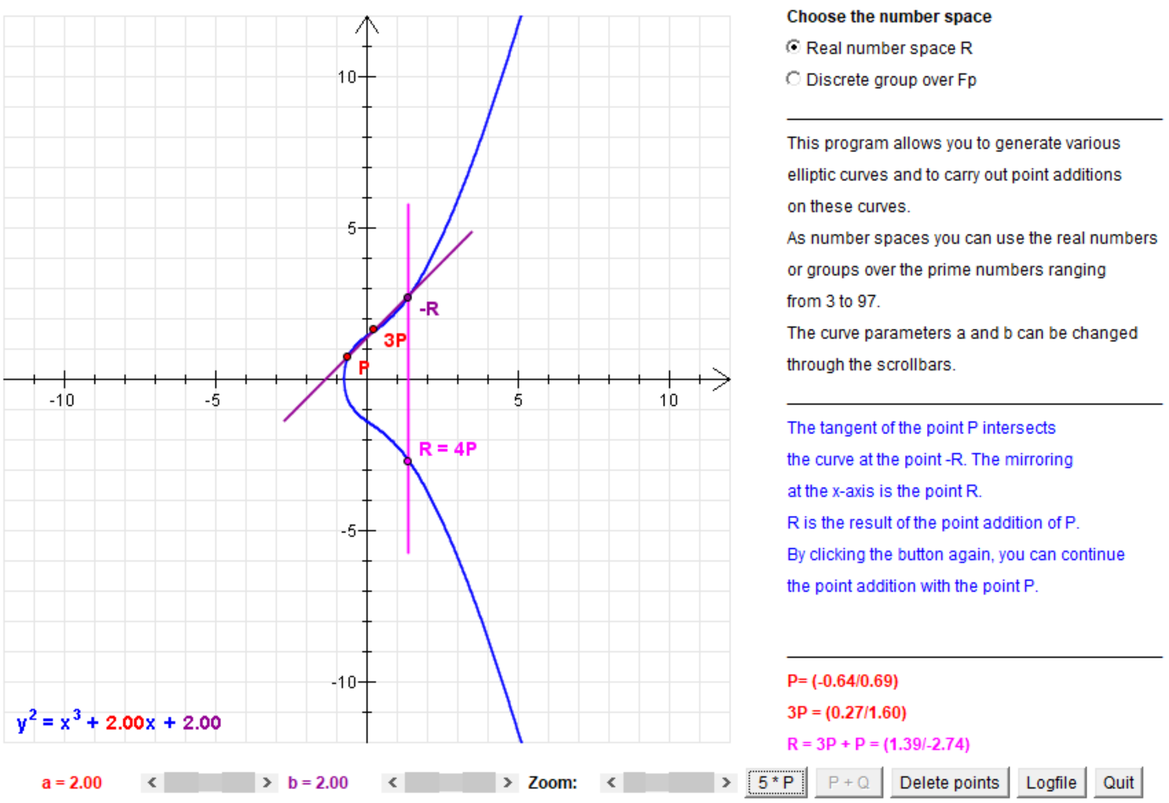
Verification:
$s^e \equiv x' \bmod n$

S^e mod 9797 = 3^{131} mod 9797 = 6280 = X'

X = 6280 , X' = 6280 → X = X' and signature is valid

Cryptool :

1.a



Choose the number space

● Real number space R

○ Discrete group over Fp

This program allows you to generate various elliptic curves and to carry out point additions on these curves.

As number spaces you can use the real numbers or groups over the prime numbers ranging from 3 to 97.

The curve parameters a and b can be changed through the scrollbars.

The tangent of the point P intersects the curve at the point -R. The mirroring at the x-axis is the point R.

R is the result of the point addition of P.

By clicking the button again, you can continue the point addition with the point P.

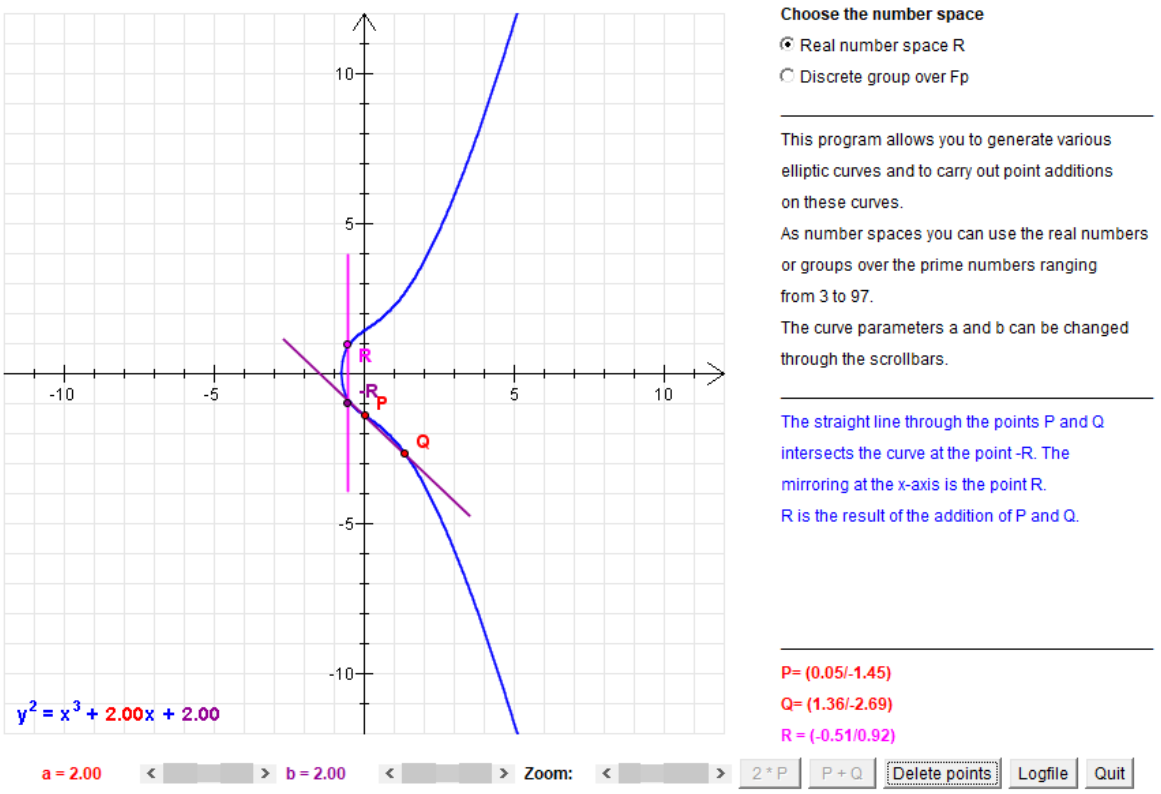
P= (-0.64/0.69)

3P = (0.27/1.60)

R = 3P + P = (1.39/-2.74)

a = 2.00 b = 2.00 Zoom:

1.b



Choose the number space

● Real number space R

○ Discrete group over Fp

This program allows you to generate various elliptic curves and to carry out point additions on these curves.

As number spaces you can use the real numbers or groups over the prime numbers ranging from 3 to 97.

The curve parameters a and b can be changed through the scrollbars.

The straight line through the points P and Q intersects the curve at the point -R. The mirroring at the x-axis is the point R.

R is the result of the addition of P and Q.

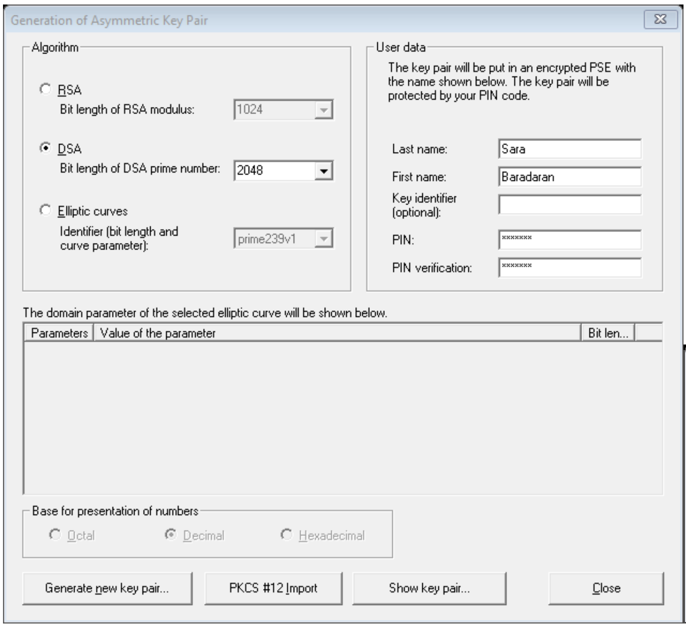
P= (0.05/-1.45)

Q= (1.36/-2.69)

R = (-0.51/0.92)

a = 2.00 b = 2.00 Zoom:

2.a



Generation of Asymmetric Key Pair

Algorithm

○ RSA
Bit length of RSA modulus: 1024

● DSA
Bit length of DSA prime number: 2048

○ 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.

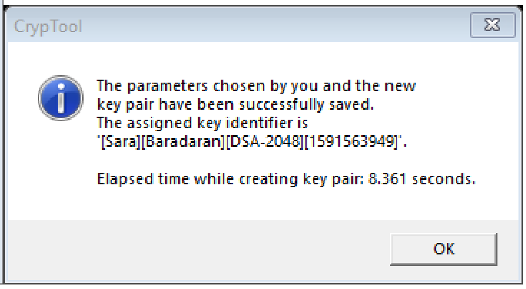
Last name: Sara
First name: Baradaran
Key identifier (optional):
PIN: *******
PIN verification: *******

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

Parameters	Value of the parameter	Bit len...

Base for presentation of numbers

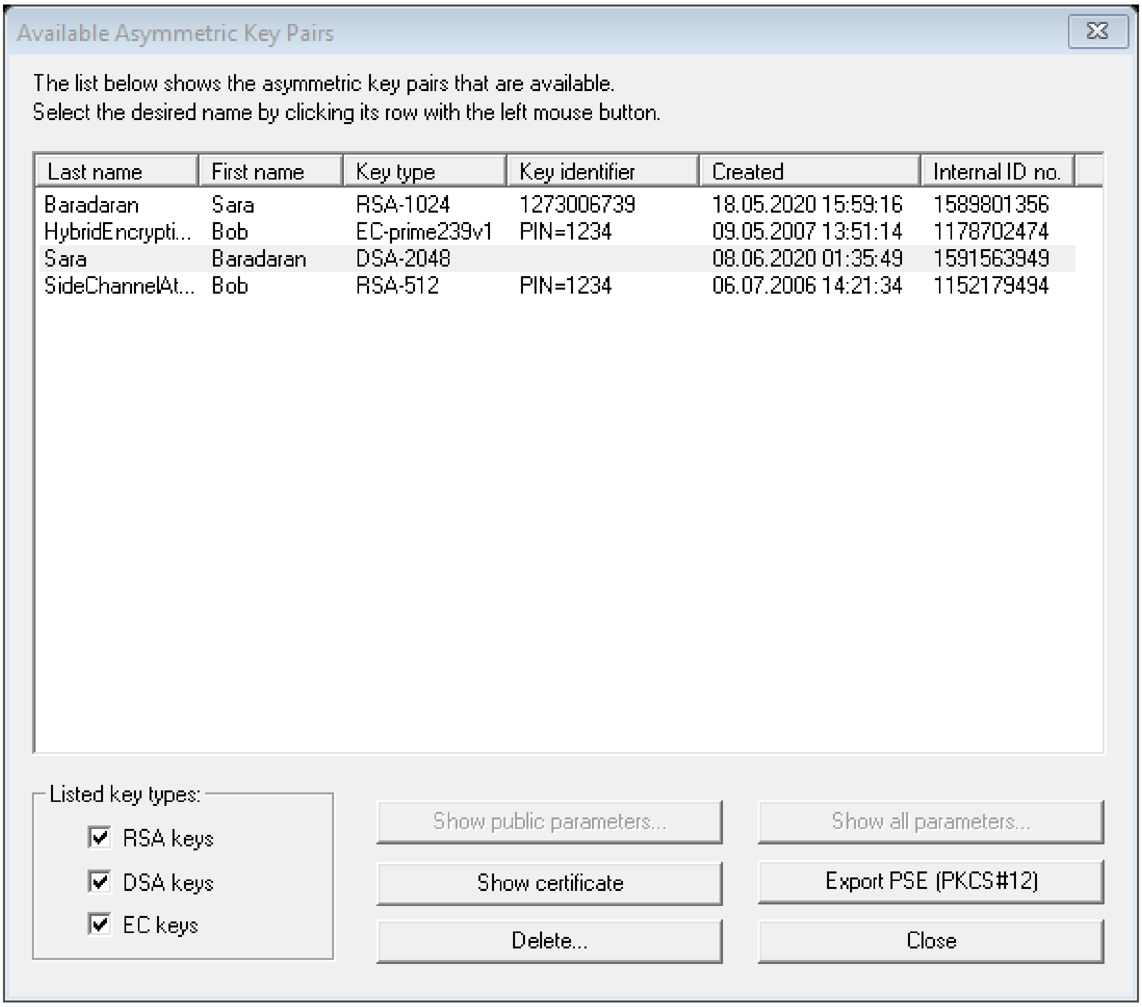
○ Octal ● Decimal ○ Hexadecimal



CrypTool

The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[Sara][Baradaran][DSA-2048][1591563949]'.

Elapsed time while creating key pair: 8.361 seconds.



Available Asymmetric Key Pairs

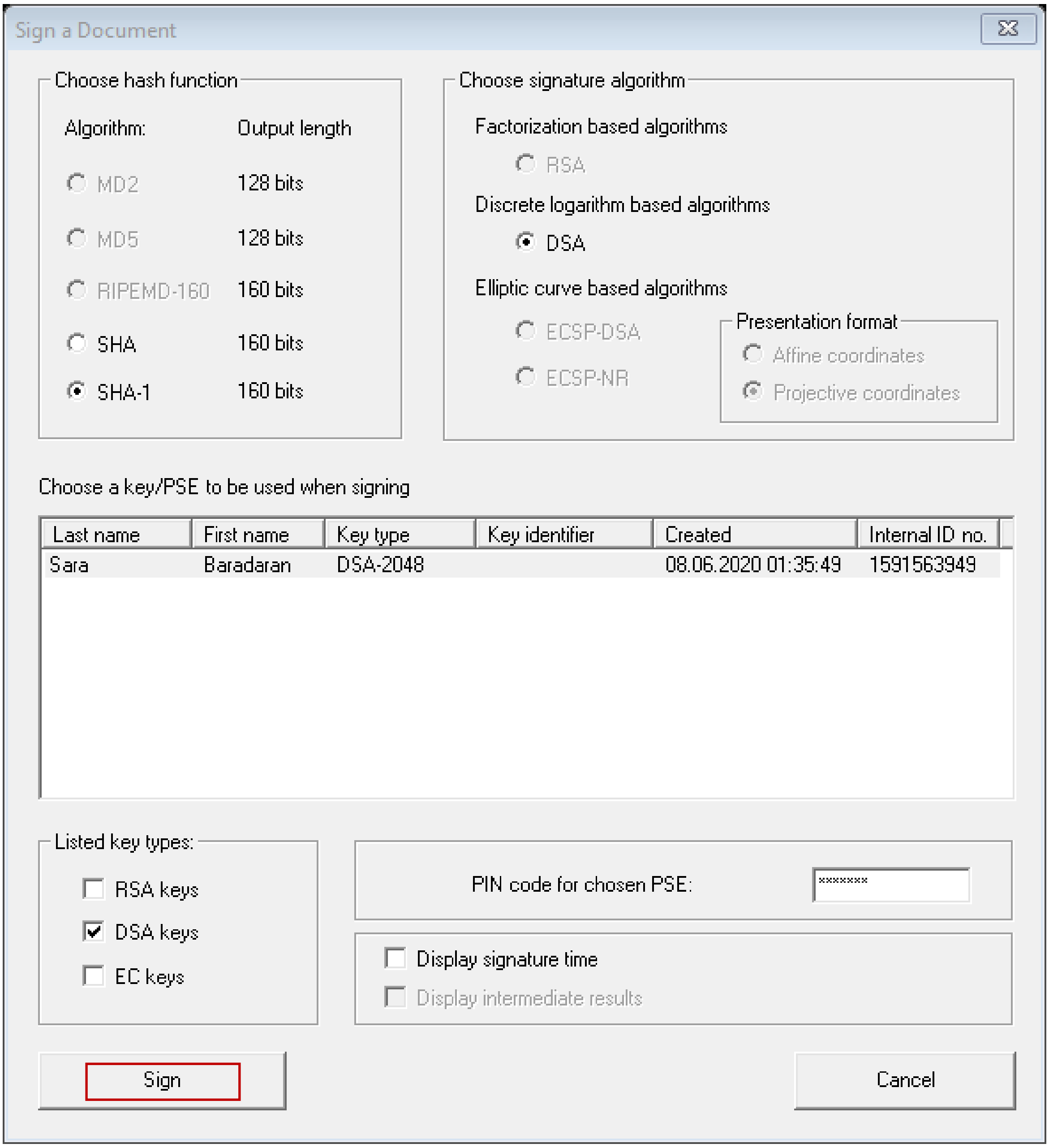
The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

Last name	First name	Key type	Key identifier	Created	Internal ID no.
Baradaran	Sara	RSA-1024	1273006739	18.05.2020 15:59:16	1589801356
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 13:51:14	1178702474
Sara	Baradaran	DSA-2048		08.06.2020 01:35:49	1591563949
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 14:21:34	1152179494

Listed key types:

☑ RSA keys
☑ DSA keys
☑ EC keys

2.b → output file has been attached :



Sign a Document

Choose hash function

Algorithm:	Output length
○ MD2	128 bits
○ MD5	128 bits
○ RIPEMD-160	160 bits
○ SHA	160 bits
● SHA-1	160 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

Choose a key/PSE to be used when signing

Last name	First name	Key type	Key identifier	Created	Internal ID no.
Sara	Baradaran	DSA-2048		08.06.2020 01:35:49	1591563949

Listed key types:

□ RSA keys

☑ DSA keys

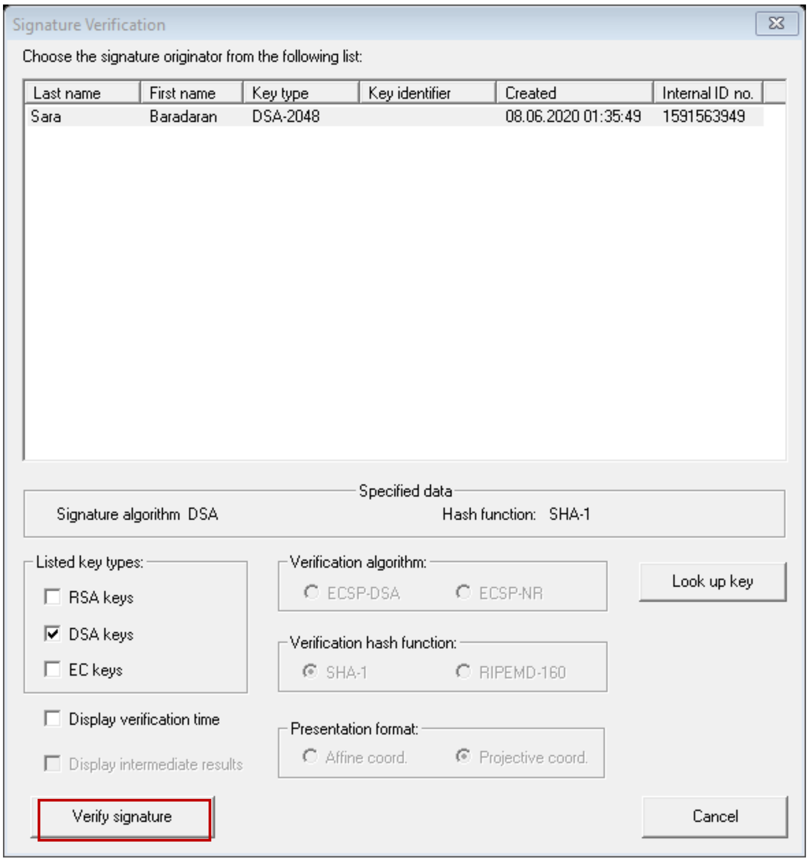
□ EC keys

PIN code for chosen PSE: ********

□ Display signature time

□ Display intermediate results

2.c



Signature Verification

Choose the signature originator from the following list:

Last name	First name	Key type	Key identifier	Created	Internal ID no.
Sara	Baradaran	DSA-2048		08.06.2020 01:35:49	1591563949

Specified data

Signature algorithm DSA

Hash function: SHA-1

Listed key types:

□ RSA keys

☑ DSA keys

□ EC keys

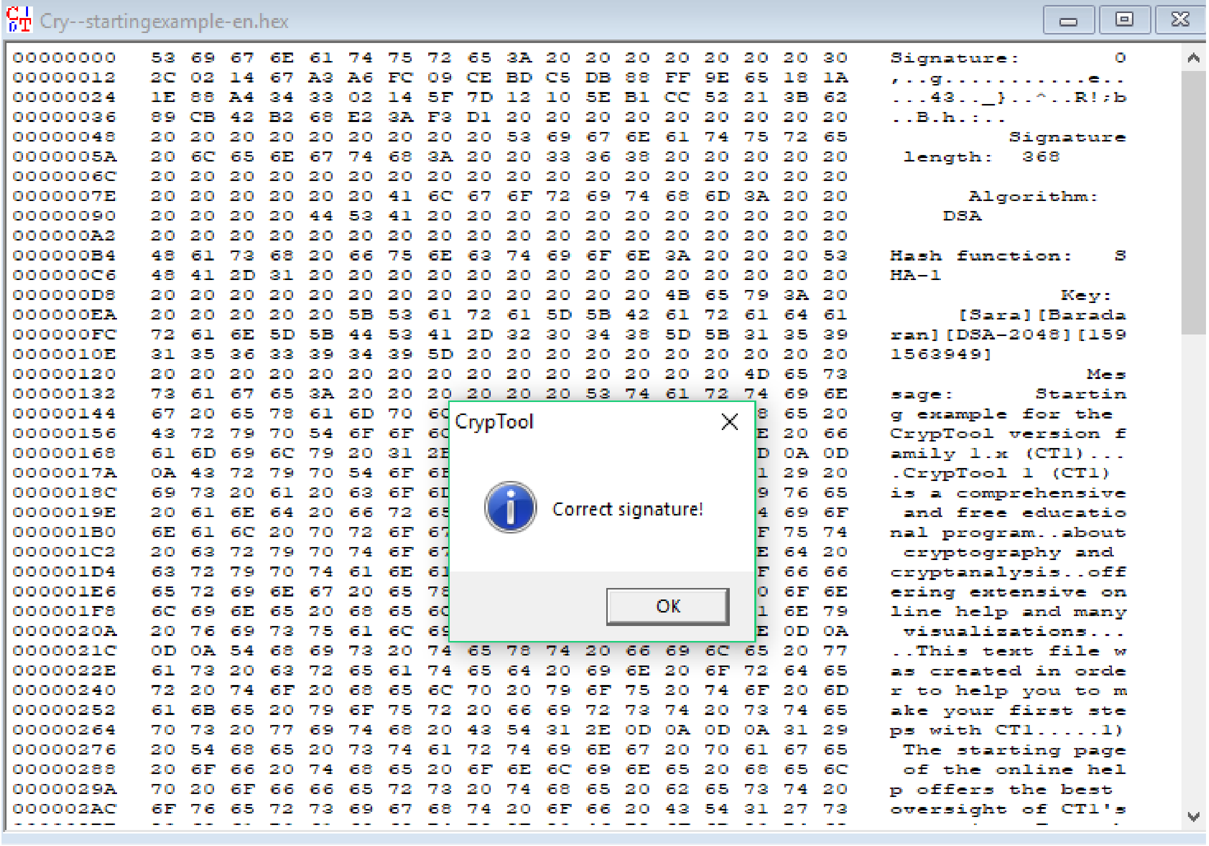
□ Display verification time

□ Display intermediate results

Verification algorithm: ○ ECSP-DSA ○ ECSP-NR

Verification hash function: ● SHA-1 ○ RIPEMD-160

Presentation format: ○ Affine coord. ● Projective coord.



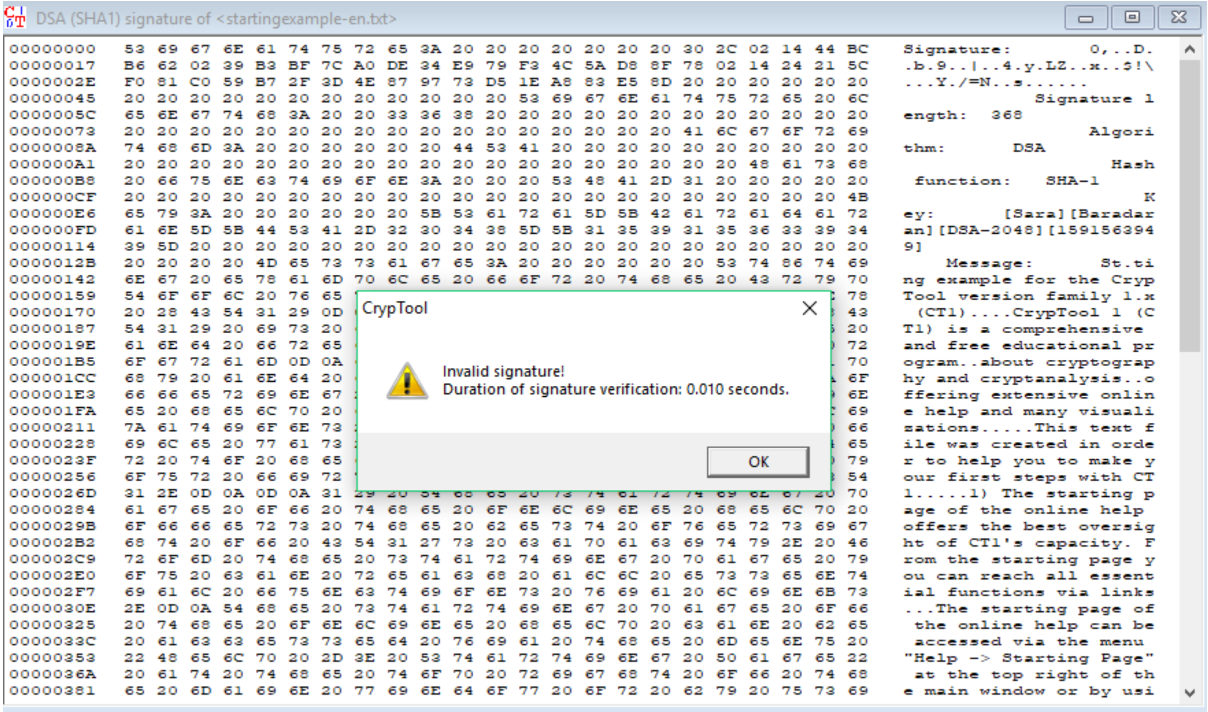
Cry--startingexample-en.hex

```
00000000   53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 30   Signature:       0
00000012   2C 02 14 67 A3 A6 FC 09 CE BD C5 DB 88 FF 9E 65 18 1A   ,..g...........e..
00000024   1E 88 A4 34 33 02 14 5F 7D 12 10 5E B1 CC 52 21 3B 62   ...43.._}..^..R!;b
00000036   89 CB 42 B2 68 E2 3A F3 D1 20 20 20 20 20 20 20 20 20   ..B.h.:..
00000048   20 20 20 20 20 20 20 20 20 53 69 67 6E 61 74 75 72 65            Signature
0000005A   20 6C 65 6E 67 74 68 3A 20 20 33 36 38 20 20 20 20 20    length:  368
0000006C   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0000007E   20 20 20 20 20 20 41 6C 67 6F 72 69 74 68 6D 3A 20 20         Algorithm:
00000090   20 20 20 20 44 53 41 20 20 20 20 20 20 20 20 20 20 20       DSA
000000A2   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
000000B4   48 61 73 68 20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 53   Hash function:   S
000000C6   48 41 2D 31 20 20 20 20 20 20 20 20 20 20 20 20 20 20   HA-1
000000D8   20 20 20 20 20 20 20 20 20 20 20 20 20 4B 65 79 3A 20                Key:
000000EA   20 20 20 20 20 5B 53 61 72 61 5D 5B 42 61 72 61 64 61        [Sara][Barada
000000FC   72 61 6E 5D 5B 44 53 41 2D 32 30 34 38 5D 5B 31 35 39   ran][DSA-2048][159
0000010E   31 35 36 33 39 34 39 5D 20 20 20 20 20 20 20 20 20 20   1563949]
00000120   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4D 65 73                  Mes
00000132   73 61 67 65 3A 20 20 20 20 20 20 53 74 61 72 74 69 6E   sage:      Startin
00000144   67 20 65 78 61 6D 70 6C                      68 65 20   g example for the
00000156   43 72 79 70 54 6F 6F 6C                      6E 20 66   CrypTool version f
00000168   61 6D 69 6C 79 20 31 2E                      0D 0A 0D   amily 1.x (CT1)...
0000017A   0A 43 72 79 70 54 6F 6F                      31 29 20   .CrypTool 1 (CT1)
0000018C   69 73 20 61 20 63 6F 6D                      69 76 65   is a comprehensive
0000019E   20 61 6E 64 20 66 72 65                      74 69 6F    and free educatio
000001B0   6E 61 6C 20 70 72 6F 67                      6F 75 74   nal program..about
000001C2   20 63 72 79 70 74 6F 67                      6E 64 20    cryptography and
000001D4   63 72 79 70 74 61 6E 61                      6F 66 66   cryptanalysis..off
000001E6   65 72 69 6E 67 20 65 78                      20 6F 6E   ering extensive on
000001F8   6C 69 6E 65 20 68 65 6C                      61 6E 79   line help and many
0000020A   20 76 69 73 75 61 6C 69                      2E 0D 0A    visualizations...
0000021C   0D 0A 54 68 69 73 20 74 65 78 74 20 66 69 6C 65 20 77   ..This text file w
0000022E   61 73 20 63 72 65 61 74 65 64 20 69 6E 20 6F 72 64 65   as created in orde
00000240   72 20 74 6F 20 68 65 6C 70 20 79 6F 75 20 74 6F 20 6D   r to help you to m
00000252   61 6B 65 20 79 6F 75 72 20 66 69 72 73 74 20 73 74 65   ake your first ste
00000264   70 73 20 77 69 74 68 20 43 54 31 2E 0D 0A 0D 0A 31 29   ps with CT1.....1)
00000276   20 54 68 65 20 73 74 61 72 74 69 6E 67 20 70 61 67 65    The starting page
00000288   20 6F 66 20 74 68 65 20 6F 6E 6C 69 6E 65 20 68 65 6C    of the online hel
0000029A   70 20 6F 66 66 65 72 73 20 74 68 65 20 62 65 73 74 20   p offers the best
000002AC   6F 76 65 72 73 69 67 68 74 20 6F 66 20 43 54 31 27 73   oversight of CT1's
```

CrypTool

Correct signature!

2.d → this signature is not valid



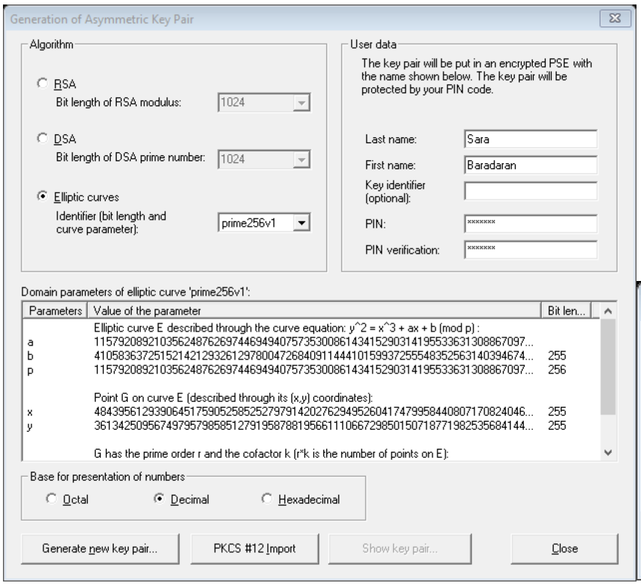
DSA (SHA1) signature of <startingexample-en.txt>

```
00000000   53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 20 30 2C 02 14 44 BC   Signature:       0,..D.
00000017   B6 62 02 39 B3 BF 7C A0 DE 34 E9 79 F3 4C 5A D8 8F 78 02 14 24 21 5C   .b.9..|..4.y.LZ..x..$!\
0000002E   F0 81 C0 59 B7 2F 3D 4E 87 97 73 D5 1E A8 83 E5 8D 20 20 20 20 20 20   ...Y./=N..s......
00000045   20 20 20 20 20 20 20 20 20 20 20 20 53 69 67 6E 61 74 75 72 65 20 6C               Signature l
0000005C   65 6E 67 74 68 3A 20 20 33 36 38 20 20 20 20 20 20 20 20 20 20 20 20   ength:  368
00000073   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 41 6C 67 6F 72 69                    Algori
0000008A   74 68 6D 3A 20 20 20 20 20 20 44 53 41 20 20 20 20 20 20 20 20 20 20   thm:      DSA
000000A1   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 48 61 73 68                      Hash
000000B8   20 66 75 6E 63 74 69 6F 6E 3A 20 20 20 53 48 41 2D 31 20 20 20 20 20    function:   SHA-1
000000CF   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 4B                         K
000000E6   65 79 3A 20 20 20 20 20 20 5B 53 61 72 61 5D 5B 42 61 72 61 64 61 72   ey:      [Sara][Baradar
000000FD   61 6E 5D 5B 44 53 41 2D 32 30 34 38 5D 5B 31 35 39 31 35 36 33 39 34   an][DSA-2048][159156394
00000114   39 5D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20   9]
0000012B   20 20 20 20 4D 65 73 73 61 67 65 3A 20 20 20 20 20 20 53 74 86 74 69       Message:      St.ti
00000142   6E 67 20 65 78 61 6D 70 6C 65 20 66 6F 72 20 74 68 65 20 43 72 79 70   ng example for the Cryp
00000159   54 6F 6F 6C 20 76 65                                              78   Tool version family 1.x
00000170   20 28 43 54 31 29 0D                                              43    (CT1)....CrypTool 1 (C
00000187   54 31 29 20 69 73 20                                              20   T1) is a comprehensive
0000019E   61 6E 64 20 66 72 65                                              72   and free educational pr
000001B5   6F 67 72 61 6D 0D 0A                                              70   ogram..about cryptograp
000001CC   68 79 20 61 6E 64 20                                              6F   hy and cryptanalysis..o
000001E3   66 66 65 72 69 6E 67                                              6E   ffering extensive onlin
000001FA   65 20 68 65 6C 70 20                                              69   e help and many visuali
00000211   7A 61 74 69 6F 6E 73                                              66   zations.....This text f
00000228   69 6C 65 20 77 61 73                                              65   ile was created in orde
0000023F   72 20 74 6F 20 68 65                                              79   r to help you to make y
00000256   6F 75 72 20 66 69 72                                              54   our first steps with CT
0000026D   31 2E 0D 0A 0D 0A 31 29 20 54 68 65 20 73 74 61 72 74 69 6E 67 20 70   1.....1) The starting p
00000284   61 67 65 20 6F 66 20 74 68 65 20 6F 6E 6C 69 6E 65 20 68 65 6C 70 20   age of the online help
0000029B   6F 66 66 65 72 73 20 74 68 65 20 62 65 73 74 20 6F 76 65 72 73 69 67   offers the best oversig
000002B2   68 74 20 6F 66 20 43 54 31 27 73 20 63 61 70 61 63 69 74 79 2E 20 46   ht of CT1's capacity. F
000002C9   72 6F 6D 20 74 68 65 20 73 74 61 72 74 69 6E 67 20 70 61 67 65 20 79   rom the starting page y
000002E0   6F 75 20 63 61 6E 20 72 65 61 63 68 20 61 6C 6C 20 65 73 73 65 6E 74   ou can reach all essent
000002F7   69 61 6C 20 66 75 6E 63 74 69 6F 6E 73 20 76 69 61 20 6C 69 6E 6B 73   ial functions via links
0000030E   2E 0D 0A 54 68 65 20 73 74 61 72 74 69 6E 67 20 70 61 67 65 20 6F 66   ...The starting page of
00000325   20 74 68 65 20 6F 6E 6C 69 6E 65 20 68 65 6C 70 20 63 61 6E 20 62 65    the online help can be
0000033C   20 61 63 63 65 73 73 65 64 20 76 69 61 20 74 68 65 20 6D 65 6E 75 20    accessed via the menu
00000353   22 48 65 6C 70 20 2D 3E 20 53 74 61 72 74 69 6E 67 20 50 61 67 65 22   "Help -> Starting Page"
0000036A   20 61 74 20 74 68 65 20 74 6F 70 20 72 69 67 68 74 20 6F 66 20 74 68    at the top right of th
00000381   65 20 6D 61 69 6E 20 77 69 6E 64 6F 77 20 6F 72 20 62 79 20 75 73 69   e main window or by usi
```

CrypTool

Invalid signature!
Duration of signature verification: 0.010 seconds.

3.a



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): prime256v1

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.

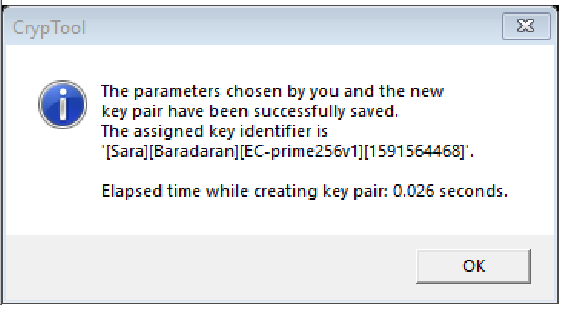
Last name: Sara
First name: Baradaran
Key identifier (optional):
PIN: *******
PIN verification: *******

Domain parameters of elliptic curve 'prime256v1':

Parameters	Value of the parameter	Bit len...
	Elliptic curve E described through the curve equation: y^2 = x^3 + ax + b (mod p) :	
a	115792089210356248762697446949407573530086143415290314195533631308867097...	
b	410583637251521421293261297800472684091144410159937255548352563140394674...	255
p	115792089210356248762697446949407573530086143415290314195533631308867097...	256
	Point G on curve E (described through its (x,y) coordinates):	
x	484395612939064517590525852527979142027629495260417479958440807170824046...	255
y	361342509567497957985851279195878819566111066729850150718771982535684144...	255
	G has the prime order r and the cofactor k (r*k is the number of points on E):	

Base for presentation of numbers

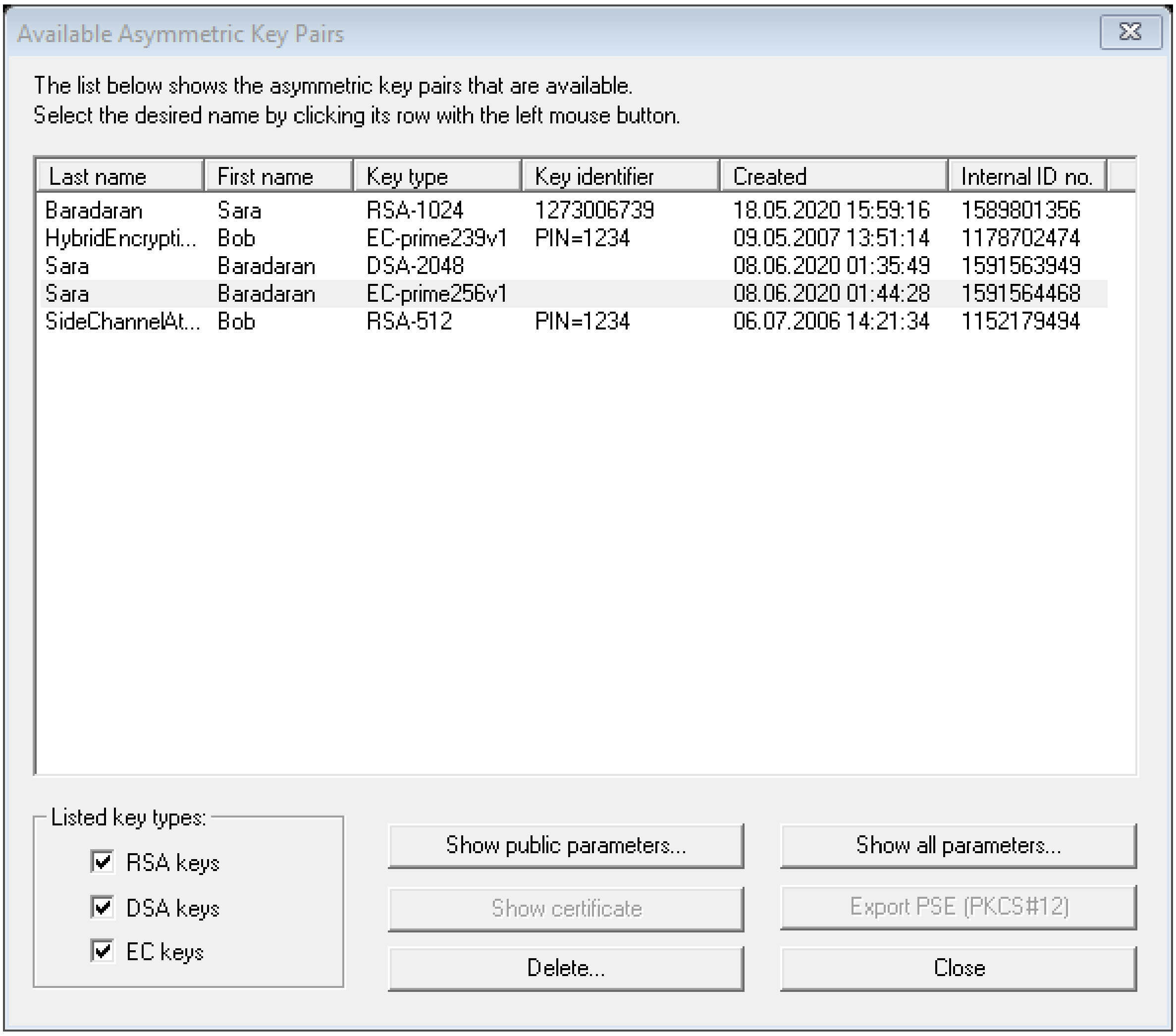
○ Octal ● Decimal ○ Hexadecimal



CrypTool

The parameters chosen by you and the new key pair have been successfully saved.
The assigned key identifier is '[Sara][Baradaran][EC-prime256v1][1591564468]'.

Elapsed time while creating key pair: 0.026 seconds.



Available Asymmetric Key Pairs

The list below shows the asymmetric key pairs that are available.
Select the desired name by clicking its row with the left mouse button.

Last name	First name	Key type	Key identifier	Created	Internal ID no.
Baradaran	Sara	RSA-1024	1273006739	18.05.2020 15:59:16	1589801356
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 13:51:14	1178702474
Sara	Baradaran	DSA-2048		08.06.2020 01:35:49	1591563949
Sara	Baradaran	EC-prime256v1		08.06.2020 01:44:28	1591564468
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 14:21:34	1152179494

Listed key types:

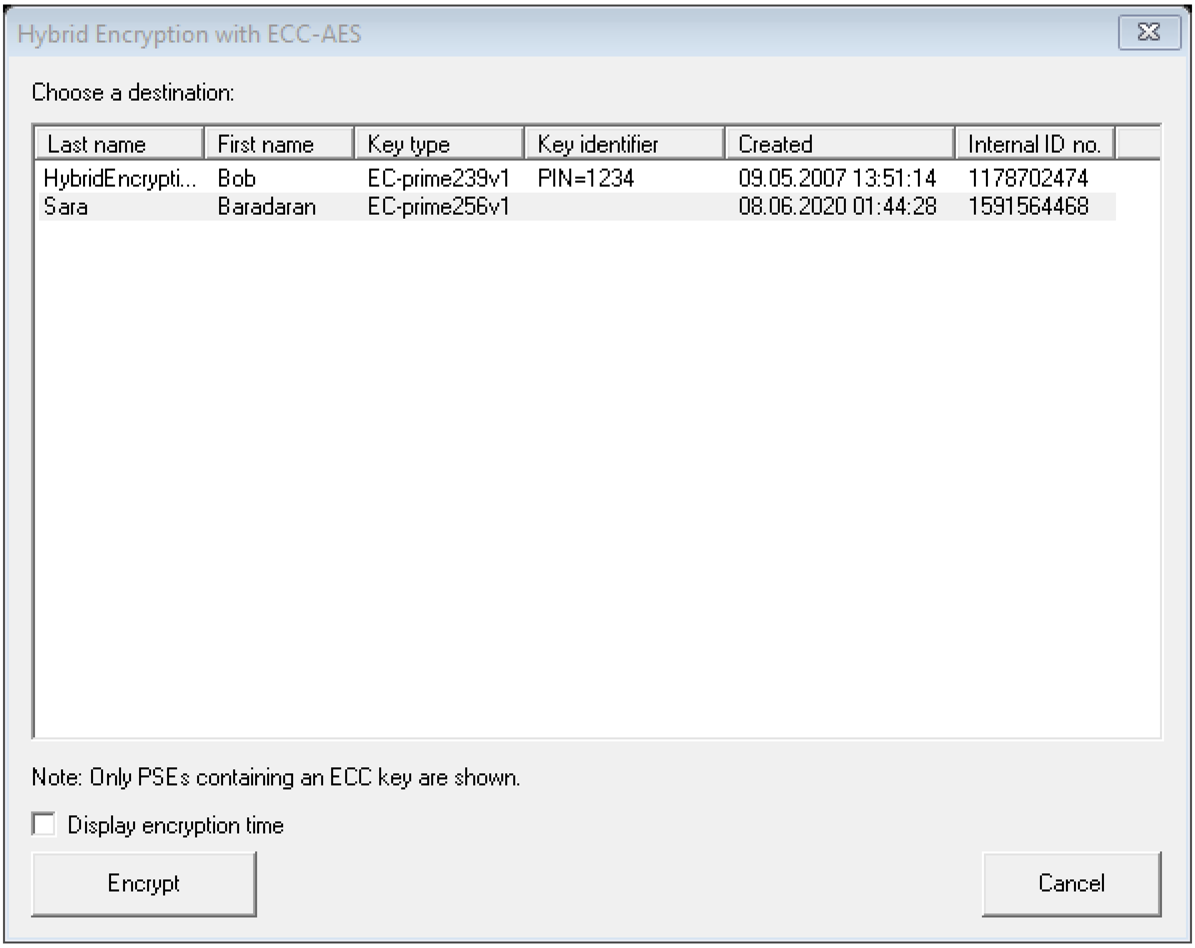
☑ RSA keys

☑ DSA keys

☑ EC keys

3.b→ output file has been attached :

عملیات توان رسانی یک عملیات سنگین و برای پیام های بزرگ بسیار هزینه بر و زمان بر است لذا نمیتوان صرفا از رمز نامتقارن برای رمز کردن کل متن پیام استفاده کرد بلکه معمولا برای مبادله کلید از این نوع رمزنگاری استفاده می شود و سپس پیام ها با یک روش رمز متقارن توسط کلید مذکور رمز می شوند.



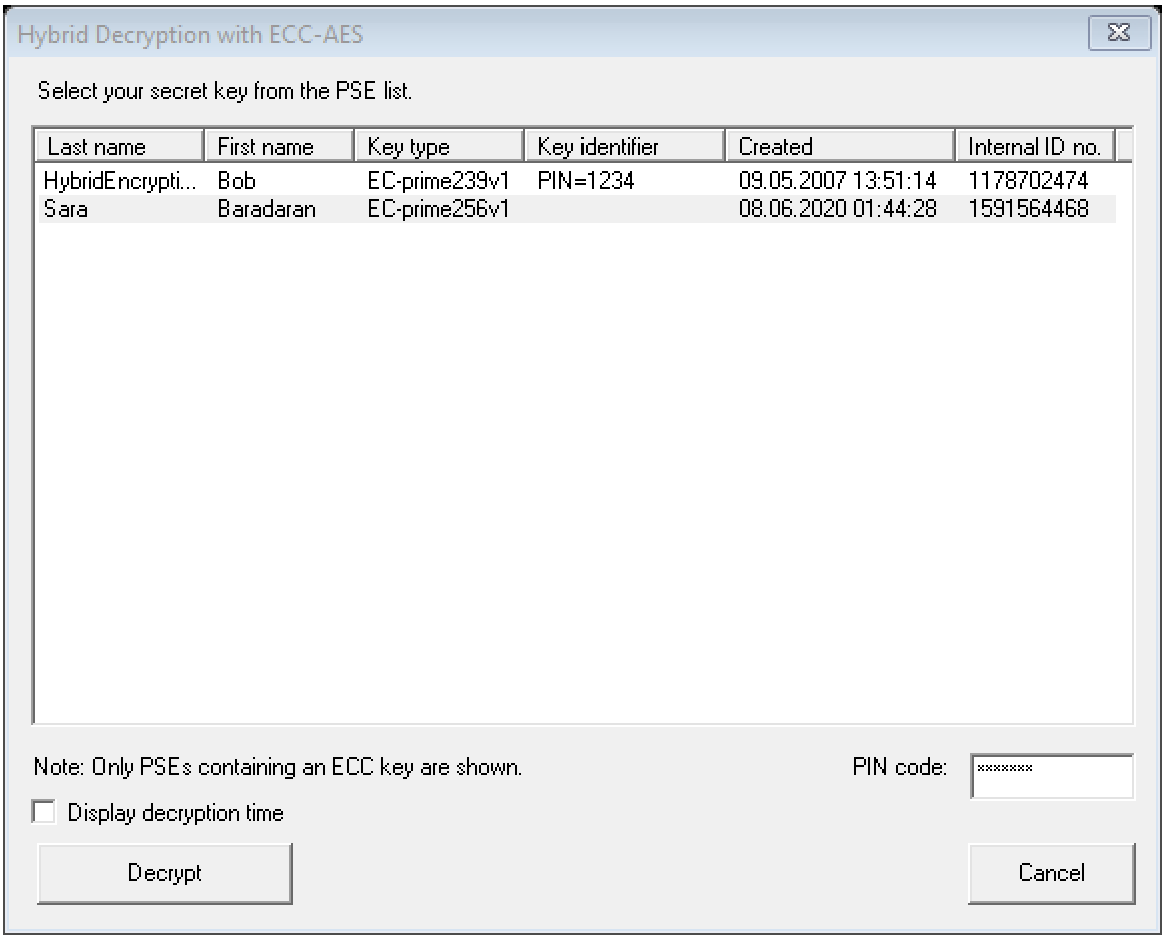
Choose a destination:

Last name	First name	Key type	Key identifier	Created	Internal ID no.
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 13:51:14	1178702474
Sara	Baradaran	EC-prime256v1		08.06.2020 01:44:28	1591564468

Note: Only PSEs containing an ECC key are shown.

☐ Display encryption time

3.c→ output file has been attached :



Hybrid Decryption with ECC-AES

Select your secret key from the PSE list.

Last name	First name	Key type	Key identifier	Created	Internal ID no.
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 13:51:14	1178702474
Sara	Baradaran	EC-prime256v1		08.06.2020 01:44:28	1591564468

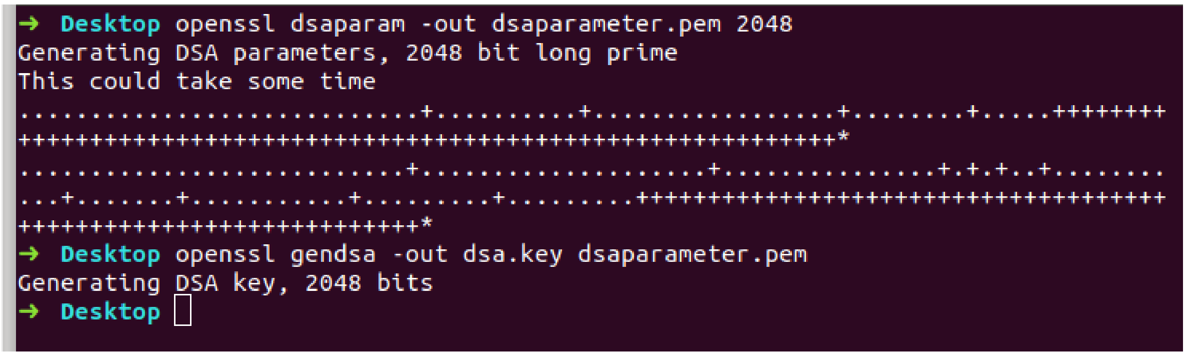
Note: Only PSEs containing an ECC key are shown.

PIN code: *******

□ Display decryption time

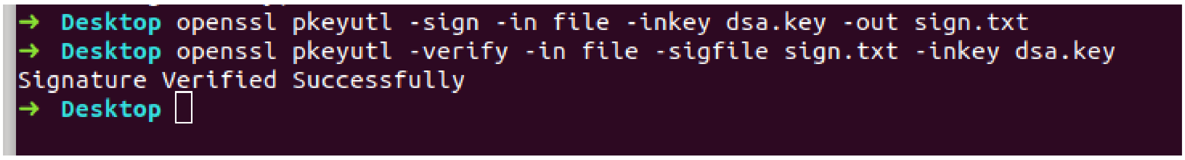
Openssl :

1.a



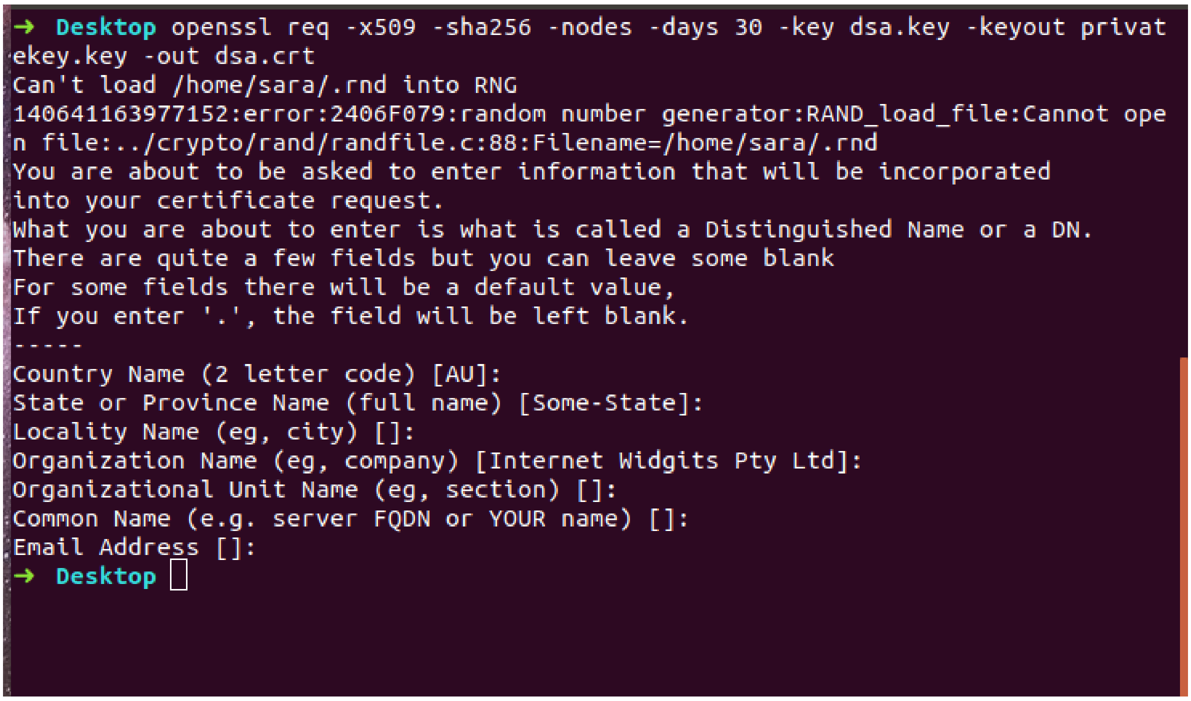
```
➜  Desktop openssl dsaparam -out dsaparameter.pem 2048
Generating DSA parameters, 2048 bit long prime
This could take some time
............................+..........+.................+........+.....++++++++
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++*
...........................+....................+...............+.+.+..+........
...+.......+...........+.........+.........+++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++*
➜  Desktop openssl gendsa -out dsa.key dsaparameter.pem
Generating DSA key, 2048 bits
➜  Desktop 
```

1.b, c

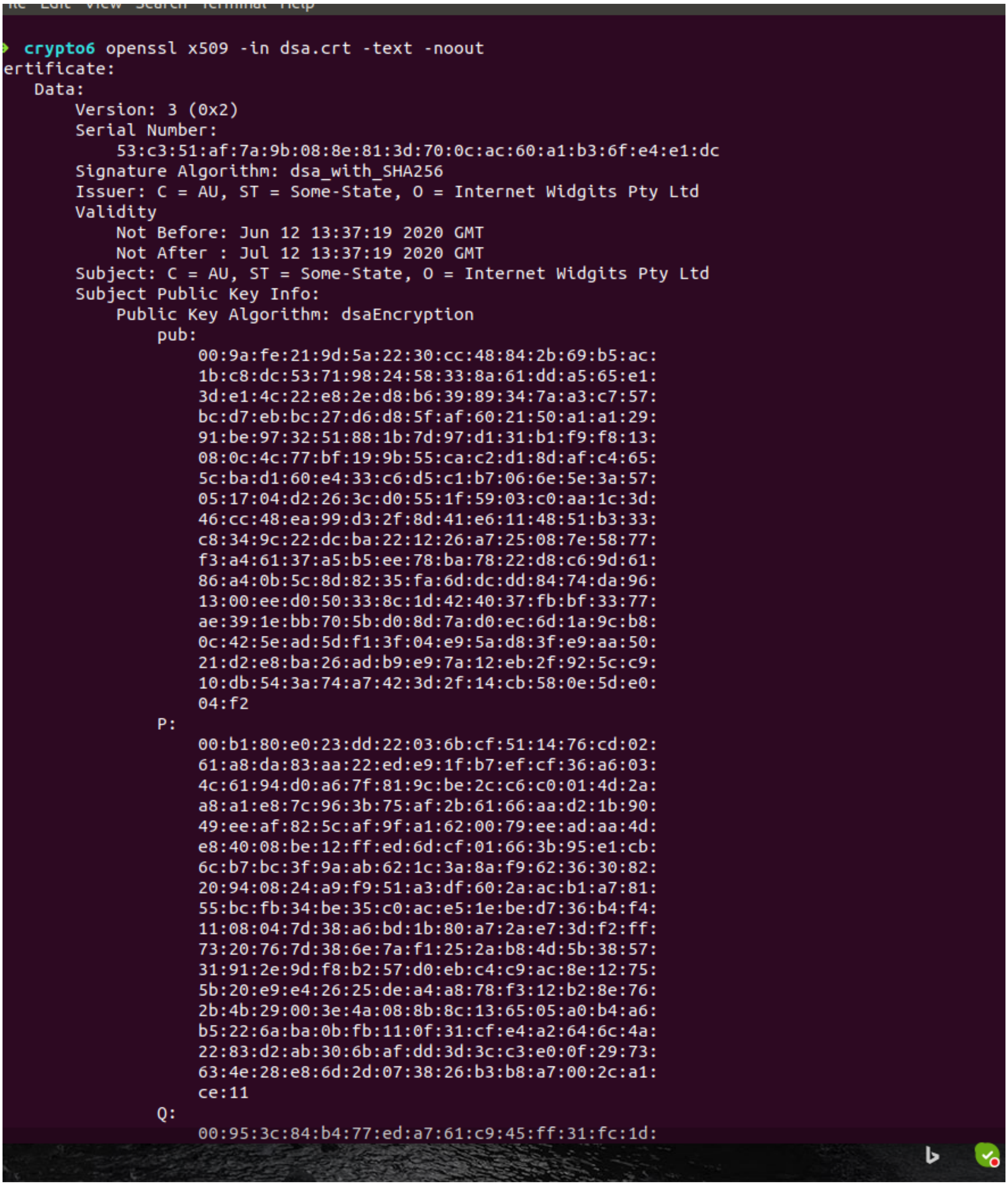


```
➜  Desktop openssl pkeyutl -sign -in file -inkey dsa.key -out sign.txt
➜  Desktop openssl pkeyutl -verify -in file -sigfile sign.txt -inkey dsa.key
Signature Verified Successfully
➜  Desktop 
```

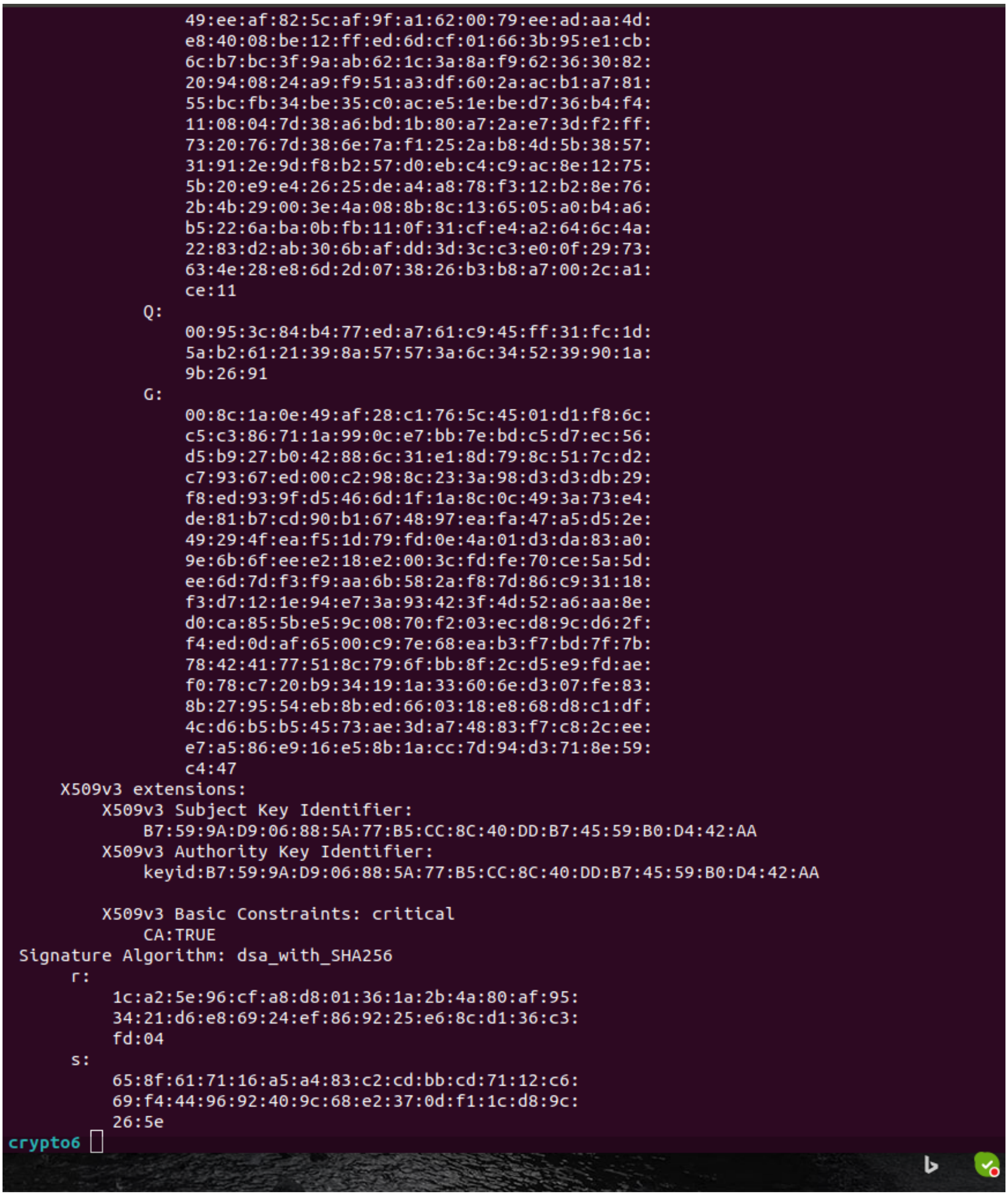
1.d



```
➜  Desktop openssl req -x509 -sha256 -nodes -days 30 -key dsa.key -keyout privat
ekey.key -out dsa.crt
Can't load /home/sara/.rnd into RNG
140641163977152:error:2406F079:random number generator:RAND_load_file:Cannot ope
n file:../crypto/rand/randfile.c:88:Filename=/home/sara/.rnd
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
➜  Desktop 
```

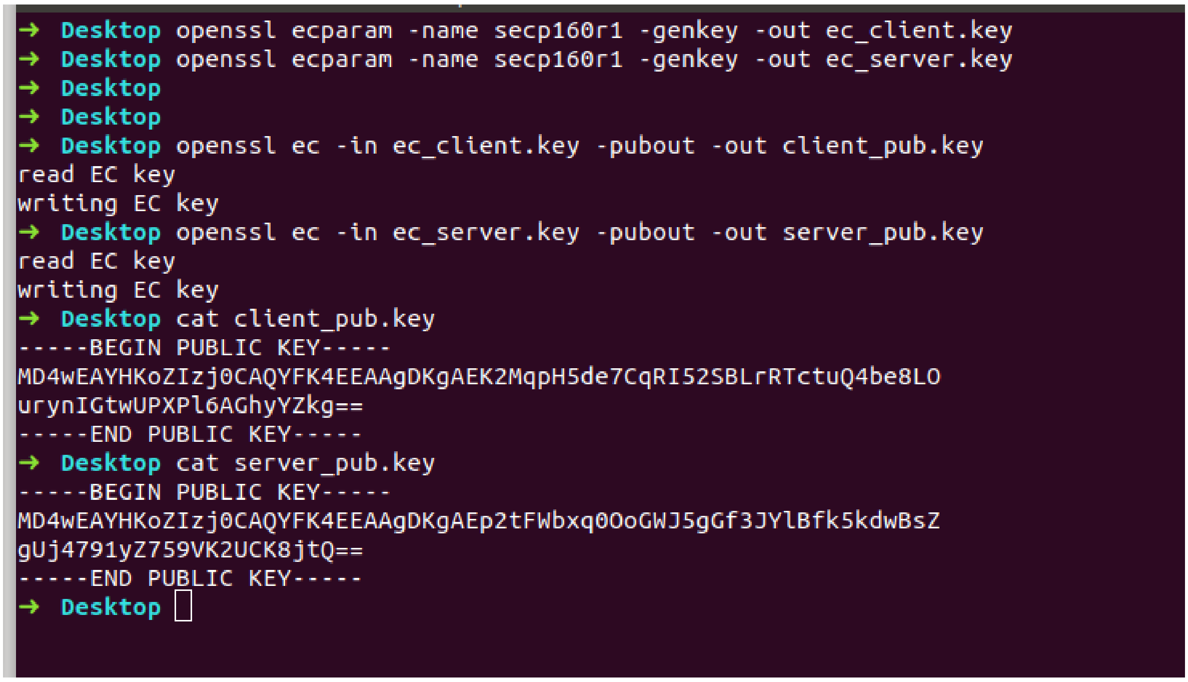


```
❯ crypto6 openssl x509 -in dsa.crt -text -noout
ertificate:
   Data:
       Version: 3 (0x2)
       Serial Number:
           53:c3:51:af:7a:9b:08:8e:81:3d:70:0c:ac:60:a1:b3:6f:e4:e1:dc
       Signature Algorithm: dsa_with_SHA256
       Issuer: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
       Validity
           Not Before: Jun 12 13:37:19 2020 GMT
           Not After : Jul 12 13:37:19 2020 GMT
       Subject: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
       Subject Public Key Info:
           Public Key Algorithm: dsaEncryption
               pub:
                   00:9a:fe:21:9d:5a:22:30:cc:48:84:2b:69:b5:ac:
                   1b:c8:dc:53:71:98:24:58:33:8a:61:dd:a5:65:e1:
                   3d:e1:4c:22:e8:2e:d8:b6:39:89:34:7a:a3:c7:57:
                   bc:d7:eb:bc:27:d6:d8:5f:af:60:21:50:a1:a1:29:
                   91:be:97:32:51:88:1b:7d:97:d1:31:b1:f9:f8:13:
                   08:0c:4c:77:bf:19:9b:55:ca:c2:d1:8d:af:c4:65:
                   5c:ba:d1:60:e4:33:c6:d5:c1:b7:06:6e:5e:3a:57:
                   05:17:04:d2:26:3c:d0:55:1f:59:03:c0:aa:1c:3d:
                   46:cc:48:ea:99:d3:2f:8d:41:e6:11:48:51:b3:33:
                   c8:34:9c:22:dc:ba:22:12:26:a7:25:08:7e:58:77:
                   f3:a4:61:37:a5:b5:ee:78:ba:78:22:d8:c6:9d:61:
                   86:a4:0b:5c:8d:82:35:fa:6d:dc:dd:84:74:da:96:
                   13:00:ee:d0:50:33:8c:1d:42:40:37:fb:bf:33:77:
                   ae:39:1e:bb:70:5b:d0:8d:7a:d0:ec:6d:1a:9c:b8:
                   0c:42:5e:ad:5d:f1:3f:04:e9:5a:d8:3f:e9:aa:50:
                   21:d2:e8:ba:26:ad:b9:e9:7a:12:eb:2f:92:5c:c9:
                   10:db:54:3a:74:a7:42:3d:2f:14:cb:58:0e:5d:e0:
                   04:f2
               P:
                   00:b1:80:e0:23:dd:22:03:6b:cf:51:14:76:cd:02:
                   61:a8:da:83:aa:22:ed:e9:1f:b7:ef:cf:36:a6:03:
                   4c:61:94:d0:a6:7f:81:9c:be:2c:c6:c0:01:4d:2a:
                   a8:a1:e8:7c:96:3b:75:af:2b:61:66:aa:d2:1b:90:
                   49:ee:af:82:5c:af:9f:a1:62:00:79:ee:ad:aa:4d:
                   e8:40:08:be:12:ff:ed:6d:cf:01:66:3b:95:e1:cb:
                   6c:b7:bc:3f:9a:ab:62:1c:3a:8a:f9:62:36:30:82:
                   20:94:08:24:a9:f9:51:a3:df:60:2a:ac:b1:a7:81:
                   55:bc:fb:34:be:35:c0:ac:e5:1e:be:d7:36:b4:f4:
                   11:08:04:7d:38:a6:bd:1b:80:a7:2a:e7:3d:f2:ff:
                   73:20:76:7d:38:6e:7a:f1:25:2a:b8:4d:5b:38:57:
                   31:91:2e:9d:f8:b2:57:d0:eb:c4:c9:ac:8e:12:75:
                   5b:20:e9:e4:26:25:de:a4:a8:78:f3:12:b2:8e:76:
                   2b:4b:29:00:3e:4a:08:8b:8c:13:65:05:a0:b4:a6:
                   b5:22:6a:ba:0b:fb:11:0f:31:cf:e4:a2:64:6c:4a:
                   22:83:d2:ab:30:6b:af:dd:3d:3c:c3:e0:0f:29:73:
                   63:4e:28:e8:6d:2d:07:38:26:b3:b8:a7:00:2c:a1:
                   ce:11
               Q:
                   00:95:3c:84:b4:77:ed:a7:61:c9:45:ff:31:fc:1d:
```



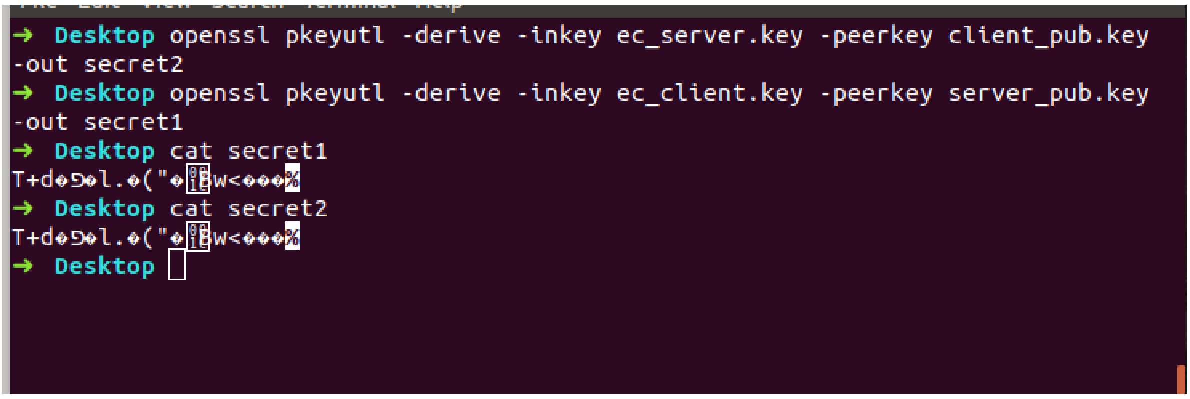
```
                    49:ee:af:82:5c:af:9f:a1:62:00:79:ee:ad:aa:4d:
                    e8:40:08:be:12:ff:ed:6d:cf:01:66:3b:95:e1:cb:
                    6c:b7:bc:3f:9a:ab:62:1c:3a:8a:f9:62:36:30:82:
                    20:94:08:24:a9:f9:51:a3:df:60:2a:ac:b1:a7:81:
                    55:bc:fb:34:be:35:c0:ac:e5:1e:be:d7:36:b4:f4:
                    11:08:04:7d:38:a6:bd:1b:80:a7:2a:e7:3d:f2:ff:
                    73:20:76:7d:38:6e:7a:f1:25:2a:b8:4d:5b:38:57:
                    31:91:2e:9d:f8:b2:57:d0:eb:c4:c9:ac:8e:12:75:
                    5b:20:e9:e4:26:25:de:a4:a8:78:f3:12:b2:8e:76:
                    2b:4b:29:00:3e:4a:08:8b:8c:13:65:05:a0:b4:a6:
                    b5:22:6a:ba:0b:fb:11:0f:31:cf:e4:a2:64:6c:4a:
                    22:83:d2:ab:30:6b:af:dd:3d:3c:c3:e0:0f:29:73:
                    63:4e:28:e8:6d:2d:07:38:26:b3:b8:a7:00:2c:a1:
                    ce:11
                Q:
                    00:95:3c:84:b4:77:ed:a7:61:c9:45:ff:31:fc:1d:
                    5a:b2:61:21:39:8a:57:57:3a:6c:34:52:39:90:1a:
                    9b:26:91
                G:
                    00:8c:1a:0e:49:af:28:c1:76:5c:45:01:d1:f8:6c:
                    c5:c3:86:71:1a:99:0c:e7:bb:7e:bd:c5:d7:ec:56:
                    d5:b9:27:b0:42:88:6c:31:e1:8d:79:8c:51:7c:d2:
                    c7:93:67:ed:00:c2:98:8c:23:3a:98:d3:d3:db:29:
                    f8:ed:93:9f:d5:46:6d:1f:1a:8c:0c:49:3a:73:e4:
                    de:81:b7:cd:90:b1:67:48:97:ea:fa:47:a5:d5:2e:
                    49:29:4f:ea:f5:1d:79:fd:0e:4a:01:d3:da:83:a0:
                    9e:6b:6f:ee:e2:18:e2:00:3c:fd:fe:70:ce:5a:5d:
                    ee:6d:7d:f3:f9:aa:6b:58:2a:f8:7d:86:c9:31:18:
                    f3:d7:12:1e:94:e7:3a:93:42:3f:4d:52:a6:aa:8e:
                    d0:ca:85:5b:e5:9c:08:70:f2:03:ec:d8:9c:d6:2f:
                    f4:ed:0d:af:65:00:c9:7e:68:ea:b3:f7:bd:7f:7b:
                    78:42:41:77:51:8c:79:6f:bb:8f:2c:d5:e9:fd:ae:
                    f0:78:c7:20:b9:34:19:1a:33:60:6e:d3:07:fe:83:
                    8b:27:95:54:eb:8b:ed:66:03:18:e8:68:d8:c1:df:
                    4c:d6:b5:b5:45:73:ae:3d:a7:48:83:f7:c8:2c:ee:
                    e7:a5:86:e9:16:e5:8b:1a:cc:7d:94:d3:71:8e:59:
                    c4:47
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                B7:59:9A:D9:06:88:5A:77:B5:CC:8C:40:DD:B7:45:59:B0:D4:42:AA
            X509v3 Authority Key Identifier:
                keyid:B7:59:9A:D9:06:88:5A:77:B5:CC:8C:40:DD:B7:45:59:B0:D4:42:AA

            X509v3 Basic Constraints: critical
                CA:TRUE
Signature Algorithm: dsa_with_SHA256
     r:
         1c:a2:5e:96:cf:a8:d8:01:36:1a:2b:4a:80:af:95:
         34:21:d6:e8:69:24:ef:86:92:25:e6:8c:d1:36:c3:
         fd:04
     s:
         65:8f:61:71:16:a5:a4:83:c2:cd:bb:cd:71:12:c6:
         69:f4:44:96:92:40:9c:68:e2:37:0d:f1:1c:d8:9c:
         26:5e
crypto6 
```

2.a, b



```
➜  Desktop openssl ecparam -name secp160r1 -genkey -out ec_client.key
➜  Desktop openssl ecparam -name secp160r1 -genkey -out ec_server.key
➜  Desktop
➜  Desktop
➜  Desktop openssl ec -in ec_client.key -pubout -out client_pub.key
read EC key
writing EC key
➜  Desktop openssl ec -in ec_server.key -pubout -out server_pub.key
read EC key
writing EC key
➜  Desktop cat client_pub.key
-----BEGIN PUBLIC KEY-----
MD4wEAYHKoZIzj0CAQYFK4EEAAgDKgAEK2MqpH5de7CqRI52SBLrRTctuQ4be8LO
urynIGtwUPXPl6AGhyYZkg==
-----END PUBLIC KEY-----
➜  Desktop cat server_pub.key
-----BEGIN PUBLIC KEY-----
MD4wEAYHKoZIzj0CAQYFK4EEAAgDKgAEp2tFWbxq0OoGWJ5gGf3JYlBfk5kdwBsZ
gUj4791yZ759VK2UCK8jtQ==
-----END PUBLIC KEY-----
➜  Desktop 
```

2.c, d, e



```
➜  Desktop openssl pkeyutl -derive -inkey ec_server.key -peerkey client_pub.key
-out secret2
➜  Desktop openssl pkeyutl -derive -inkey ec_client.key -peerkey server_pub.key
-out secret1
➜  Desktop cat secret1
T+d�Ͽ�l.�("��w<����%
➜  Desktop cat secret2
T+d�Ͽ�l.�("��w<����%
➜  Desktop 
```

Result → secret1 and secret2 files have the same content.

کلید مشترک از طریق زیر محاسبه می شود. که برای هر دو طرف ارتباط یکسان بدست می آید لذا محتوای دو فایل secret1
و secret2 کاملا یکسان است.

Server :

$K_{pr\_server} = a$, $K_{pub\_client} = bP$

$K_{pr\_server} K_{pub\_client} = abP$

client :

$K_{pr\_client} = b$, $K_{pub\_server} = aP$

$K_{pr\_client} K_{pub\_server} = baP$