**Aria Javani**

**9725303**

**1:**

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

**2.1:**

**2.2:**

**2.3 :**

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

upper bound :

lower bound :

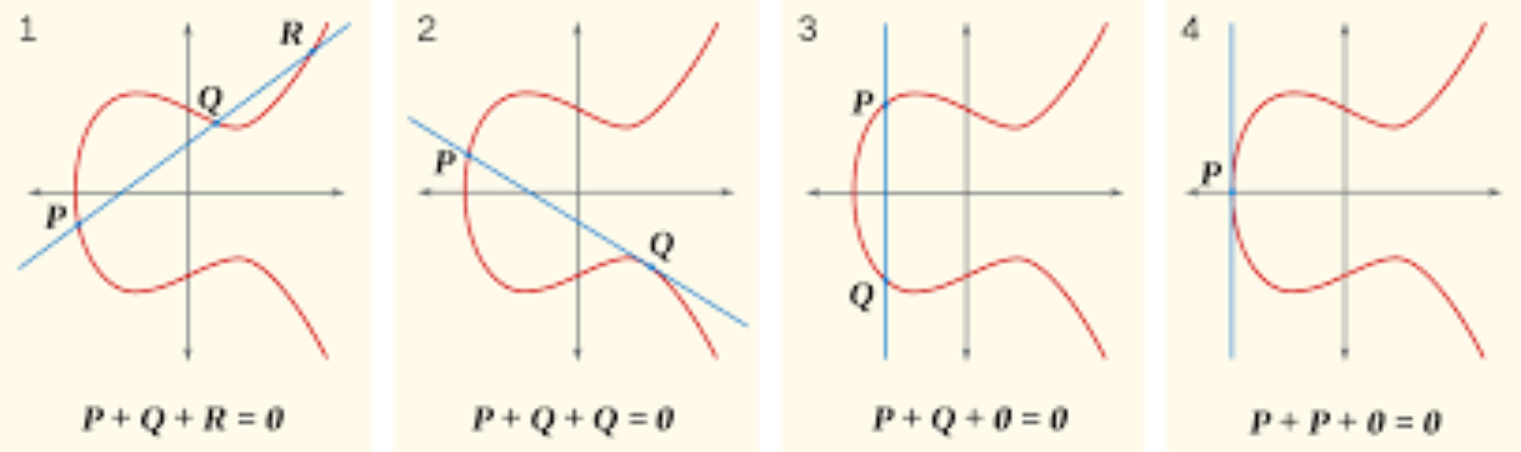
**2.4 :**

since the group cardinality is 19, which means all the elements except are primitive element.

**3.1 :**

all the points on x-axis

**3.2 :**

****

**4 :**

**4.1 :**

first verification step :

**4.2 :**

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

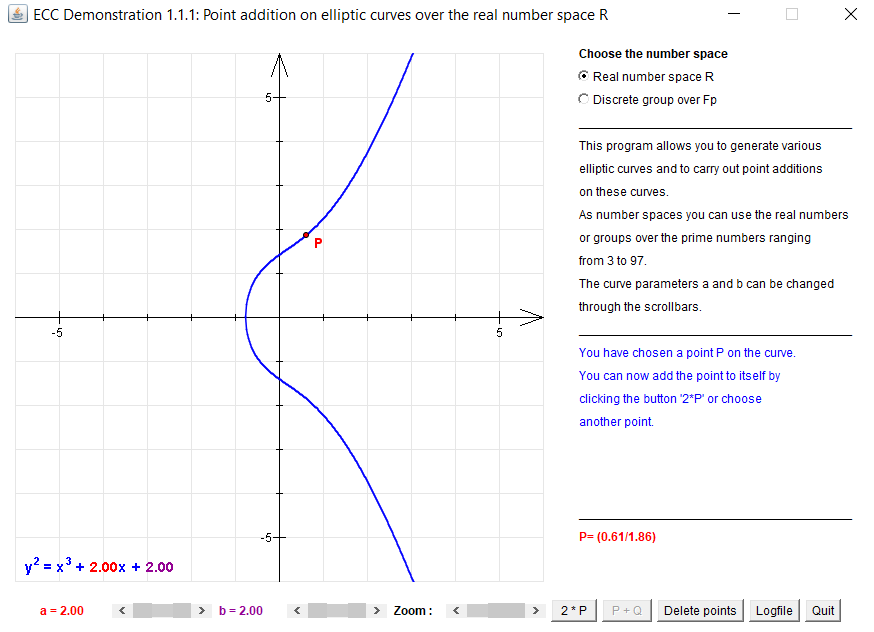
**5 :**

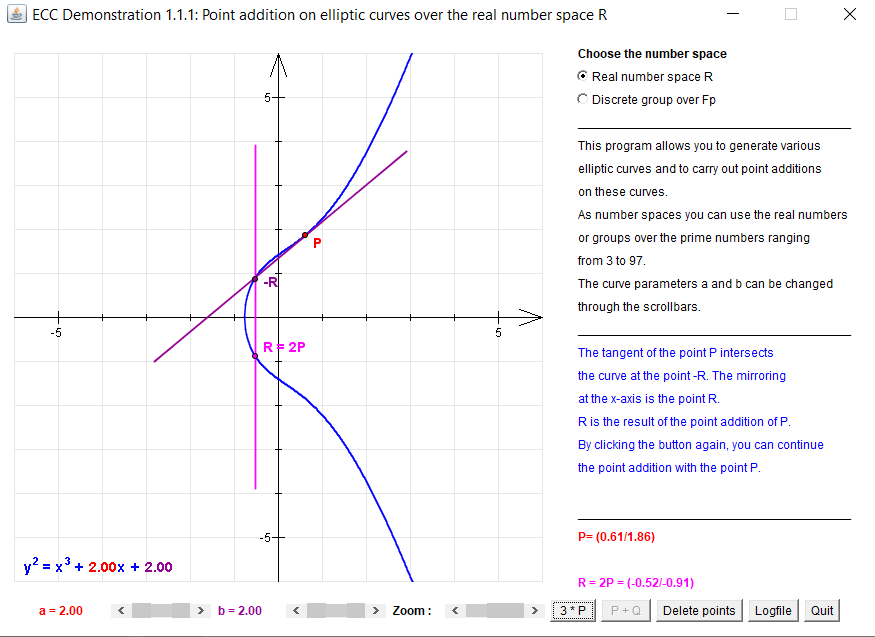
first Oscar receives public key then he chooses a random number smaller that 9797 , then Oscar computes then Oscar sends to Alice so when Alice checks she verifies the signature

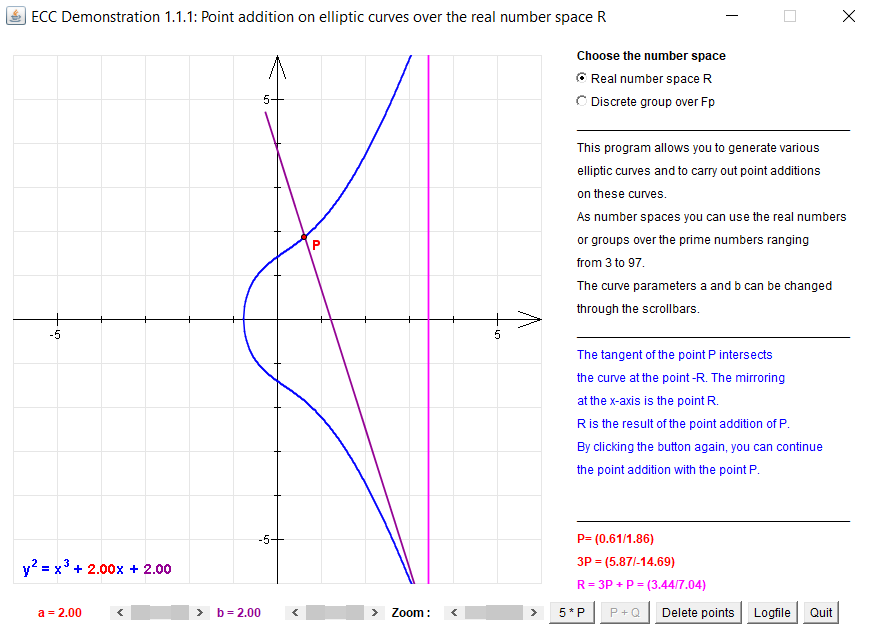
**6 :**

**1.**

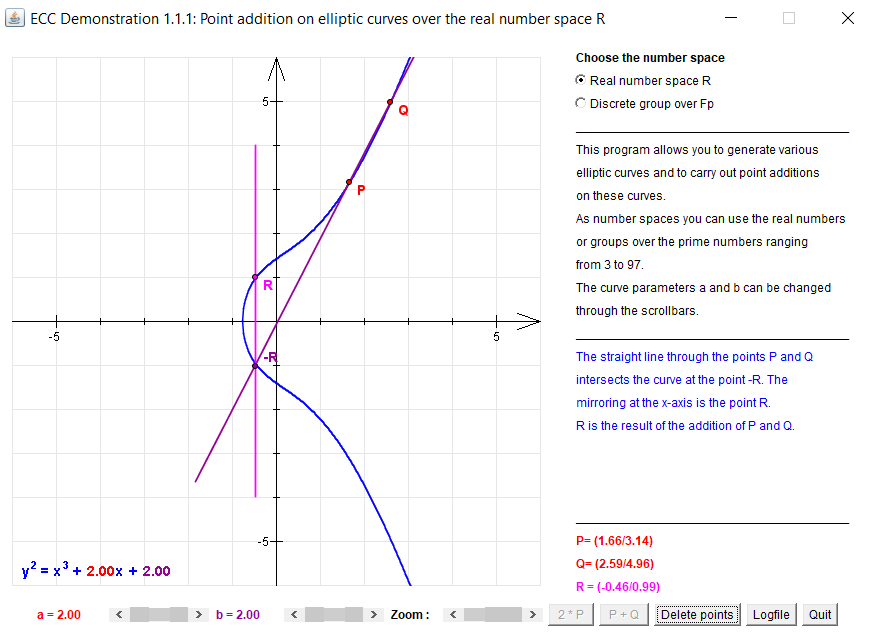
**a)**

****



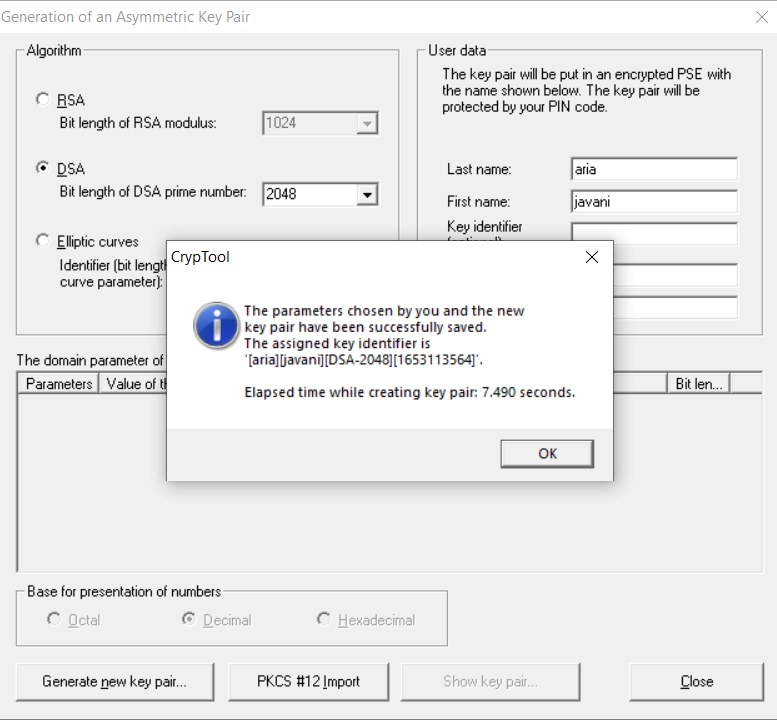


**b)**

****

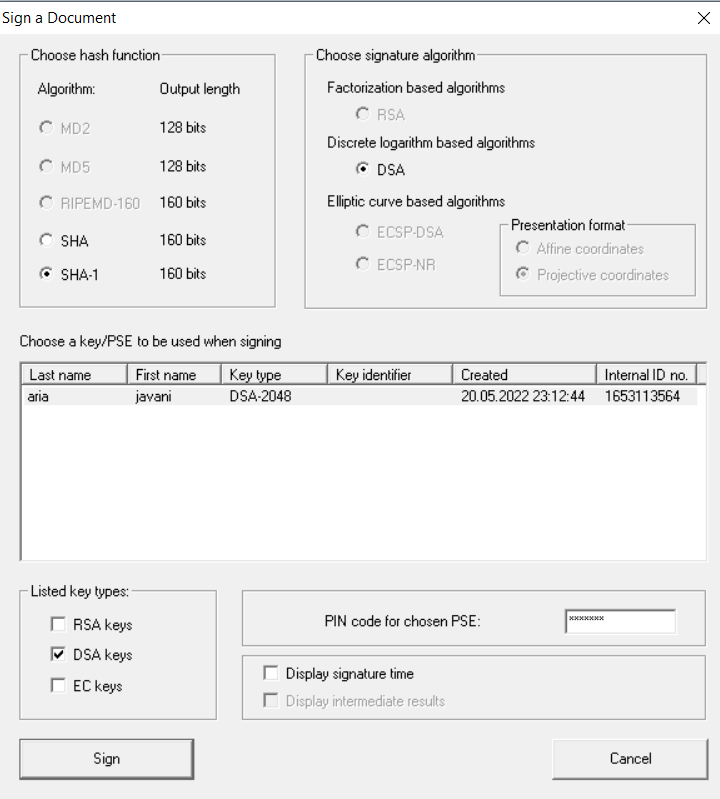
**2.**

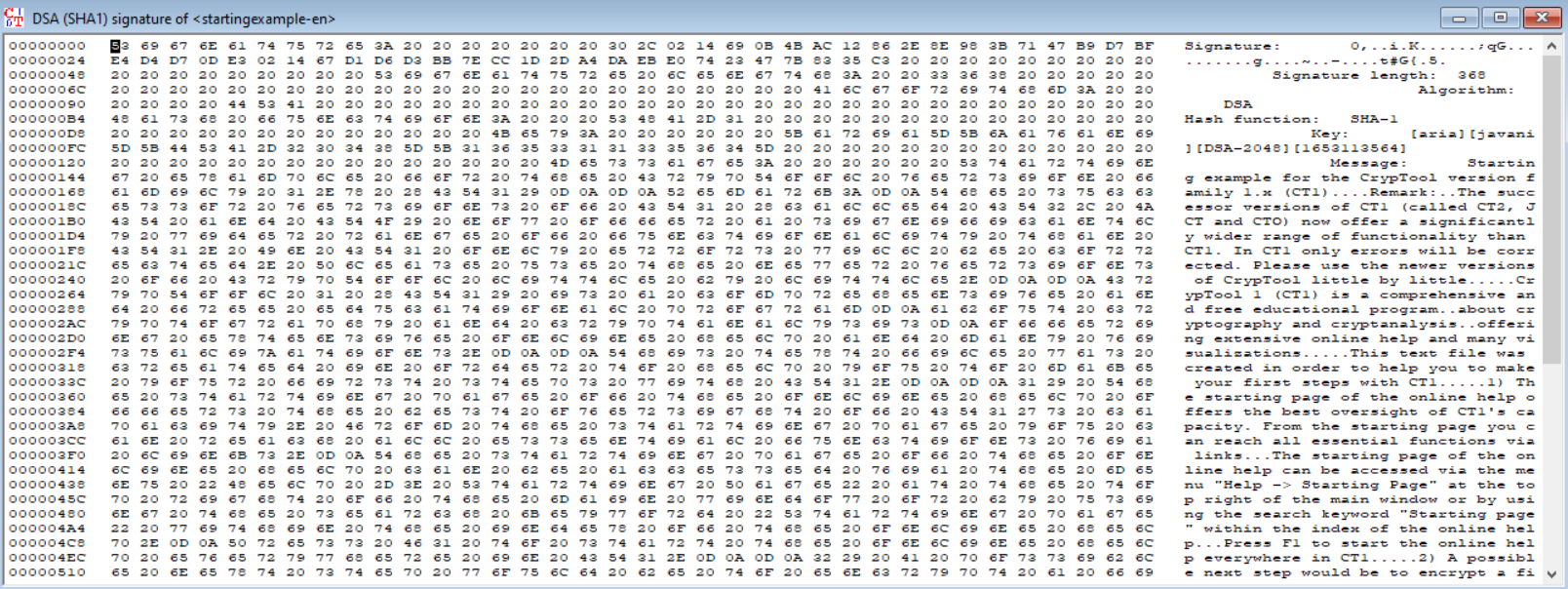
**a)**

****

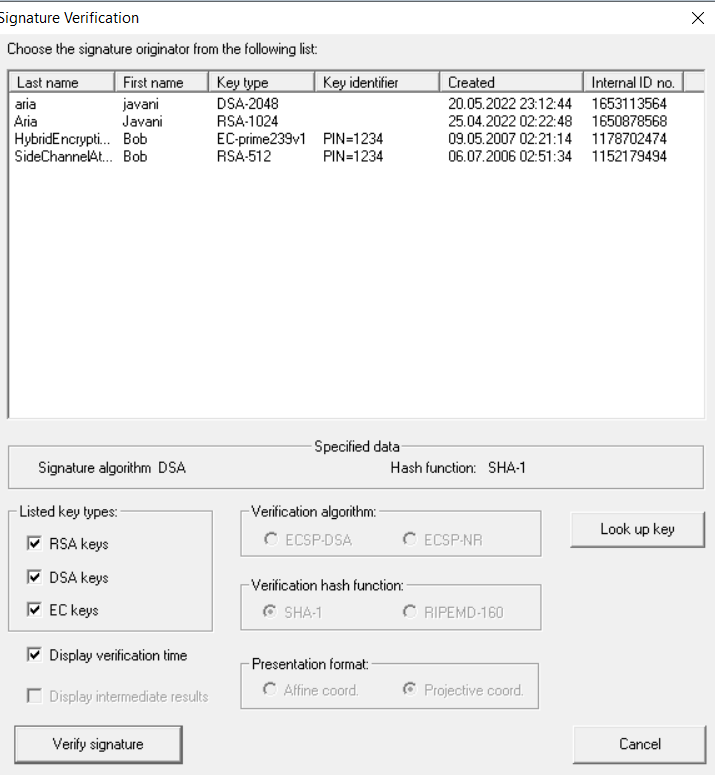
**b)**

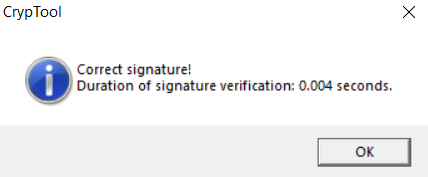
original text and signed text



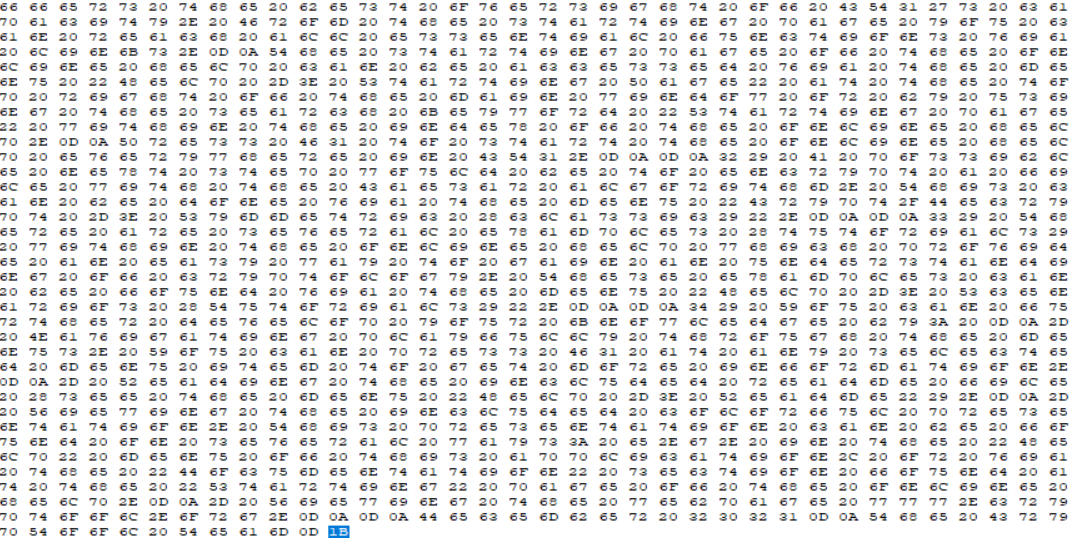


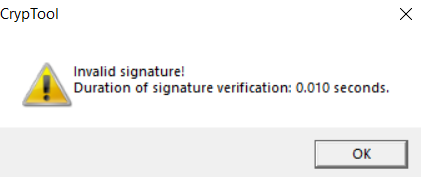
**c)**

****

****

**d)**

****

****

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