

1.

1.1. If we put $a = 2, b = 2$:

$$4 \cdot 2^3 + 27 \cdot 2^2 = 4 \cdot 8 + 27 \cdot 4 = 32 + 108 = 140 \equiv 4 \pmod{17} \neq 0 \pmod{17}$$

1.2. $P = (2, 7)$ and $Q = (5, 2)$

$$l = (y_P - y_Q) / (x_P - x_Q) \pmod{p} = (7 - 2) / (2 - 5) \pmod{17} = 5 / (-3) \pmod{17} = 15.33$$

$$x_R = l^2 - x_P - x_Q \pmod{p} = 235 - 2 - 5 \pmod{17} = 7$$

$$y_R = -y_P + l(x_P - x_R) \pmod{p} = -7 + 15.33 \cdot (2 - 7) \pmod{17} = -83.65 \pmod{17} = 1.35$$

$$\text{so } P + Q = (7, 1.35)$$

$$1.3. \rightarrow 17 + 1 = 2 \sqrt{17} \approx 9.75 \leq 19 \leq 17 + 1 + 2 \sqrt{17} \approx 26.25$$

1.4. An elliptic curve E_K clear over a field k of point not equal to 2 or 3 is the set of explanation (X, Y) belong to k to the equation

$$Y^2 = x^3 + ax + b, \text{ where } a, b \text{ belongs to } K$$

The points on elliptic curve[^] (i.e. a point at infinity) structure a group below a certain addition law.

A primitive point P is only a generator of this collection; every elements of the group can be spoken as $P + P + P + \dots + P$ (k times) for a number of k .

if the elliptic curve has a prime number of points, then all its points (except the point at infinity) are primitive, but in general, the elliptic can or may not have a primitive point.

2. $K = aB = 6 \cdot B = 2(2B + B)$

$$2B = (x_3, y_3) : x_1 = x_2 = 5; \quad y_1 = y_2 = 9$$

$$s = (3x_1^2 + a) \cdot y_1^{-1} = (3 \cdot 25 + 1)(2 \cdot 9)^{-1} = 76 \cdot 18^{-1} \pmod{11}$$

$$s \equiv 10 \cdot 8 = 80 \equiv 3 \pmod{11}$$

$$x_3 = s^2 - x_1 - x_2 = 3^2 - 10 = -1 \equiv 10 \pmod{11}$$

$$y_3 = s(x_1 - x_3) - y_1 = 3(5 - 10) - 9 = -15 - 9 = -24 \equiv 9 \pmod{11}$$

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

$$3B = 2B+B = (x'_3, y'_3) : x_1 = 10, x_2 = 5, y_1 = 9, y_2 = 9$$

$$s = (y_2 - y_1)(x_2 - x_1)^{-1} = 0 \bmod 11$$

$$x'_3 = 0 - x_1 - x_2 = -15 \equiv 7 \bmod 11$$

$$y'_3 = s(x_1 - x_3) - y_1 = -y_1 = -9 \equiv 2 \bmod 11$$

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

$$6B = 2 \cdot 3B = (x''_3, y''_3) : x_1 = x_2 = 7, y_1 = y_2 = 2$$

$$s = (3x_1^2 + a) \cdot y_1^{-1} = (3 \cdot 49 + 1) \cdot 4^{-1} \equiv 5 \cdot 4^{-1} \equiv 5 \cdot 3 = 15 \equiv 4 \bmod 11$$

$$x_3'' = s^2 - x_1 - x_2 = 4^2 - 14 = 16 - 14 = 2 \bmod 11$$

$$y_3'' = s(x_1 - x_3) - y_1 = 4(7 - 2) - 2 = 20 - 2 = 18 \equiv 7 \bmod 11$$

$$6B = (2, 7) \Rightarrow K_{AB} = 2$$

3.

$$3.1. \alpha^x = 3^{10} \equiv 25 \bmod 31$$

$$(17, 5) \rightarrow \gamma = 17, \delta = 5$$

$$t = \beta^\gamma \cdot \gamma^\delta = 6^{17} \cdot 17^5 \equiv 26 \cdot 26 \equiv 25 \bmod 31 \Rightarrow t = \alpha^x \Rightarrow \text{ver}(x, (\gamma, \delta)) = 1$$

$$(13, 5) \rightarrow \gamma = 13, \delta = 5$$

$$t = \beta^\gamma \cdot \gamma^\delta = 6^{13} \cdot 13^5 \equiv 6 \cdot 6 \equiv 36 \bmod 31 = 5 \bmod 31 \Rightarrow t = \alpha^x \Rightarrow \text{ver}(x, (\gamma, \delta)) \neq 1$$

→ As we see, just (17, 5) is valid.

3.2. There are $p - 1 = 30$ different signatures for each message x , because the Elgamal signature scheme is probabilistic.

4. Given the private key as d , to sign message m : $s = \text{Hash}(m)d \bmod n$, signing and decryption are the same mathematical operation in RSA.

5.

5.1.

i. Pin = 9631983

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: Marzieh

First name: Alidadi

Key identifier (optional):

PIN:

PIN verification:

The domain parameters

Parameters Value

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 '[Marzieh][Alidadi][DSA-2048][1622912571]'.
Elapsed time while creating key pair: 15.640 seconds.

OK

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.

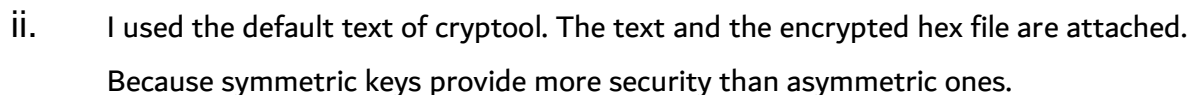
Last name	First name	Key type	Key identifier	Created	Internal ID no.
Alidadi	Marzieh	RSA-1024		17.05.2021 19:03:01	1621261981
HybridEncrypti...	Bob	EC-prime239v1	PIN=1234	09.05.2007 13:51:14	1178702474
Marzieh	Alidadi	DSA-2048		05.06.2021 21:32:51	1622912571
SideChannelAt...	Bob	RSA-512	PIN=1234	06.07.2006 14:21:34	1152179494

Listed key types:

☒ RSA keys
☒ DSA keys
☒ EC keys

Show public parameters... Show all parameters... Show certificate Export PSE (PKCS#12) Delete... Close

i.



iii. It resulted the proper text:

