ASSIGNMENT OF Cryptography

Q1. $y^2 = x^3 + 1$ Mod 19 $\quad P(14, 3)$

Asked: $4P_1 = ?$

$2P_1 = P_1 + P_1 = (14, 3) + (14, 3)$

So that $x_1 = 14$, $x_2 = 14$, $y_1 = 3$, $y_2 = 3$

$$\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{3(14)^2 + 0}{2(3)} = \frac{588}{6} \text{ Mod } 19 = \frac{18}{6} = 3 \text{ Mod } 19$$

$$x_3 = \lambda^2 - x_1 - x_2 = (3)^2 - 14 - 14$$

$$= 9 - 14 - 14$$

$$x_3 = -19 \text{ Mod } 19$$

$$x_3 = 0$$

$$V = y_1 - \lambda x_1$$

$$V = 3 - 3(14) = 3 - 42 = -39 \text{ Mod } 19$$

$$V = 18$$

$$y_3 = \lambda(x_3) + V$$

$$y_3 = 3(0) + 18 = 0 + 18$$

$$y_3 = 18$$

$$P = (x_3, -y_3) \Rightarrow 2P(0, -18) \Rightarrow 2P = (0, 1)$$

$$3P_1 = 2P_1 + P_1 = (0, 1) + (14, 3)$$

So that $x_1 = 0$, $x_2 = 14$, $y_1 = 1$, $y_2 = 3$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3 - 1}{14 - 0} = \frac{2}{14} = 2 \times 14^{-1} = 2 \times 15 = 30$$

$$\lambda = 30 \text{ Mod } 19 \qquad \lambda = 11$$

$$x_3 = \lambda^2 - x_1 - x_2 = (11)^2 - 0 - 14 = 107 \text{ Mod } 19$$

$$x_3 = 12$$

$$V = y_1 - \lambda x_1 = 1 - (11)0 = 1 - 0$$

$$V = 1$$

$$y_3 = \lambda(x_3) + V = 11(12) + 1 = 132 + 1 = 133 \text{ Mod } 19$$

$y_3 = 0$

$3P_1 = (12, -0) \Rightarrow 3P_1 = (12, 0)$

$4P_1 = 3P_1 + P_1 = (12, 0) + (14, 3)$

so that $x_1 = 12$, $y_1 = 0$, $x_2 = 14$, $y_2 = 3$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{3 - 0}{14 - 12} = \frac{3}{2} = 3 \times 2^{-1} = 3 \times 10$$

$\lambda = 30 \bmod 19$ $\quad \lambda = 11$

$x_3 = \lambda^2 - x_1 - x_2 = (11)^2 - 12 - 14 = 121 - 12 - 14$

$x_3 = 95 \bmod 19$ $\quad x_3 = 0$

$V = y_1 - \lambda x_1 = 0 - 11(12) = 0 - 132$

$V = -132 \bmod 19$

$V = 1$

$y_3 = \lambda(x_3) + V = 11(0) + 1 = 0 + 1$

$y_3 = 1$

$4P_1 = (0, -1) \Rightarrow 4P_1 = (0, 18)$

$4P_1 = (0, 18)$