

Cryptography Homework 7: Elliptic Curve Diffie-Hellman Key Exchange (ECDH)

A simple key exchange

Use Andrea's [calculator for EC multiplication over a finite field](#) and select the curve $y^2 = x^3 + 5x + 3$ with a modulus, p , of 97. Together, select a point that will be the base point, P . The curve, modulus, and base point will be public knowledge. Record them.

Individually, each partner should select a number for n that is greater than 1 and less than 91 to be their private key. Use the calculator to determine the coordinates of their public key ($Q = n \cdot P$ in the calculator. (The entire public key is the curve, p , P , and the coordinates Q that you computed.)

Exchange public keys with your partner. Compute the shared key by putting your partner's public coordinates into P , and your private number into n . The value of Q in the calculator is your shared session key and should be the same as the value your partner gets.

Our modulus is 97. How many bits of security do we have (i.e., how many bits does it take to represent 97)? Our shared key x coordinate can be represented by that many bits, as can our y coordinate. Can we double the security of our key by concatenating x and y to double the number of bits? Why or why not? ([Hand in 1](#))

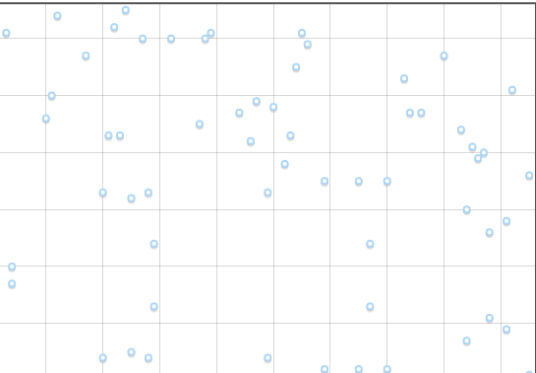
Sample Answer

curve $y^2 = x^3 + 5x + 3$ with a modulus, p , of 97

Select base point--I just plugged different values in for the X coordinate of P until the subgroup had a reasonable number of points--better than 5, and the max possible is 96. I happened to get 50.

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 12 y 3

$Q = n \cdot P$: x 24 y 2

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 50 points.

Alice select private key, computes public key

Alice chooses $n = 5$, and puts that into n . P holds the base point $(12, 3)$ and the public key is $Q = (29, 43)$. Instead of doing $A = \alpha a$ as we did in straight Diffie-Hellman, we do $Q = n \circ P$.

Curve: a 2 b 3

Field: p 97

n: n 5

P: x 12 y 3

Q = n · P: x 29 y 43

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 50 points.

Alice Public key is the point (29, 43), and her private key is $n = 5$.

Bob selects private key, computes public key

Bob chooses $n = 24$ for his private key and puts that into the calculator. The base point is the same (12, 3) that Alice used. The calculator gives him his public key for $Q = 24 \circ P = (74, 77)$.

Curve: a 2 b 3

Field: p 97

n: n 24

P: x 12 y 3

Q = n · P: x 74 y 77

Bob's Public key is the point (74, 77) and his Private key is $n = 24$.

Alice computes shared key

Now they compute the shared secret. Alice puts Bob's public key (74, 77) into P and her private key, 5, into n. The result is $Q = (80, 87)$

Curve: a 2 b 3

Field: p 97

n: n 5

P: x 74 y 77

Q = n · P: x 80 y 87

Bob computes shared key

Bob puts Alice's public key (29, 43) into P , and his private key, 24, into n . The result is $Q = (80, 87)$, the same as Alice's result.

Curve:	a	2	b	3
Field:	p	97		
n:	n	24		
P:	x	29	y	43
$Q = n \cdot P$:	x	80	y	87

Effectively, they both did the operation on the base point 29 times. Alice did it 5 times with her public key and gave the result to Bob. Bob did the operation 24 more times for a total 29, and got the result (80, 87). Going the other way, Bob did the operation 24 times with his public key and gave the result to Alice. Alice did the operation 5 more times (her private key) for a total of 29, with the same result as Bob, (80, 87). They could use 80 as their shared key.

Note that Eve knows the curve and the base point, (12, 3) in this case. She does not know the private keys. To break the encryption, she would have to calculate either Alice or Bob's private key. For example, she would have to take Alice's public key (29, 43) and figure out that Alice had used $n = 5$ on the base point to get (29, 43). That isn't hard with the small numbers we are using. What if the numbers were 2048 bits long, and the number of points generated by the subgroup was 224 bits long? That would be much harder.

Subgroups

When cryptographers select a curve and modulus, they like the number of points on the curve to be a prime number, or at least have large prime numbers as factors. If the number of points is factorable, the field we are using will contain subgroups. Each subgroup will contain the same number of points as the factors of the number. For example, if the number of points is 30, there will be subgroups with 2, 3, 5, 6, 10, 15, and 30. If the base point you select is in a small subgroup, your security is weakened.

Set your calculator to the curve $y^2 = x^3 + x + 2$, with modulus $p = 97$. How many points are on the curve? If you experiment with the calculator by using different coordinates for P , the largest number of points on the curve you can get is 104.

Curve:	a	1	b	2
Field:	p	97		
n:	n	24		
P:	x	4	y	19
$Q = n \cdot P$:	x	46	y	44

Scalar multiplication over the elliptic curve $y^2 = x^3 + 1x + 2$ in \mathbb{F}_{97} .

The curve has 104 points (including the point at infinity).

The subgroup generated by P has 104 points.

What are the factors of that number? (Hand in 2) Experiment with the following base points:

Point	Points on the curve (Points generated)
(1, 2)	4
(4, 19)	104
(15,26)	52
(26,12)	13

Which one provides the best security? Which one provides the worst security? (Hand in 3) The point (4, 19) generates the largest subgroup and is most secure. The point (1, 2) generates the smallest subgroup and is least secure.

The problem of subgroups is common to all encryption that uses finite fields (i.e., most of them), not just ECC.

Choose your own

With your partner, choose a curve, modulus, and base point that gives you a group or subgroup with more than 200 points. If the group has a prime number of points you don't have to be so careful about your selection of a base point.

Hand in

- 1) Does using both the X and Y coordinates of the shared key increase security? Why or why not?
If you know the X coordinate, there are at most two Y coordinates that will work. So, you don't get much increase in security.
- 2) How many points are on the curve $y^2 = x^3 + x + 2$, with modulus $p = 97$? What are the factors of that number?
There are 104 points on the curve, which has factors 1, 2, 4, 8, 13, 26, & 52. There for there is one subgroup with size 1, one with size 2, and so on, up to 52.
- 3) Which point provides the best security?
The point (4, 19) has the largest subgroup (size 104) and is most secure
- 4) From the Choose your own paragraph, submit the curve, modulus, base point, and number of points in the subgroup.
Similar to Sample Answer, above, but with numbers of the students' choosing. This would be a great choice since it has 199 points, which is a prime number.

Curve: a 4 b 1

Field: p 211

n: n 13

P: x 0 y 1

$Q = n \cdot P$: x 178 y 151

Scalar multiplication over the elliptic curve $y^2 = x^3 + 4x + 1$ in \mathbb{F}_{211} .

The curve has 199 points (including the point at infinity).

The subgroup generated by P has 199 points.

5)