4 a) Looking at the power consumption graph, we can infer the value 1010110101111. Thus, the most significant byte in Alice's private key corresponds to 10101101.

b) $P = (2,3), Q = (5,2),\ y^2 = x^3 - x + 3$

i. $m = \frac{3*2^2-1}{2*3} = \frac{11}{6} = \frac{4}{6} = \frac{2}{3} = \frac{2}{10} = \frac{1}{5} = 3,$

$$x_{P+P} = m^2 - x_P - x_P = 3^2 - 2 - 2 = 5,$$

$$y_{P+P} = -(m(x_{P+P} - x_P) + y_P) = -(3*(5-2)+3) = -12 = -5 = 2,$$

$P + P = (5,2)$

ii. $m = \frac{2-3}{5-2} = -\frac{1}{3} = 2,$

$$x_{P+Q} = m^2 - x_P - x_q = 2^2 - 2 - 5 = -3 = 4,$$

$$y_{P+Q} = -\left(m\left(x_{P+Q} - x_P\right) + y_P\right) = -(2*(4-2)+3) = -7 = 0,$$

$$P + Q = (4,0)$$

iii. $m = \frac{3*5^2-1}{2*2} = \frac{37}{2} = \frac{2}{2} = 1$

$$x_{Q+Q} = m^2 - x_q - x_q = 1^2 - 5 - 5 = -9 = -2 = 5,$$

$$y_{Q+Q} = -\left(m\left(x_{Q+Q} - x_Q\right) + y_Q\right) = -(1*(5-5)+2) = -2 = 5,$$

$$Q + Q = (5,5)$$

c) $using\ m = \frac{\left(x_P+x_Q\right)^2 - x_P x_Q + a}{y_P + y_Q},$

iv. $for\ P+P,\ m = \frac{(2+2)^2-2*2-1}{3+3} = \frac{11}{6} = 3,\ P + P = (5,2)$

v. $for\ P+Q,\ m = \frac{(2+5)^2-2*5-1}{2+3} = \frac{38}{5} = \frac{3}{5} = \frac{3}{12} = \frac{1}{4} = 2$

$$x_{P+Q} = 2^2 - x_P - x_q = 2^2 - 2 - 5 = -3 = 4$$

vi. $for\ Q+Q,\ m = \frac{(5+5)^2-5*5-1}{2+2} = \frac{37}{2} = 1,\ Q + Q = (4,0)$

d) Add noise to the emitted channel by introducing arbitrary and artificial noise via random delays.