Michael Chillemi
Final
12/14/2021

1. $y^2 = x^3 + 2x + 2 \bmod 17$
Point = (5, 1)
Q = (6, 3)

- Verify that the points P and Q indeed lie on the curve line.
  - plug in P(5, 1)

$1^2 \bmod 17 = 5^3 + 2(5) + 2 \bmod 17$
$1 \bmod 17 = 125 + 10 + 2 \bmod 17$
$1 \bmod 17 = 137 \bmod 17$
$1 = 1$

a = b mod n
a mod n = b mod n

- since both sides equal 1 then that means P(5, 1) lies on the curve
- plug in Q(6, 3)

$3^2 \bmod 17 = 6^3 + 2(6) + 2 \bmod 17$
$9 \bmod 17 = 230 \bmod 17$
$9 = 9$

- Q(6, 3) is also on the curve since $9 = 9$.

- Find the point on the curve
R = P + Q.
P = (5, 1) = (x_1, y_1) p = 17
Q = (6, 3) = (x_2, y_2) a = 2

P ≠ a point addition

$$s = \frac{y_2 - y_1}{x_2 - x_1} \bmod p$$

$$= \frac{3 - 1}{6 - 5} \bmod 17$$

$$= \frac{2}{1} \bmod 17$$

$$s = 2$$

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$= 2^2 - 5 - 6 \bmod 17$$
$$= 4 - 11 \bmod 17$$
$$-7 \bmod 17$$

formula: $\text{mod}(a, n) = a - n \cdot \text{floor}\left(\frac{a}{n}\right)$

$$x_3 = -7 \bmod 17 = -7 - 17 \cdot \text{floor}\left(\frac{-7}{17}\right)$$
$$= -7 + 17$$
$$x_3 = 10$$

- now y_3

$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$
$$= 2(5 - 10) - 1 \bmod 17$$
$$= -11 \bmod 17$$
$$= -11 - 17 \cdot \text{floor}\left(\frac{-11}{17}\right)$$
$$= -11 + 17$$
$$y_3 = 6$$

$$R = (x_3, y_3) = (10, 6)$$

- Find the Point on the curve $S = P + P$.

$P(5, 1) = (x_1, y_1)$
$Q = (6, 3) = (x_2, y_2)$
$y^2 = x^3 + 2x + 2 \mod 17$

$a = 2, \quad p = 17$
$S = P + P$

$$S = \frac{3x_1^2 + a}{2y} \mod p$$

$$= \frac{3(5)^2 + 2}{2 \cdot 1} \mod 17$$

$$= \frac{77}{2} \mod 17$$

$$= 77 (2^{-1}) \mod 17$$
$$= (77 \mod 17)(2^{-1} \mod 17) \mod 17$$
$$= (9 \cdot 9) \mod 17$$
$$= 81 \mod 17$$
$$S = 13$$

$$x_3 = S^2 - x_1 - x_2 \mod p$$
$$= 13^2 - 5 - 5 \mod 17$$
$$= 161 - 10 \mod 17$$
$$x_3 = 6$$

$$y_3 = S(x_1 - x_3) - y_1 \mod p$$
$$= (13(5-6) - 1) \mod 17$$
$$= -14 \mod 17$$
$$= -14 - 17 \times \text{floor}\left(\frac{-14}{17}\right)$$
$$= 3 \quad (+17)$$

$y_3 = 3$

$S = (5,1) + (5,1) = (6, 3)$

2. $r = a^k \bmod p$

$s = B^k \cdot m \bmod p$

$p = 97$

$a = 23$

$13 = 17$

$m(x) = 17$

$k = 31$

$r = 23^{31} \bmod 97$

$= 87$

$s = 15^{31} \cdot 17 \bmod 97$

$= 15^{31} \bmod 97 \cdot 17 \bmod 97$

$= 17 \cdot 17 = 289$

$(r, s) = (87, 289)$

3. $e = 27$

$p = 17$

$q = 89$

$n = p \cdot q$

$= 17 \cdot 89$

$= 1513$

$\phi(n) = (p-1)(q-1) = (17-1)(89-1)$

$= 1408$

$e = 271$

$d = e^{-1} \bmod \phi(n)$

$= 271^{-1} \bmod 1408$

3pt2 | 1 mod 1404 = 271 • 239

d = 239

$S = x^d \bmod n$

$S = 114^{239} \bmod 1513$

$= 1319 \bmod 1513$

$S = 1319$

$(x, s) = (114, 1319$ bob sends this to Alice.

$= 1319^{271} \bmod 1513$

$x = 114$

$(x, s) = (114, 1319)$

-Alic will resend to bob

If you assume (1)(2)(3)(4) the signature is correct

4. [illegible]

a). $y^2 = x^3 + 2x + 2 \mod 17$

$P = (5, 1)$

$A = \frac{dy}{dx} \mod 17$

$= \frac{3x^2 + 2}{2y} \mod 17$

$= \frac{77}{2} \mod 17$

$= 77 \cdot 9 \mod 17$

$= 81 \mod 17$

$= 13 \mod 17$

$x_r = (13)^2 - 2 \cdot 5 \mod 17$

$= 151 \mod 17$

$= 6 \mod 17$

$2P = 2P + P \qquad 2P = (6, 5)$

$3P = 2P + P$

$= (6, 3) + (5, 1)$

$= (x_r, y_r)$

$= \frac{1-3}{5-6} \mod 17$

$= 2 \mod 17$

$x_r = 4 - 6 \mod 17$

$= -7 \mod 17$

$= 10 \mod 17$

$y_r = 2(6-10) - 3 \mod 17$

$= -8 - 3 \mod 17$

$= 6 \mod 17$

$Sp = (10, 6)$

b.

- $\frac{p}{a} = 0$
- $\gcd(a, p) = 1$
- $\log(p-1) + \alpha$
- $m = x \pmod{p-1}$
- $m = x \pmod{p-1}$
- RHS
- $a^{m \pmod{p-1}} \pmod{p} = a \pmod{p}$
- $m = x \pmod{p-1}$
- $m = \log(p-1) + \alpha$
- $a^{p-1} = 1 \mod p$
- $a^m \mod p = a^{k(p-1)+\alpha} \mod p = (a^{p-1})^k \cdot a^\alpha \mod p$

$\mod p = a^\alpha \mod p$

conclude! $a^{m \pmod{p-1}} \pmod{p} = a^m \pmod{p}$

$4Q + 4Q$

$= \frac{3q^2 + 2}{2y} \mod 17$

$= \frac{2}{5} \bmod 17$

$= 14 \bmod 17$

$x_r = 14^2 - 2 \cdot 0 \pmod{17}$
$= 9 \bmod 17$

$y_r = 14(0-9) - 11 \bmod 17$
$= 16 \bmod 17$

$8\phi = (9, 16)$

$10\phi = 8\phi + 2\phi$
$= (9, 16) + (16, 13)$

$\frac{13-16}{16-9} \bmod 17$

$= -1 \cdot 5 \bmod 17$
$= 3 \bmod 17$

$x_r = 4 - 9 - 16 \bmod 17$
$= -21 \bmod 17$
$= 13 \bmod 17$

$y_r = 3(9-13) - 16 \bmod 17$
$= -8 - 16 \bmod 17$
$= 10 \bmod 17$

Assume: $\{1, 2, 3, 4, 5\}$ that hellman key is $(13, 10)$

Alice key = (10, 6)

$2Q_A = (10, 6) + (10, 6) = (x_r, y_r)$

$= \frac{dy}{dx} \bmod 17$

$= \frac{3x^2 + 2}{2y} \bmod 17$

$= \frac{302}{12} \bmod 17$

$= -90 \bmod 17$

$= 11 \bmod 17$

$x_r = 121 - 2.10 \bmod 17$

$= 101 \bmod 17$

$= 16 \bmod 17$

$y_r = 11(10 - 16) - 6 \bmod 17$

$\equiv 13 \bmod 17$

$2Q_{(A)} = (16, 13)$

$4Q_{(A)} = (16, 13) + (16, 13) = (x_r, y_r)$

$x_r = 169 \to 16 \bmod 17$

$= 0 \bmod 17$

$y_r = 10(16 - 0) - 13 \bmod 17$

$= 11 \bmod 17$

$\therefore Q_{(A)} = (0, 11)$