«به نام خدا»

تکلیف پنجم – مرضیه علیدادی – 9631983

1.

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

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

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

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

$x_R = l^2 - x_P - x_Q \bmod p = 235 - 2 - 5 \bmod 17 = 7$

$y_R = -y_P + l(x_P - x_R) \bmod p = -7 + 15.33*(2-7) \bmod 17 = -83.65 \bmod 17 = 1.35$

so **P + Q = (7,1.35)**

1.3. → $17+1 = 2\sqrt{17} \approx 9{,}75 \leq 19 \leq 17+1+2\sqrt{17} \approx 26{,}25$

1.4. An elliptic curve EK 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

$Y^2 = x^3+ax+b$, where a, b 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+ . . . +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 ·B = 2(2B+B)

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

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

$s \equiv 10 \cdot 8 = 80 \equiv 3 \bmod 11$

$x_3 = s^2 - x_1 - x_2 = 3^2 - 10 = -1 \equiv 10 \bmod 11$

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

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) → $\gamma = 17, \delta = 5$

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

(13,5) → $\gamma = 13, \delta = 5$

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

➔ 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.

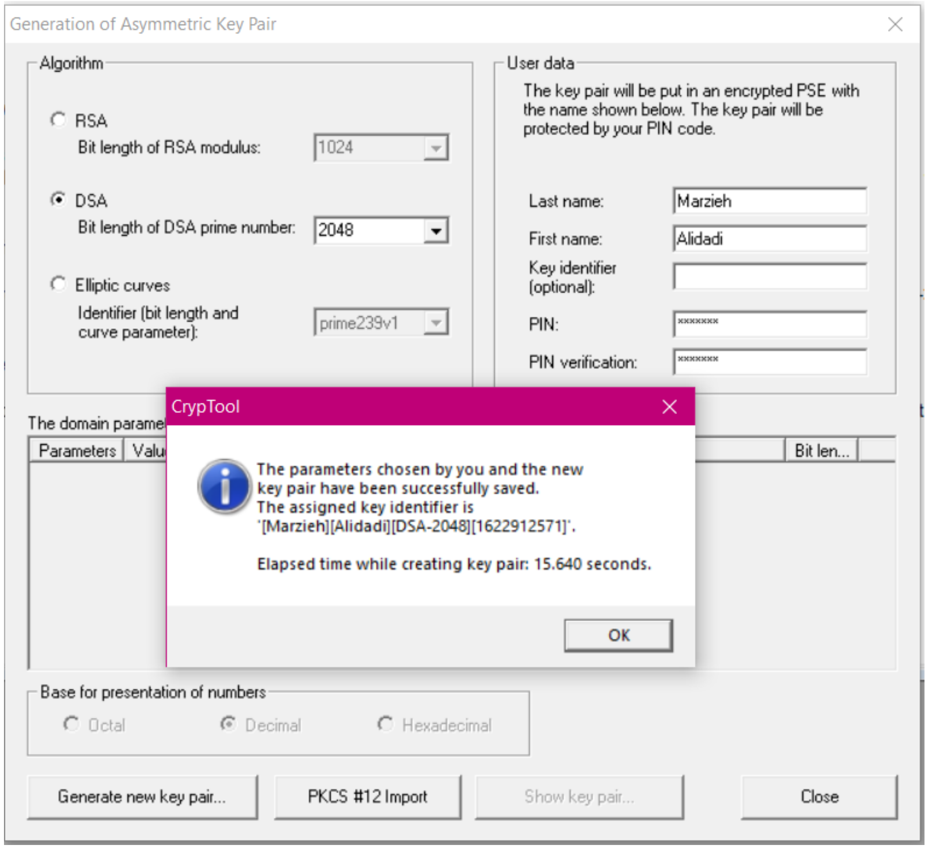
---

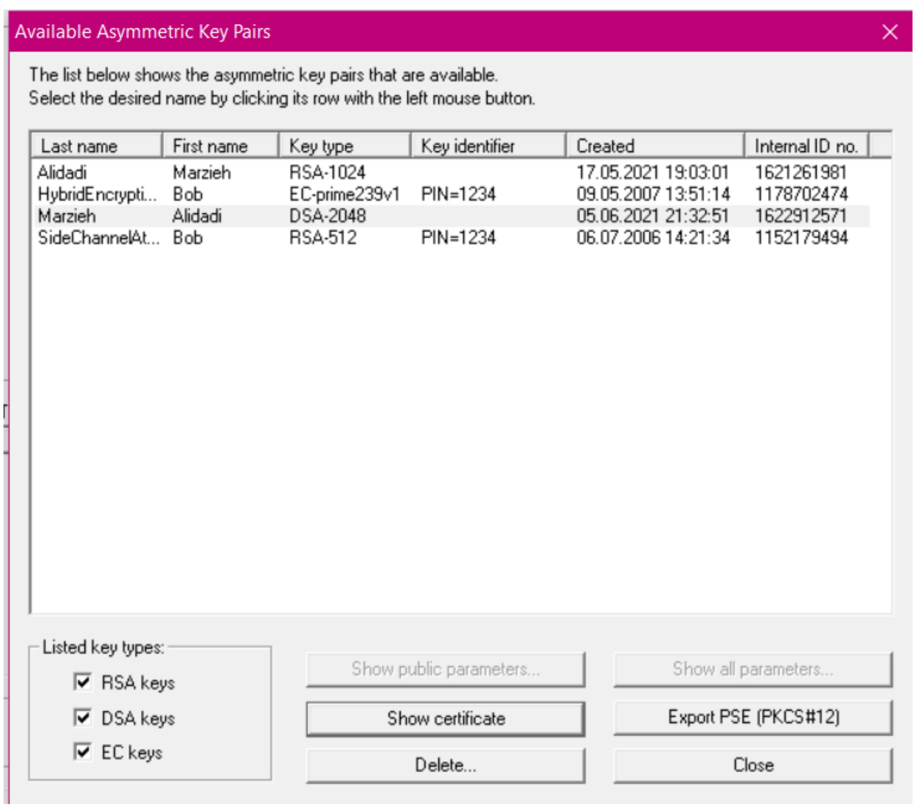
4. Given the private key as d, to sign message m: s= Hash(m)d mod n,
signing and decryption are the same mathematical operation in RSA.

5.

5.1.

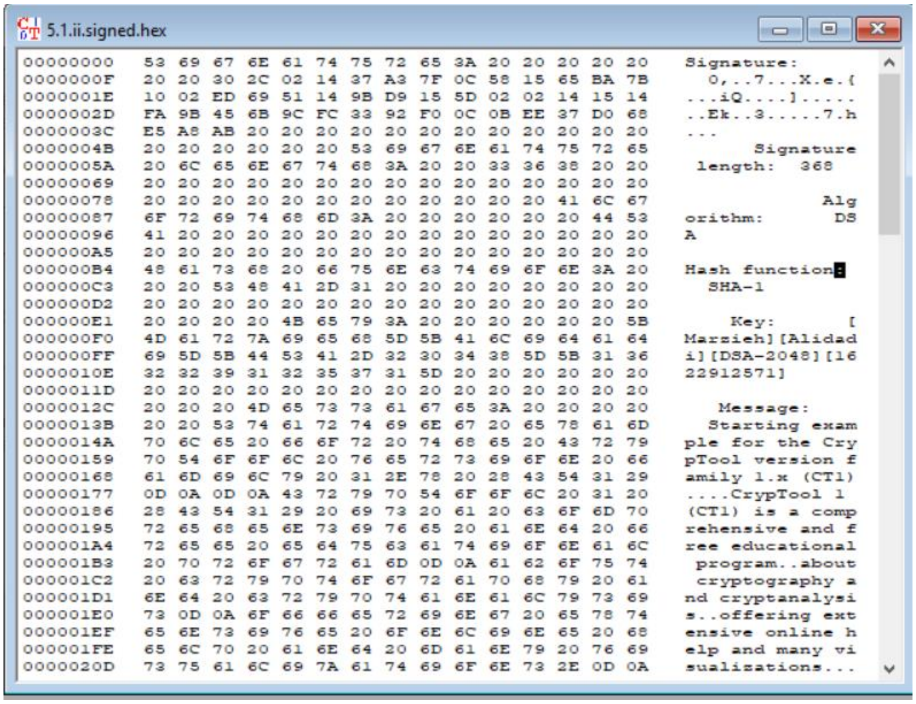
i. Pin = 9631983





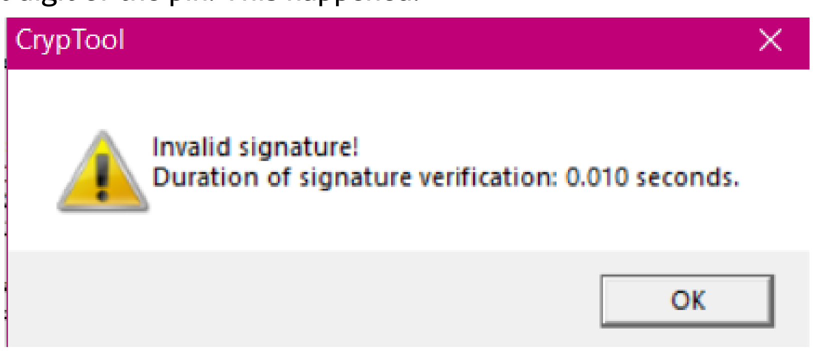
ii. I used the default text of cryptool. The text and the resulting hex file are attached.

The resulting file consists of ‘signature’ , ‘signature length’ , ‘signature algorithm’ , ‘hash function’ , ‘key’ , ‘message’.



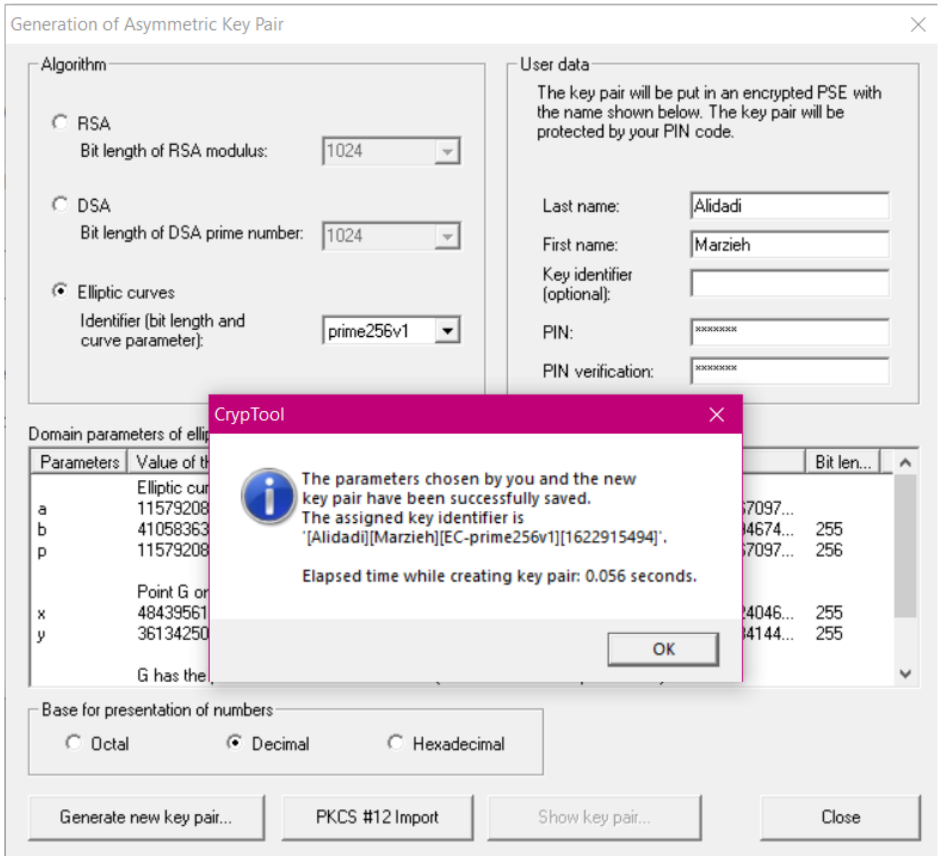
iii.

iv. I changed the last digit of the pin. This happened:

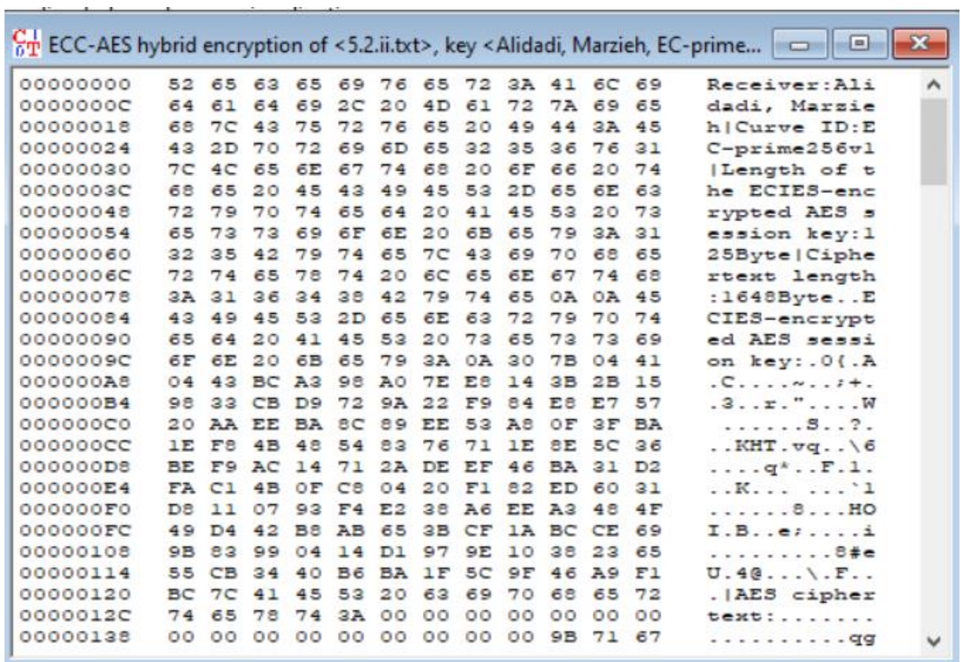


5.2.

i.



ii. I used the default text of cryptool. The text and the encrypted hex file are attached. Because symmetric keys provide more security than asymmetric ones.



iii. It resulted the proper text: