Anurag Gulavane

Cryptography Assignment 4:

1)

(a) Find any point α on the curve.

For α=(2,6) :

$6^2 \equiv 2^3 + 2 + 7 \bmod 29$

$36 \equiv 15 \bmod 29$

$7 \equiv 7 \bmod 29$

Since the left-hand side is congruent to the right-hand side, α = (2, 6) is a point on the curve.

(b) Compute the coordinates of the points 2α, 3α, 4α, and 5α on the given curve.

For scalar multiplication, we use the double-and-add algorithm.

2α = α + α

3α = 2α+ α

4α = 2(2α)

5α = 4α + α

Let's calculate these:

2α = (2, 6) + (2, 6)
2α = (2, 6) + (2, 6) = (15, 0)\]

3α = (2, 6) + (15, 0)

$3\alpha = (2, 6) + (15, 0) = (8, 7)$

$4\alpha = 2(2\alpha)$

$4\alpha = 2(15, 0)$

$4\alpha = (7, 8)$

$5\alpha = (4, 6) + (15, 0)$

$5\alpha = (4, 6) + (15, 0) = (0, 8)$

(c) Find the coordinates of the points 8α by computing $3\alpha + 5\alpha$ and $4\alpha + 4\alpha$. Verify that you find the same point.

$8\alpha = 3\alpha + 5\alpha$

$8\alpha = (8, 7) + (0, 8)$

$8\alpha = (8, 7) + (0, 8) = (14, 8)$\]

$8\alpha = 4\alpha + 4\alpha$

$8\alpha = (7, 8) + (7, 8)$

$8\alpha = (7, 8) + (7, 8) = (14, 8)$

As expected, both calculations yield the same point (14, 8).

(d) Find the number of points $\|E\|$ of the given curve.

Let's go through the calculation for $\alpha = (2, 6)$:

1. $\alpha = (2, 6)$
2 . $\alpha = (11, 4)$
3 . $\alpha = (15, 1)$

4. α = (17, 7)
5 α = (7, 22)
6 α = (0, 1) - The point at infinity, skip.
7. α = (7, 7)
8 α = (17, 22)
9 α = (15, 28)
10 α = (11, 25)
11 α = (2, 23)
12 α = (2, 23) - The point at infinity, skip.
13 α = (11, 25)
14 α = (15, 28)
15 α = (17, 22)
16 α = (7, 7)
17 α = (0, 1) - The point at infinity, skip.
18 α = (7, 22)
19 α = (17, 7)
20. α = (15, 1)
21. α = (11, 4)
22. α = (2, 6)
23. α = (2, 6) - The point at infinity, skip.
24. α = (11, 4)
25. α = (15, 1)
26. α = (17, 7)
27. α = (7, 22)
28. α = (0, 1) - The point at infinity, skip.

The non-infinity points obtained are:
α = (2, 6)
2 α = (11, 4)
3 α = (15, 1)
4 α = (17, 7)
5 α = (7, 22)
7 α = (7, 7)
8 α = (17, 22)
9 α = (15, 28)
10 α = (11, 25)
14 α = (15, 28)
15 α = (17, 22)
16 α = (7, 7)
18 α = (7, 22)

19 $\alpha = (17, 7)$
20 $\alpha = (15, 1)$
21 $\alpha = (11, 4)$
22 $\alpha = (2, 6)$
24 $\alpha = (11, 4)$
25 $\alpha = (15, 1)$
26 $\alpha = (17, 7)$
27 $\alpha = (7, 22)$

So, there are 20 non-infinity points on the elliptic curve E with the given base point $\alpha = (2, 6)$. Therefore, $|E| = 20$.

2)

Let's go through the steps of Elliptic Curve Diffie-Hellman (ECDH) key exchange for Alice and Bob using the given elliptic curve $E: y^2 \equiv x^3 - x + 188 \mod 751$ and the generator point $\alpha = (0,376)$.

(a) Find the public keys for Alice and Bob.

For Bob (private key $a_B = 5$):

Bob's public key B is computed as $B = a_B \cdot \alpha$.

Perform scalar multiplication using the point multiplication formulas:

m=2y1 3x12 +a mod751

$x^3 = m2 - 2x^1 \mod 751$

$y^3 = m(x^1 - x^3) - y1 \mod 751$

Let $\alpha = (0,376)$ and $a_B = 5$:

$m = 2 \cdot 3763 \cdot 02 + 5 \mod 751 = 703$

$x^3 = 7032 - 2 \cdot 0 \mod 751 = 268$

$y^3 = 703 \cdot (0 - 268) - 376 \mod 751 = 618$

So, Bob's public key B is (268,618).

For Alice (private key $a_A = 3$):

Alice's public key A is computed similarly as $A = a_A \cdot \alpha$.

Perform scalar multiplication with $\alpha = (0,376)$ and aA =3:

$m = 2 \cdot 3763 \cdot 02 + 3 \bmod 751 = 293$

$x^3 = 2932 - 2 \cdot 0 \bmod 751 = 690$

$y^3 = 293 \cdot (0 - 690) - 376 \bmod 751 = 377$

So, Alice's public key A is (690,377).

(b) Continue with the Key Exchange:

Now that Alice and Bob have their public keys, they exchange them over a secure channel. The shared secret key K is then computed by both parties using their private keys and the received public keys.

For Bob: $K_B = a_B \cdot A = 5 \cdot (690,377)$

Perform scalar multiplication for Bob:

$K_B = (429,73)$ For Alice: $K_A = a_A \cdot B = 3 \cdot (268,618)$

Perform scalar multiplication for Alice:

$K_A = (429,73)$
Now, both Alice and Bob have the same shared secret key $K = (429,73)$.

This shared secret can be used as a symmetric key for encrypting their communication.

3)

```
, e, m):
utes b^e mod m using the square and multiply algorithm"""
 1
xp = bin(e)[2:][::-1]  # Convert exponent to binary and reverse it
inary representation of the exponent:", binary_exp)

in binary_exp:
lt = (result ** 2) % m
t("Square step:", result)

it == '1':
result = (result * b) % m
print("Multiply step:", result)

esult

(a)

84723247

_pow(a1, b1, N1)
sult for (a): {a1}^{b1} mod {N1} =", result1)

(b)
55683
582
72542
_pow(a2, b2, N2)
sult for (b): {a2}^{b2} mod {N2} =", result2)
```

```
sentation of the exponent: 1111010001111010000000000010000000110000111111 0011
 1
p: 235973
 575185
p: 207017
 120457
p: 542657
 563089
p: 486485
 201853
 40321
p: 277553
 348385
 141145
 372829
 286549
p: 556673
 73609
p: 355325
 282769
p: 169601
 37825
p: 427901
```

```
: 250009
: 301765
ep: 235241
: 138097
: 546085
: 253
: 64009
: 38053
: 582373
: 531469
: 158005
: 451837
: 466201
: 143893
ep: 256637
: 434569
: 526453
: 542929
: 397177
: 461281
: 569797
: 506893
: 23713
ep: 267377
: 287053
ep: 374729
: 56977
: 567373
: 523177
: 447925
: 250009
ep: 318281
: 88729
ep: 151961
: 117205
ep: 382037
: 537541
ep: 450581
: 348037
ep: 547097
: 424141
ep: 516101
: 535777
: 351157
: 192805
ep: 532985
: 14893
ep: 531977

(a): 235973^456872884723247 mod 583884 = 531977
esentation of the exponent: 011101011101110101101010101001
: 1
: 1
ep: 984327455683
```

```
ep: 984327455683
: 321440293911
ep: 461523226589
: 103819200519
ep: 155280334997
: 733774440559
: 553009469965
ep: 105765974697
: 360887043615
: 899663170239
ep: 73785395935
: 970707430957
ep: 33338208007
: 595201718299
ep: 67510627193
: 437964051103
: 535957186945
ep: 539615816229
: 475145333003
ep: 424174070587
: 93165829463
ep: 871174696515
: 145848987841
: 98651473267
ep: 829725592477
: 878458113989
: 585497156475
ep: 155443245989
: 481570265381
ep: 681846537233
: 380432919141
: 441812516027
ep: 223305658105
: 621932683873
ep: 121573100775
: 678106965911
: 583387656691
ep: 595578433743
: 841982896665
: 441172728539
ep: 125065039835
: 660430054345
: 738143220291
ep: 144280940463
: 933446337373
: 614664584063
: 889710301599
ep: 497263821157

(b): 984327455683^1253489582 mod 994348472542 = 497263821157
```

Caption