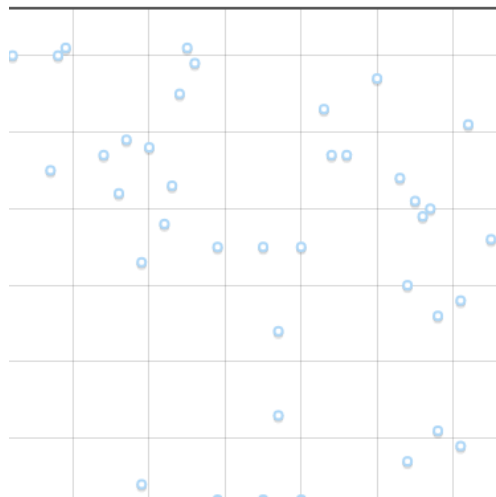


ECC Example with the Calculator.

Use <https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/modk-mul.html>. Be sure you are on the \mathbb{F}_p multiplication page. For this example, we will use the page default settings. Our curve will be $y^2 = x^3 + 2x + 3$ ($a = 2$ and $b = 3$), and our modulus/field will be 97. Our base point will be $P: (3, 6)$. Note that it is not a secure example, as the subgroup only has 5 points.

Elliptic Curve scalar multiplication (\mathbb{F}_p)

\mathbb{R} ADDITION MULTIPLICATION \mathbb{F}_p ADDITION MULTIPLICATION



Curve: a 2 b 3
Field: p 97
n: n 2
P: x 3 y 6
 $Q = n \cdot P$: x 80 y 10

Scalar multiplication over the elliptic curve $y^2 = x^3 + 2x + 3$ in \mathbb{F}_{97} .
The curve has 100 points (including the point at infinity).
The subgroup generated by P has 5 points.

So far, we have selected the public information.

Curve $y^2 = x^3 + 2x + 3$ Modulus 97

P 3, 6

Note: The subgroup only has 5 points, so it is not a great choice. We will use it anyway.

Alice's Public Key

Let's say that Alice selects 9 as her private key, a . She puts 9 into the n : box in the calculator to compute $9 \cdot P$.



Curve: a 2 b 3
Field: p 97
n: n 9
P: x 3 y 6
 $Q = n \cdot P$: x 3 y 91

Scalar multiplication over the elliptic curve $y^2 = x^3 + 2x + 3$ in \mathbb{F}_{97} .
The curve has 100 points (including the point at infinity).
The subgroup generated by P has 5 points.

The result is that her public key is (3, 91) which she gives to Bob.

Alice

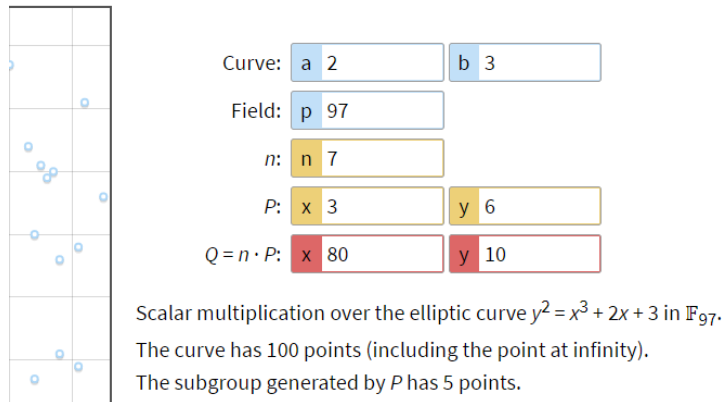
Select a 9

Compute A 3, 91 $A = aP$

Give A to Bob

Bob's Public Key

Let's say that Bob selects 7 as his private key, b. He puts 7 into the n: box in the calculator to compute $7 \cdot P$



The result is that his public key is (80, 10), which he gives to Alice.

Bob

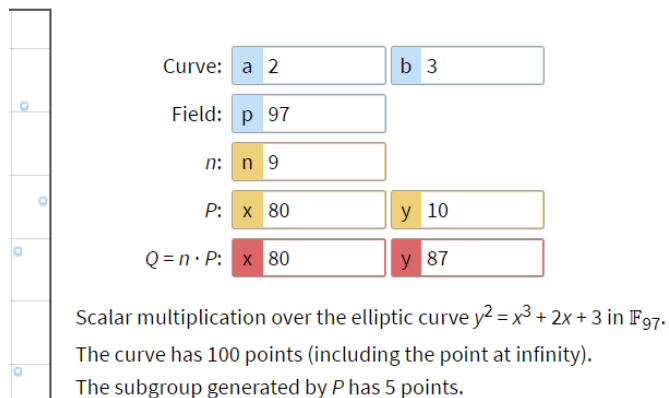
Select b 7

Compute B 80, 10 $B = bP$

Give B to Alice

Alice computes the shared key


Alice puts her private key, 9, in the n: box. She puts Bob's public key (80, 10) in the box for P:



The result is (80, 87), so she uses the X coordinate 80 as the shared key.

Bob computes the shared key

Bob puts his private key, 7, in the n: box. He puts Alice's public key (3, 91) in the box for P:



Curve: a 2 b 3

Field: p 97

n: n 7

P: x 3 y 91

$Q = n \cdot P$: x 80 y 87

Scalar multiplication over the elliptic curve $y^2 = x^3 + 2x + 3$ in \mathbb{F}_{97} .
The curve has 100 points (including the point at infinity).
The subgroup generated by P has 5 points.

Bob also gets the result (80, 87), and uses 80 as the shared key.

Notes

First, this example only has 5 possible results. You can see that by starting n : at 1 and just incrementing it. When you get to $n=5$, you will get the point at infinity (zero). After that, it will repeat. This is a poor choice of curve and base point.

For the large numbers used in the real world, the process of calculating the number of points in the subgroup is not simple. This is another reason why we use curves developed by cryptographers.

https://en.wikipedia.org/wiki/Counting_points_on_elliptic_curves

Since Alice's private key is 9 and Bob's is 7, the result is that they both effectively multiply the base point by $9 * 7 = 63$. Since our subgroup size is 5, $63 \bmod 5 = 3$ gives the same result.