Fall 2020 CIS 3362 Quiz #5 Part B: El-Gamal, ECC Solution

Date: 11/13/2020

1) (12 pts) You have received the ciphertext (6, 10), which was encrypted using the public key system, El Gamal. Your secret key, $X_A = 19$ and the prime number modulus is q = 31. Decrypt the ciphertext and clearly mark the correct plaintext. **Please show your work for modular exponentiation by hand. You may plug in individual multiplications and mods in the calculator, but show each step you would normally show, by hand.**

Solution

$C_1 = 6$, so we must first calculate $C_1^{X_A} = 6^{19} \ mod 31$.

Let's print a chart of the first few powers of 6 mod 31:

Exp	0	1	2	3	4	5	6
Value	1	6	5	30	25	26	1

Thus, $6^{19} = 6^{18}(6) = (6^6)^3 6 \equiv 1(6) \equiv 6 \pmod{31}$

Thus, K = 6. Now, we must find $K^{-1} \pmod q$, or $6^{-1} \bmod 31$. Use the Extended Euclidean:

31 = 6 x 5 + 1
31 - 6 x 5 = 1

Take this equation mod 31 and we find that $6^{-1} \equiv -5 \equiv 26 \pmod{31}$.

Finally, we can recover the Plaintext: $P = K^{-1}C_2 = 26(10) = 260 \equiv$ **12 (mod 31).**

Grading: 2 pts for writing that 6^{19} must be determined first.
6 pts for this calculation, can use fast mod expo instead of course
3 pts to find 6^{-1} mod 31
1 pt to use this to get to the result modded in range.

2) (12 pts) Consider the Elliptic Curve $E_{29}(3, 8)$. (The prime number is 29, a = 3 and b = 8.) Two points on this curve are P = (8, 14) and Q = (21, 9). What is P + Q?

Solution

$$\Delta = \frac{y_Q - y_P}{x_Q - x_P} = \frac{9 - 14}{21 - 8} = (-5)13^{-1} mod 29$$

Thus, we must determine 13^{-1} mod 29 via the Extended Euclidean Algorithm:

29 = 2 x 13 + 3
13 = 4 x 3 + 1

13 - 4 x 3 = 1
13 - 4(29 - 2 x 13) = 1
13 - 4 x 29 + 8 x 13 = 1
9 x 13 - 4 x 29 = 1

Take this equation mod 29 to yield:

9 x 13 ≡ 1 (mod 29), thus, $13^{-1} \equiv 9$ (mod 29)

It follows that $\Delta = (-5)(9) = -45 \equiv 13\ (mod\ 29)$

Now, solve for the point R, that is the sum of the points P and Q:

$$x_R = \Delta^2 - x_P - x_Q = 13^2 - 8 - 21 = 140 \equiv 24\ (mod\ 29)$$

$$y_R = -y_P + \Delta(x_P - x_R) = -14 + 13(8 - 24) = -14 - 208 = -222 = 10\ (mod\ 29)$$

Thus, the sum of P and Q is **(24, 10).**

Note: On the original quiz given, the curve was mistakenly identified as $E_{29}(3, 4)$. But, it is really $E_{29}(3, 8)$.

Grading: 2 pts for written formula for delta,
4 pts to find 13^{-1}
3 pts to find x_R
3 pts to find y_R

Award points for the last two steps if they carry them out correctly with the Incorrect delta, but only if the formula and everything else substituted is correct.

3) (1 pt) Hurricane Eta is named after which Greek letter? **Eta (Grading: Give to All)**