Aria Javani

9725303

1:

$y^2 = x^3 + x + 6 \; mod \; 11, K_{prA} = 6, \; K_{pubB} = (5,9)$

$session \; key = K_{prA} K_{pubB} = 6(5,9)$

we should use double and add algorithm to reach 6 in the fastest way

$P \to 2P \to 3P \to 6P$

$P + P = (5,9) + (5,9)$

$P = Q \to s = \frac{3x_1^2+1}{2y_1} \; mod \; 11 = 76(18)^{-1} = 10 \times 8 =$
$80 \; mod \; 11 = 3$

$x_3 = s^2 - x_1 - x_2 = -1 mod 11 = 10$

$y_3 = s(x_1 - x_3) - y_1 = 3 \times 6 - 9 = 9$

$2P = (10,9)$

$3P = 2P + P = (10,9) + (5,9)$

$P \neq Q \to s = \frac{y_2 - y_1}{x_2 - x_1} = 0$

$x_3 = 0 - 10 - 5 = -15 \; mod \; 11 = -4 \; mod \; 11 = 7$

$y_3 = -9 \; mod \; 11 = 2$

$3P = (7,2)$

$6P = 3P + 3P = (7,2) + (7,2)$

$P = Q \rightarrow s = \ s = \frac{3x_1^2+1}{2y_1}\ mod\ 11 = 148(4)^{-1} = 5 \times 3 =$
$15\ mod\ 11 = 4$

$x_3 = 16 - 7 - 7 = 2$

$y_3 = 4(7-2) - 2 = 7$

$6P = (2,7)$

$session\ key = (2,7)$

2.1:

$a = 2, b = 2$

$4a^3 + 27b^2 = 4(2)^3 + 27(2)^2 = 32 + 108 = 140\ mod\ 17 \equiv 4$

2.2:

$(2,7) \neq (5,2) \rightarrow s = \frac{y_2-y_1}{x_2-x_1} mod\ p\ \rightarrow$
$s = (2-7)(5-2)^{-1} mod\ 17 = 12 \times 6 = 72\ mod\ 17 = 4$

$x_3 = s^2 - x_1 - x_2\ mod\ 17 \rightarrow x_3 = 16 - 2 - 5 = 9$

$y_3 = s(x_1 - x_3) - y_1 = 4(2-9) - 7 = 40 - 7 = 16 \rightarrow$

$(x_3, y_3) = (9,16)$

2.3 :

from the book example we know #E=19 now we should calculate upper and lower bounds:

upper bound : $P + 1 + 2\sqrt{P} = 17 + 1 + 2 \times 4.12 = 26.24$

lower bound : $P + 1 - 2\sqrt{P} = 17 + 1 - 2 \times 4.12 = 9.76$

$$9.76 \leq 19 \leq 26.24$$

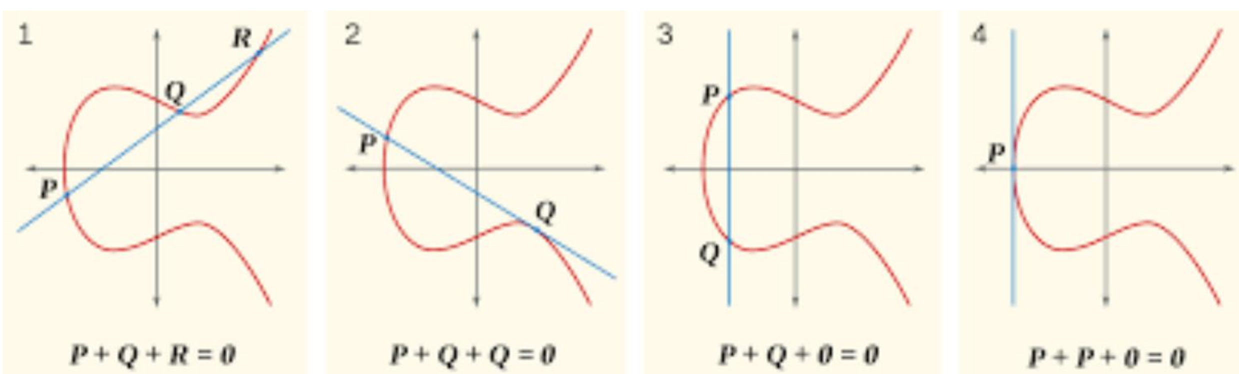
2.4 :

since the group cardinality is 19, $\varphi(19) = 18$ which means all the elements except θ are primitive element.

3.1 :

all the points on x-axis

3.2 :



4 :

$p = 31, \alpha = 3, \beta = 6, x = 10, keys = (17,5)\ and\ (13,5)$

4.1 :

$\alpha^{x} = \alpha^{10} = 3^{10} = 25$

first verification step :

$t = \beta^{r}.r^{s} \ mod \ p$

$t_1 = 6^{17}.17^{5} \ mod \ 31 = 25$

$t_2 = 6^{13}.13^{5} \ mod \ 31 = 5$

$t_1 = \alpha^{x} \ , t_2 \neq \alpha^{x} \rightarrow first \ signature \ is \ valid$

4.2 :

$k_E \in \{0,1, \dots ,31-2\} \ such \ that \ \gcd(k_E, 30) = 1$

so we can choose every number in the given range except 2,3,5,6,10,15 , the overall amount is (29-0)+1-6=24

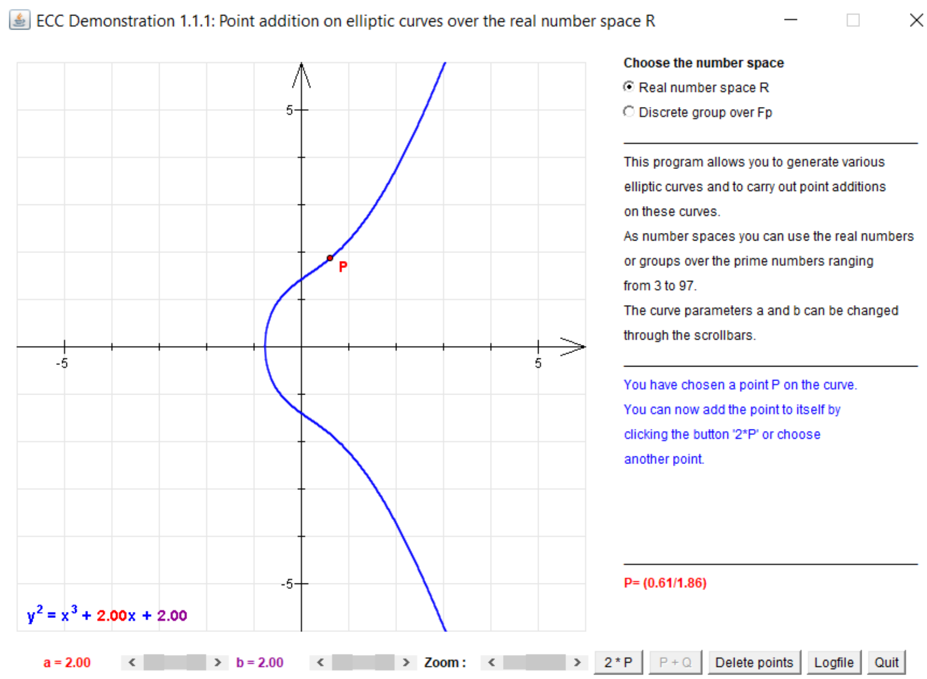
5 :

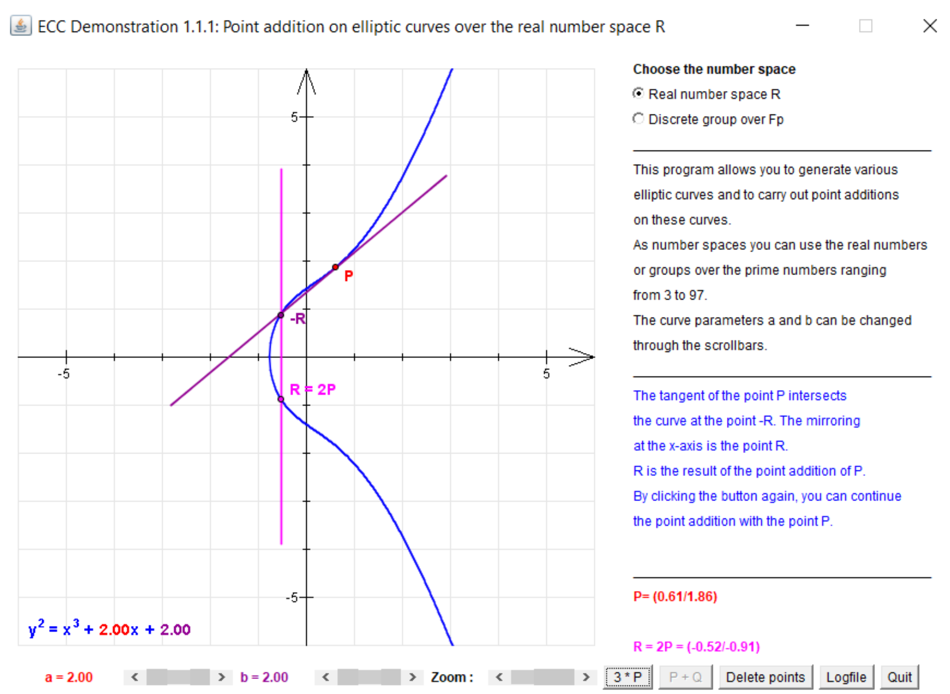
first Oscar receives public key (9797,131) then he chooses a random number smaller that 9797 $, s = 100$ then Oscar computes $x \equiv s^{e} \rightarrow 100^{131} = 9190 \ mod \ 9797$ then Oscar sends (9190,100) to Alice so when Alice checks $x = s^{e}$ she verifies the signature

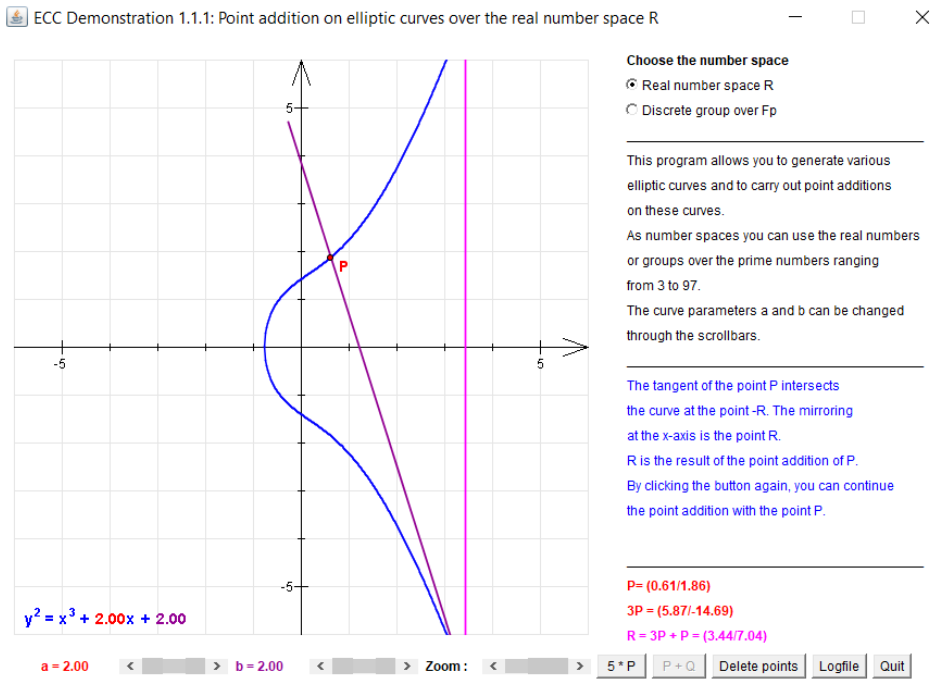
6 :

1.

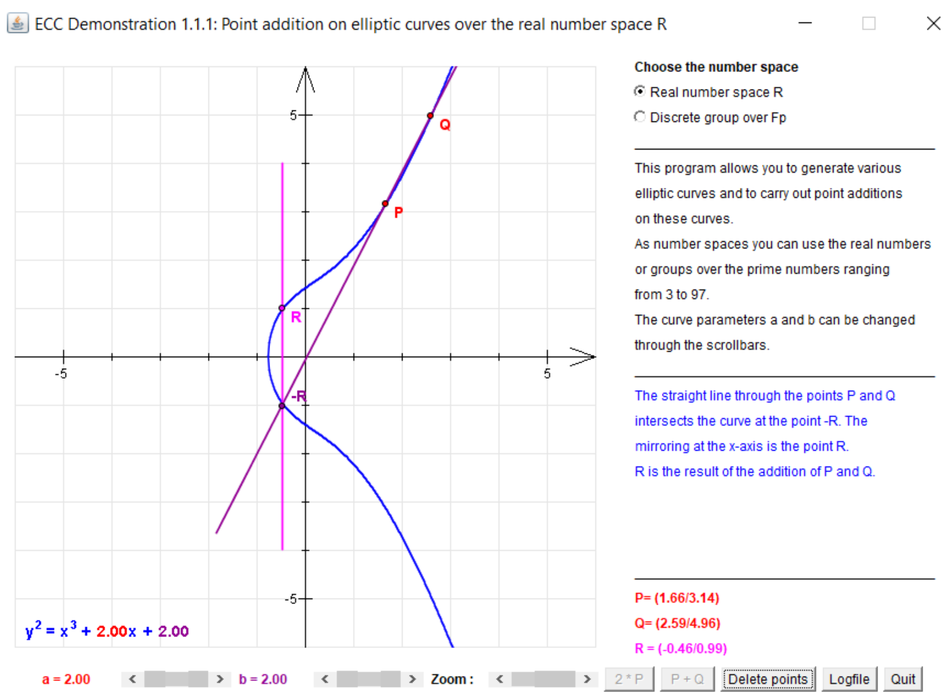
a)


ECC Demonstration 1.1.1: Point addition on elliptic curves over the real number space R
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.
You have chosen a point P on the curve. You can now add the point to itself by clicking the button '2*P' or choose another point.
P= (0.61/1.86)
P
5
-5
-5
5
y2 = x3 + 2.00x + 2.00
a = 2.00
b = 2.00
Zoom :
2 * P
P + Q
Delete points
Logfile
Quit


ECC Demonstration 1.1.1: Point addition on elliptic curves over the real number space R
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= (0.61/1.86)
R = 2P = (-0.52/-0.91)
P
-R
R = 2P
5
-5
-5
5
y2 = x3 + 2.00x + 2.00
a = 2.00
b = 2.00
Zoom :
3 * P
P + Q
Delete points
Logfile
Quit

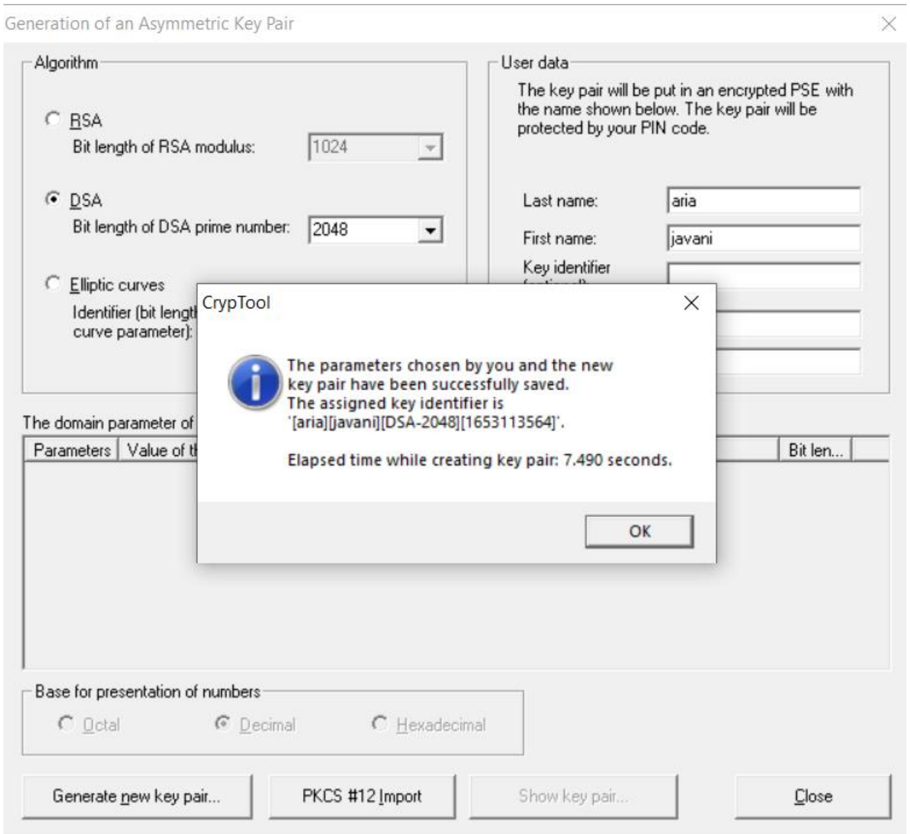

ECC Demonstration 1.1.1: Point addition on elliptic curves over the real number space R
Choose the number space
Real number space R
Discrete group over Fp
This program allows you to generate various elliptic curves and to carry out point additions on these curves.
As number spaces you can use the real 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= (0.61/1.86)
3P = (5.87/-14.69)
R = 3P + P = (3.44/7.04)
P
5
-5
y^2 = x^3 + 2.00x + 2.00
a = 2.00
b = 2.00
Zoom :
5 * P
P + Q
Delete points
Logfile
Quit

b)


ECC Demonstration 1.1.1: Point addition on elliptic curves over the real number space R
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= (1.66/3.14)
Q= (2.59/4.96)
R = (-0.46/0.99)
Q
P
R
-R
5
-5
y^2 = x^3 + 2.00x + 2.00
a = 2.00
b = 2.00
Zoom :
2 * P
P + Q
Delete points
Logfile
Quit

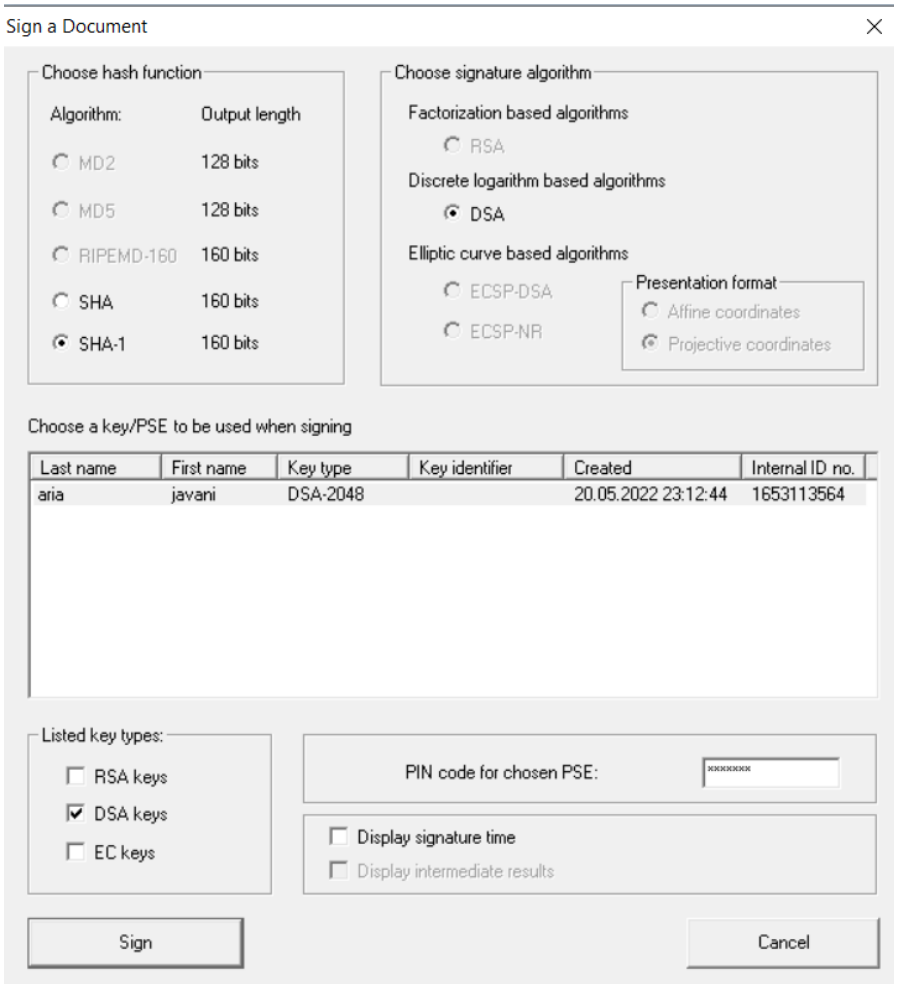
2.

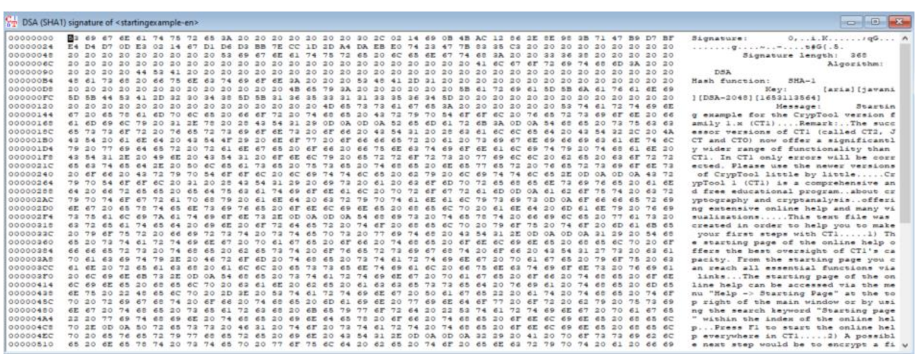
a)



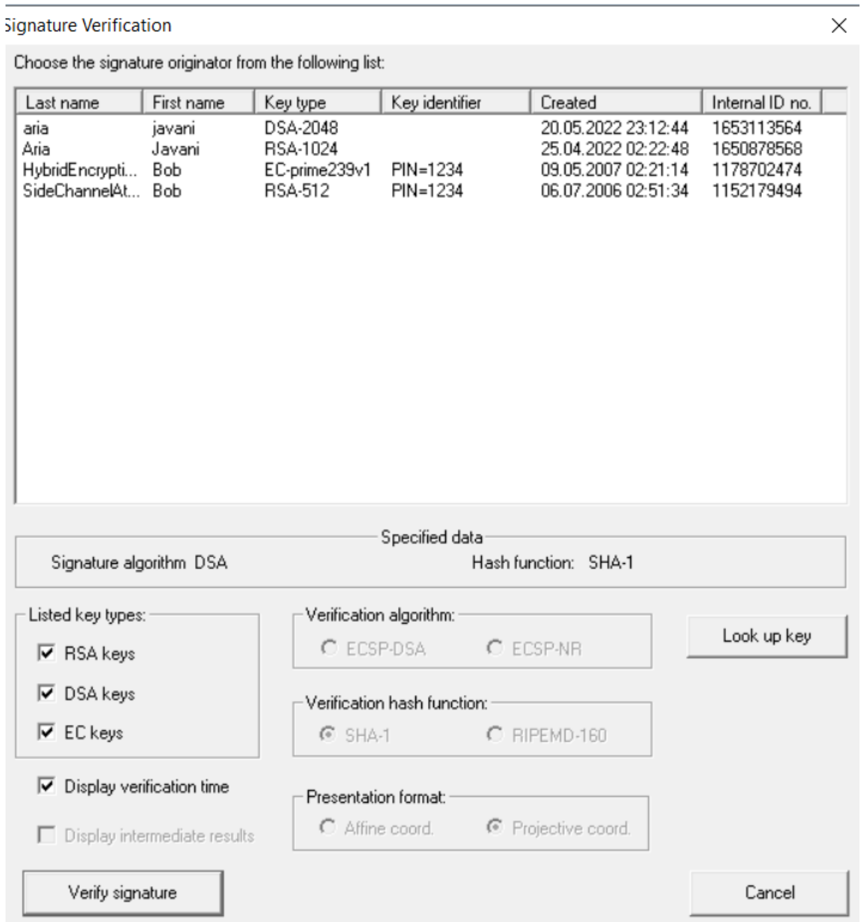
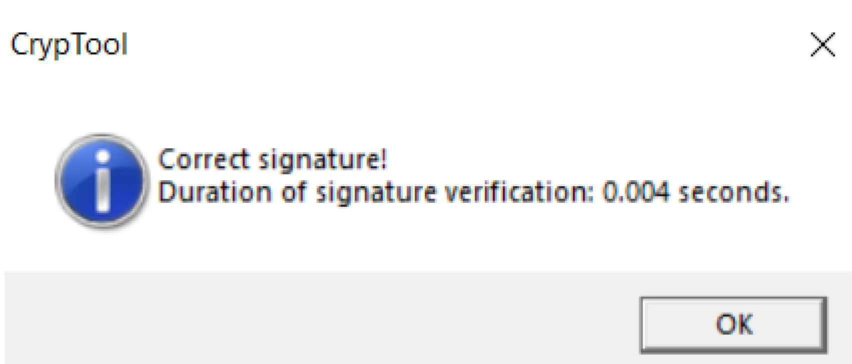
b)

original text and signed text

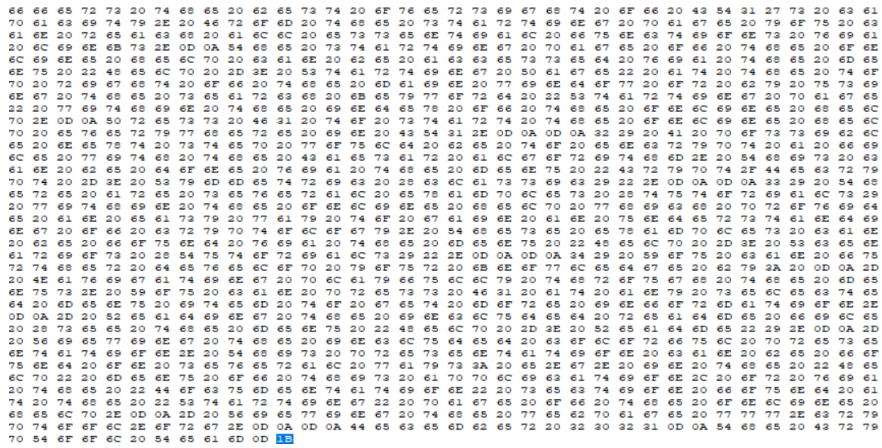

Sign a Document
Choose hash function
Algorithm:
Output length
MD2
128 bits
MD5
128 bits
RIPEMD-160
160 bits
SHA
160 bits
SHA-1
160 bits
Choose signature algorithm
Factorization based algorithms
RSA
Discrete logarithm based algorithms
DSA
Elliptic curve based algorithms
ECSP-DSA
ECSP-NR
Presentation format
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.
aria
javani
DSA-2048
20.05.2022 23:12:44
1653113564
Listed key types:
RSA keys
DSA keys
EC keys
PIN code for chosen PSE:
Display signature time
Display intermediate results
Sign
Cancel

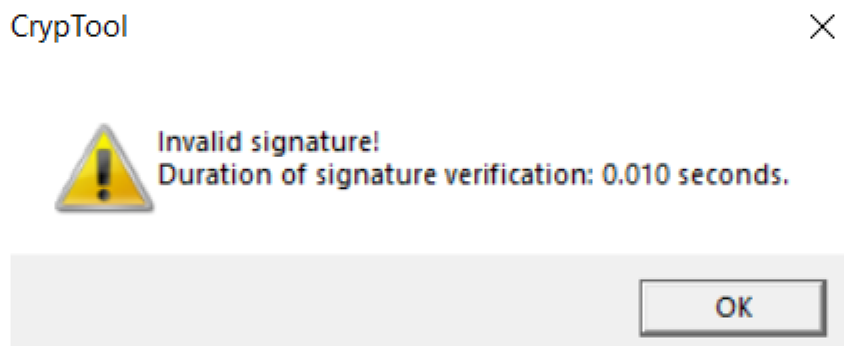


c)


Signature Verification
Choose the signature originator from the following list:
Last name
First name
Key type
Key identifier
Created
Internal ID no.
aria javani DSA-2048 20.05.2022 23:12:44 1653113564
Aria Javani RSA-1024 25.04.2022 02:22:48 1650878568
HybridEncrypti... Bob EC-prime239v1 PIN=1234 09.05.2007 02:21:14 1178702474
SideChannelAt... Bob RSA-512 PIN=1234 06.07.2006 02:51:34 1152179494
Specified data
Signature algorithm DSA
Hash function: SHA-1
Listed key types:
RSA keys
DSA keys
EC keys
Verification algorithm:
ECSP-DSA
ECSP-NR
Look up key
Verification hash function:
SHA-1
RIPEMD-160
Display verification time
Display intermediate results
Presentation format:
Affine coord.
Projective coord.
Verify signature
Cancel

CrypTool
Correct signature!
Duration of signature verification: 0.004 seconds.
OK

d)





since we changed the signature after verifying messages are not identical so this signature doesn't belong to this text.