Semih Balki
Yildiz Technical University

semihbalki@sabanciuniv.edu

Assignment 4

BLM 5153 : Fall 2019 : Prof. Koc
Due Saturday, December 28, 2019

Problem - Consider the Weierstrass curve ε: $y^2 = x^3$ - x + 1 in $GF(29)$.
Note that: Point at infinity is represented as ϑ and (0, 0) in the code.

(1) The group order is 37 which is a prime.

(2) All points on the curve are primitive, except ϑ(point at infinity).

(3) Take P = (0, 1) whose order is n = 37. Given the private key d = 25 compute the public key Q = [d]P.

(4) Let the hashed message be h(m) = 10. Compute the signature (r,s) on the hashed message h(m) using the parameters ε, P, n, d.

(5) Verify the signature (r,s) on the message h(m).

Solution
(1) Points of the curve:
1 : [0, 1]
2 : [0, 28]
3 : [1, 1]
4 : [1, 28]
5 : [2, 6]
6 : [2, 23]
7 : [3, 5]
8 : [3, 24]
9 : [5, 11]
10 : [5, 18]
11 : [9, 5]
12 : [9, 24]
13 : [10, 11]
14 : [10, 18]
15 : [11, 4]
16 : [11, 25]

17 : [12, 8]
18 : [12, 21]
19 : [14, 11]
20 : [14, 18]
21 : [17, 5]
22 : [17, 24]
23 : [20, 8]
24 : [20, 21]
25 : [22, 10]
26 : [22, 19]
27 : [23, 9]
28 : [23, 20]
29 : [25, 12]
30 : [25, 17]
31 : [26, 8]
32 : [26, 21]
33 : [27, 13]
34 : [27, 16]
35 : [28, 1]
36 : [28, 28]
37 : [0, 0]

(2)

Primitive points on the curve:
1 : [0, 1]
2 : [0, 28]
3 : [1, 1]
4 : [1, 28]
5 : [2, 6]
6 : [2, 23]
7 : [3, 5]
8 : [3, 24]
9 : [5, 11]
10 : [5, 18]
11 : [9, 5]
12 : [9, 24]
13 : [10, 11]
14 : [10, 18]
15 : [11, 4]
16 : [11, 25]
17 : [12, 8]
18 : [12, 21]
19 : [14, 11]
20 : [14, 18]
21 : [17, 5]
22 : [17, 24]
23 : [20, 8]
24 : [20, 21]
25 : [22, 10]
26 : [22, 19]
27 : [23, 9]
28 : [23, 20]
29 : [25, 12]

30 : [25, 17]
31 : [26, 8]
32 : [26, 21]
33 : [27, 13]
34 : [27, 16]
35 : [28, 1]
36 : [28, 28]

(3) Computing public key:
1 : [0, 1]
2 : [22, 10]
3 : [27, 13]
4 : [9, 24]
5 : [14, 18]
6 : [11, 25]
7 : [23, 20]
8 : [12, 8]
9 : [26, 8]
10 : [2, 23]
11 : [3, 24]
12 : [1, 1]
13 : [28, 28]
14 : [5, 18]
15 : [17, 5]
16 : [25, 17]
17 : [20, 21]
18 : [10, 18]
19 : [10, 11]
20 : [20, 8]
21 : [25, 12]
22 : [17, 24]
23 : [5, 11]
24 : [28, 1]
25 : Q = [1, 28]

(4) To sign message m, A does the following:

- Select a random integer k, 1 ≤ k ≤ n - 1.
  k = 29
- Compute kP = (x_1, y_1) and r = x_1 mod n.
  If r = 0 then go to step 1.
  [29](0, 1) = (12, 21) and r = 12.
- Compute k^{-1} mod n.
  k^{-1} = 23.
- Compute s = k^{-1}(h(m) + d.r) mod n.
  If s = 0 then go to Step 1. s = 26
- The signature for the message m is (r, s). m = (12, 26)

(5) To verify A's signature (r, s) on m, B should do the following:

- Verify that r and s are integers in the interval [1, n - 1].
  (r, s) = (12, 26) and they are in the interval [1, 36].

- Compute w = s^{-1} mod n and h(m). w = 10.
- Compute u_1 = h(m).w (mod n) and u_2 = r.w (mod n).
  u_1 = 10.10 (mod 37) then u_1 = 26.
  u_2 = 12.10 (mod 37) then u_2 = 9.
- Compute u_1.P + u_2.Q = (x_1, y_1) and v = x_1 (mod n).
  [26].(0, 1) + [9].(1, 28) = (12, 21) and v = 12.
- Accept the signature if and only if v = r.
  v = 12 and r = 12 then v = r.
  Therefore, accept the signature.