

Aria Javani

9725303

1:

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

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

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

$$P \rightarrow 2P \rightarrow 3P \rightarrow 6P$$

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

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

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

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

$$2P = (10,9)$$

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

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

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

$$y_3 = -9 \bmod 11 = 2$$

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

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

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

$$x_3 = 16 - 7 - 7 = 2$$

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

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

$$\text{session key} = (2,7)$$

2.1:

$$a = 2, b = 2$$

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

2.2:

$$(2,7) \neq (5,2) \rightarrow s = \frac{y_2-y_1}{x_2-x_1} \bmod p \rightarrow$$

$$s = (2 - 7)(5 - 2)^{-1} \bmod 17 = 12 \times 6 = 72 \bmod 17 = 4$$

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

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

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

2.3 :

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

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

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

$$9.76 \leq 19 \leq 26.24$$

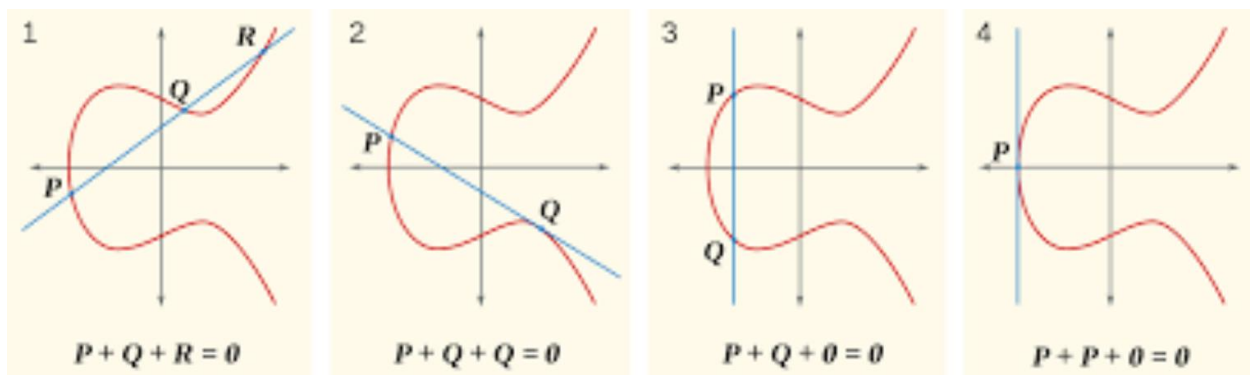
2.4 :

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 :

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

4.1 :

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

first verification step :

$$t = \beta^r \cdot r^s \mod p$$

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

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

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

4.2 :

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

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

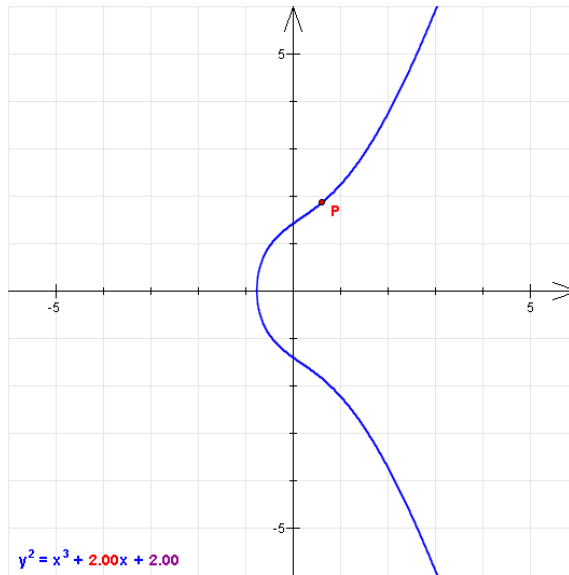
5 :

first Oscar receives public key (9797,131) then he chooses a random number smaller than 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)



a = 2.00



b = 2.00



Zoom :



2 * P



P + Q



Delete points



Logfile



Quit

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.

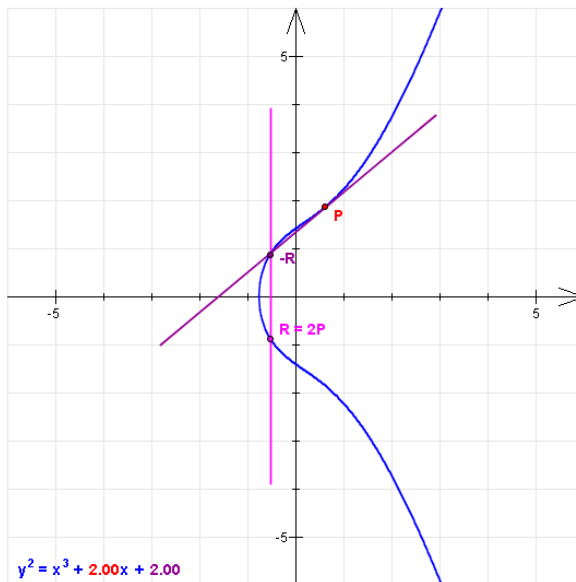
As number spaces you can use the real numbers or groups over the prime numbers ranging from 3 to 97.

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)



a = 2.00



b = 2.00



Zoom :



3 * P



P + Q



Delete points



Logfile



Quit

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.

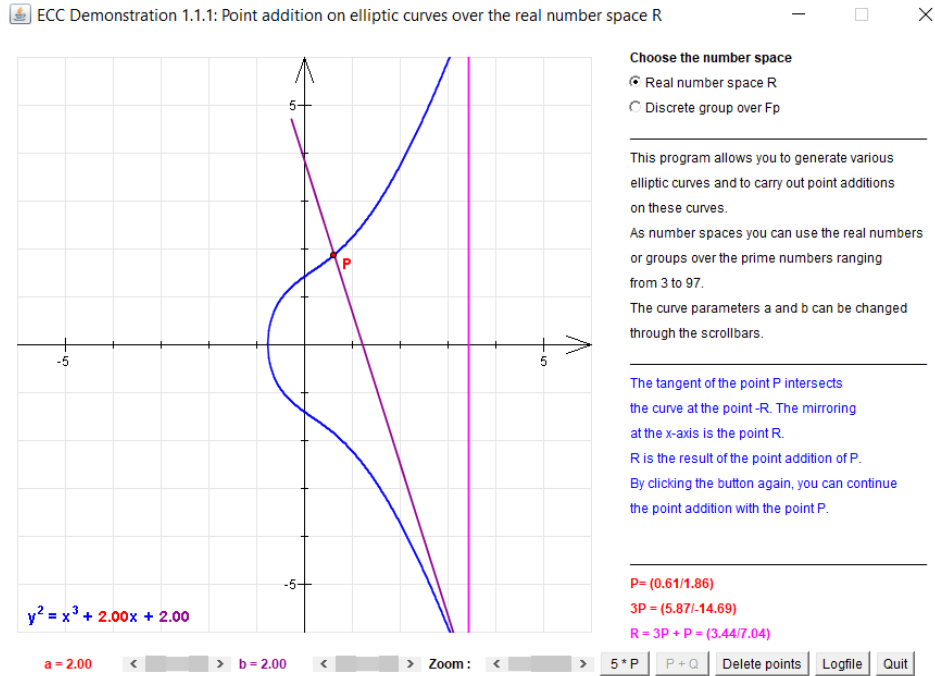
The tangent of the point P intersects the curve at the point -R. The mirroring at the x-axis is the point R.

R is the result of the point addition of P.

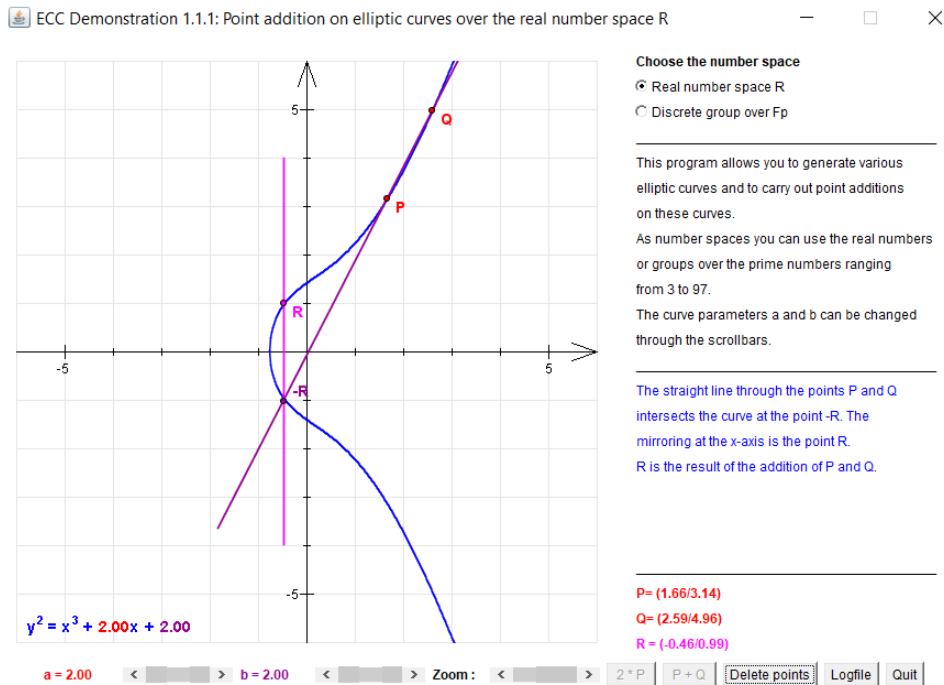
By clicking the button again, you can continue the point addition with the point P.

P = (0.61/1.86)

R = 2P = (-0.52/-0.91)

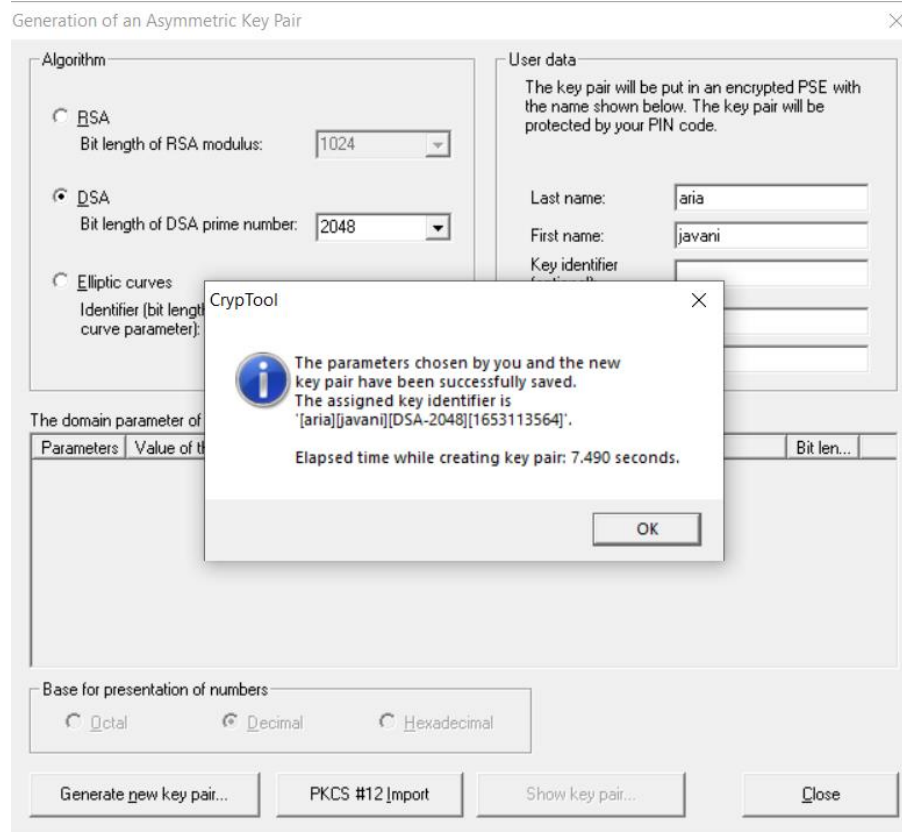


b)



2.

a)



b)

original text and signed text

X

[illegible]

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)

66 66 65 72 73 20 74 65 65 20 62 65 73 74 20 6F 76 65 72 73 69 67 65 74 20 6F 66 20 43 54 31 27 73 20 63 61
70 61 63 69 74 75 2E 20 46 72 6F 6D 20 74 65 65 20 73 74 61 72 74 69 6E 67 20 70 61 67 65 20 79 6F 75 20 63
61 6E 20 72 65 61 63 65 20 61 6C 6C 20 65 73 73 65 6E 74 69 61 6C 20 66 75 6E 63 74 69 6F 6E 73 20 76 69 61
20 6C 69 6E 65 20 65 65 6C 70 20 63 61 6E 20 62 65 20 61 63 63 65 73 73 65 64 20 76 69 61 20 74 65 65 20 6D 65
6E 75 20 22 45 65 6C 70 20 2D 3E 20 53 74 61 72 74 69 6E 67 20 50 61 67 65 22 20 61 74 20 74 65 65 20 74 6F
70 20 72 69 67 65 74 20 6F 66 20 74 65 65 20 6D 61 69 6E 20 77 69 6E 64 6F 77 20 6F 72 20 65 79 20 75 73 69
6E 67 20 74 65 65 20 73 65 61 72 63 65 20 6B 65 79 77 6F 72 64 20 22 53 74 61 72 74 69 6E 67 20 70 61 67 65
22 20 77 69 74 65 69 6E 20 74 65 65 20 69 6E 64 65 78 20 6F 66 20 74 65 65 20 6F 6E 6C 69 6E 65 20 65 65 6C
70 2E 0D 0A 50 72 65 73 73 20 46 31 20 74 6F 20 73 74 61 72 74 20 74 65 65 20 6F 6E 6C 69 6E 65 20 65 65 6C
70 20 65 76 65 72 79 77 65 65 72 65 20 69 6E 20 43 54 31 2E 0D 0A 0D 0A 32 29 20 41 20 70 6F 73 73 69 62 6C
65 20 6E 65 78 74 20 73 74 65 70 20 77 6F 75 6C 64 20 62 65 20 74 6F 20 65 6E 63 72 79 70 74 20 61 20 66 69
6C 65 20 77 69 74 65 20 74 65 65 20 42 61 65 73 61 72 20 61 6C 67 6F 72 69 74 65 6D 2E 20 54 65 69 73 20 63
61 6E 20 62 65 20 64 6F 6E 65 20 76 69 61 20 74 65 65 20 6D 65 6E 75 20 22 43 72 79 70 74 2F 44 65 63 72 79
70 74 20 2D 3E 20 53 79 6D 6D 65 74 72 69 63 20 25 63 6C 61 73 73 69 63 29 22 2E 0D 0A 0D 0A 33 29 20 54 65
65 72 65 20 61 72 65 20 73 65 76 65 72 61 6C 20 65 78 61 6D 70 6C 65 73 20 25 74 75 74 6F 72 69 61 6C 73 29
20 77 69 74 65 69 6E 20 74 65 65 20 6F 6E 6C 69 6E 65 20 65 65 6C 70 20 77 69 69 63 65 20 70 72 6F 76 69 64
65 20 61 6E 20 65 61 73 79 20 77 61 79 20 74 6F 20 67 61 69 6E 20 61 6E 20 75 6E 64 65 72 73 74 61 6E 64 69
6E 67 20 6F 66 20 63 72 79 70 74 6F 6C 6F 67 79 2E 20 54 65 65 73 65 20 45 75 61 6D 70 6C 65 73 20 63 61 6E
20 62 65 20 66 6F 75 6E 64 20 76 69 61 20 74 65 65 20 6D 65 6E 75 20 22 45 65 6C 70 20 2D 3E 20 53 65 65 6E
61 72 69 6F 73 20 25 54 75 74 6F 72 69 61 6C 73 29 22 2E 0D 0A 0D 0A 34 29 20 59 6F 75 20 63 61 6E 20 66 75
72 74 65 65 72 20 64 65 76 65 6C 6F 70 20 79 6F 75 72 20 6B 6E 6F 77 6C 65 64 67 65 20 62 79 2A 20 0D 0A 2D
20 4E 61 76 69 67 61 74 69 65 67 20 70 6C 61 79 66 75 6C 6C 79 20 74 65 72 6F 75 67 65 20 74 65 65 20 6D 65
6E 75 73 2E 20 59 6F 75 20 65 61 6E 20 70 72 65 73 73 20 46 31 20 61 74 20 61 6E 79 20 73 65 6C 65 69 74 65
64 20 6D 65 6E 75 20 69 74 65 6D 20 74 6F 20 67 65 74 20 6D 6F 72 65 20 69 6E 66 6F 72 6D 61 74 69 6F 6E 2E
0D 0A 2D 20 52 65 61 64 69 6E 67 20 74 65 65 20 69 6E 63 6C 75 64 65 64 20 72 65 61 64 6D 65 20 66 69 6C 65
20 25 73 65 65 20 74 65 65 20 6D 65 6E 75 20 22 45 65 6C 70 20 2D 3E 20 52 65 61 64 6D 65 22 29 2E 0D 0A 2D
20 56 69 65 77 69 6E 67 20 74 65 65 20 69 6E 63 6C 75 64 65 64 20 69 6F 6C 6F 72 66 75 6C 20 70 72 65 73 65
6E 74 61 74 69 6F 6E 2E 20 54 65 69 73 20 70 72 65 73 65 6E 74 61 74 69 6F 6E 20 63 61 6E 20 62 65 20 66 6F
75 6E 64 20 6F 6E 20 73 65 76 65 72 61 6C 20 77 61 79 73 3A 20 65 2E 67 2E 20 69 6E 20 74 65 65 20 22 45 65
6C 70 22 20 6D 65 6E 75 20 6F 66 20 74 65 69 73 20 61 70 70 6C 69 69 61 74 69 6F 6E 2C 20 6F 72 20 76 69 61
20 74 65 65 20 22 44 6F 63 75 6D 65 6E 74 61 74 69 6F 6E 22 20 73 65 63 74 69 6F 6E 20 66 6F 75 6E 64 20 61
74 20 74 65 65 20 22 53 74 61 72 74 69 6E 67 22 20 70 61 67 65 20 6F 66 20 74 65 65 20 6F 6E 6C 69 6E 65 20
65 65 6C 70 2E 0D 0A 2D 20 56 69 65 77 69 6E 67 20 74 65 65 20 77 65 62 70 61 67 65 20 77 77 77 2E 63 72 79
70 74 6F 6F 6C 2E 6F 72 67 2E 0D 0A 0D 0A 44 65 63 65 6D 62 65 72 20 32 20 32 31 0D 0A 54 65 65 20 42 72 79
70 54 6F 6F 6C 20 54 65 61 6D 0D

CrypTool



Invalid signature!

Duration of signature verification: 0.010 seconds.

OK

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