**Tutorial 5.1: ECC over prime field P**

**Instruction: Take your *i* = 10 + (ID mod 100 or nearest assigned number) mod 59.**

Step 0: My sample number is *i*=8. I am taking P1(*x*1, *y*1) = (28, 197).

Choose a prime number. Let *p*=257.

1. Choose a random sample *a* = −4 and *b* = 7 for the curve

*E*: *y*2 = *x*3 + *ax* + *b*

such that 4*a*3 + 27*b*2 ≠0 (mod p).

1. Choose a base Point P1(*x*1, *y*1) = (*xi*, *yi*). Compute P2(*x*2, *y*2) = 2⊗P1(*x*1, *y*1)

**Double Point**

Let (*x*1, *y*1) be a point on an elliptic curve E(Fp), and (*x*1, *y*1) ≠ (*x*2, –*y*2)

then let (*x*2, *y*2) = 2⊗(*x*1, *y*1) such that



Let slope of the tangent line at (*x*1, *y*1) = (28, 197)

,

nume = 3⋅282 – 4 = 2348 ≡ 35 (mod 257)

Deno = 2⋅197 = 394 – 257 ≡ 137 (mod 257)

Let us compute an inverse of deno,

137−1 ≡ 242 (mod 257)

Then c = 35⋅137−1 = 35⋅242 ≡ 246 (mod 257).

And c2 = 2462 ≡ 121 (mod 257).

then

*x*2 = c2 – 2*x*1  = 121 – 2⋅28 = 65,

and

*y*2 = c (*x*1 – *x*2) – *y*1

= 246(28 – 65) – 197

= −9299 ≡ 210 (mod 257)

A double point here is P2(*x*2, *y*2) = (65, 210).

1. **Add Point**

To compute P3(*x*3, *y*3) = P1(*x*1, *y*1) ⊕ P2(*x*2, *y*2) = (28, 197) ⊕ (65, 210).

Let (*x*1, *y*1) and (*x*2, *y*2) are two points on an elliptic curve E(Fp), and

(*x*1, *y*1) ≠ (*x*2, ± *y*2)

then let (*x*3, *y*3) = (*x*1, *y*1)⊕(*x*2, *y*2) such that



Let the slope

of the line connecting (*x*1, *y*1) and (*x*2, *y*2)

then

*x*3 = *m*2 – (*x*1 + *x*2) and *y*3 = *m*⋅(*x*1 – *x*3) – *y*1.

Let us add 2 points, namely, P1(*x*1, *y*1) + P2(*x*2, *y*2) = (28, 197) ⊕ (65, 210).

First, we compute denominator of the slope of secant line,

Nume = 210 – 197 =13.

Deno = *x*2 – *x*1 = 65 – 28 = 37.

Second, we need to compute an inverse of the denominator,

(*x*2 – *x*1)−1 = 37−1 ≡ 132 (mod 257).

Let us compute the numerator = *y*2 – *y*1 = 210 – 197 = 13.

Third, the slope of secant line shall be

= 13⋅132 ≡ 1716 ≡ 174(mod 257).

Finally, we can compute the add point,

*x*3 = *m*2 – (*x*1 + *x*2) = 1742 – (28+65) ≡ 207 – 93 ≡ 114 (mod 257).

and

*y*3 = *m*(*x*1 – *x*3) – *y*1 = 174(28 – 114) – 197 = 0 – 15161 ≡ 2 (mod 257)

Final answer is 3⊗(28, 197) = (114, 2).

Additional lesson for this tutorial is 3⊗(28, 197) = 3⊗8⊗(1, 2)

= 24⊗(1, 2)

= (114, 2).

Let us check 2⊗(28, 197) = 2⊗8⊗ (1, 2) = 16⊗(1,2) = (65, 210).

|  |  |  |  |
| --- | --- | --- | --- |
| *i* | *ai* | Left | Right |
| 8 | 1 | 1 | 2 |
| 7 | 1 | 3 | 4 |
| 6 | 0 | 6 | 7 |
| 5 | 0 | 12 | 13 |
| 4 | 0 | 24 | 25 |
| 3 | 1 | 49 | 50 |
| 2 | 1 | 99 | 100 |
| 1 | 1 | 199 | 200 |

if *ai*  = 1, Left = Left + Right, Right = double(Right)

if *ai*  = 0, Right= Left + Right, Left = double(Left)

Let us introduce a basic sum. Given a target sum =199.

Compute a public key by projecting via balanced technique in little endian

Let us compute ⊗

|  |  |  |  |
| --- | --- | --- | --- |
| *i* | *ai* | Left | Right |
| 8 | 1 | (1, 2) 1P | (239, 186) 2P |
| 7 | 1 | (46, 28) 3P | (97, 131) 4P |
| 6 | 0 | 6P | 7P |
| 5 | 0 | 12P | 13P |
| 4 | 0 | 24P | 25P |
| 3 | 1 | 49P | 50P |
| 2 | 1 | 99P | 100P |
| 1 | 1 | 199P | 200P |

Table 5: A list of points on a curve E: *y*2 = *x*3−4*x*+7 (mod 257)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *i* | *xi* | *yi* | *i* | *xi* | *yi* | *i* | *xi* | *yi* |
| 1 | 1 | 2 | 21 | 161 | 136 | 41 | 34 | 232 |
| 2 | 239 | 186 | 22 | 193 | 197 | 42 | 57 | 184 |
| 3 | 46 | 28 | 23 | 72 | 211 | 43 | 65 | 47 |
| 4 | 97 | 131 | 24 | 114 | 2 | 44 | 209 | 173 |
| 5 | 18 | 192 | 25 | 142 | 255 | 45 | 96 | 104 |
| 6 | 49 | 36 | 26 | 103 | 154 | 46 | 147 | 128 |
| 7 | 50 | 231 | 27 | 16 | 21 | 47 | 130 | 200 |
| 8 | 28 | 197 | 28 | 44 | 132 | 48 | 172 | 130 |
| 9 | 112 | 53 | 29 | 36 | 197 | 49 | 22 | 95 |
| 10 | 22 | 162 | 30 | 36 | 60 | 50 | 112 | 204 |
| 11 | 172 | 127 | 31 | 44 | 125 | 51 | 28 | 60 |
| 12 | 130 | 57 | 32 | 16 | 236 | 52 | 50 | 26 |
| 13 | 147 | 129 | 33 | 103 | 103 | 53 | 49 | 221 |
| 14 | 96 | 153 | 34 | 142 | 2 | 54 | 18 | 65 |
| 15 | 209 | 84 | 35 | 114 | 255 | 55 | 97 | 126 |
| 16 | 65 | 210 | 36 | 72 | 46 | 56 | 46 | 229 |
| 17 | 57 | 73 | 37 | 193 | 60 | 57 | 239 | 71 |
| 18 | 34 | 25 | 38 | 161 | 121 | 58 | 1 | 255 |
| 19 | 79 | 224 | 39 | 141 | 183 | 59 | -1 | -1 |
| 20 | 141 | 74 | 40 | 79 | 33 | 60 | 1 | 2 |