UNIVERSIDADE FEDERAL DO MARANHÃO
DEIN0217 - Introdução à Criptografia
prof. Antonio de Abreu Batista Júnior
Prova III

Aluno(a): Thalles Alencar Silva

Questão 1

Como o grupo dos pontos de uma curva elíptica é usado em sistemas criptográficos?

Questão 2

Quais são as vantagens do uso de sistemas criptográficos de curvas elípticas?

Questão 3

Considere a curva elíptica E dada por $Y^2 = X^3 + 2X + 2 \ mod \ 17$ e o ponto $P(5, 1)$

1. Calcule $4P$.
2. Calcule $-P$.
3. Encontre a ordem de P em E.
4. descubra k, onde k é um inteiro tal que $k * P$ é o ponto $(10, 6)$.

$P(x_1, y_1) + Q(x_2, y_2) = R(x_3, y_3)$

$x_3 = s_2 - x_1 - x_2 \ mod \ p$ and $y_3 = s(x_1 - x_3) - y_1 \ mod \ p$

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p & ; \text{if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p & ; \text{if } P = Q \text{ (point doubling)} \end{cases}$$

$\frac{1}{3} \ mod \ 17$

$3x \equiv 1 \ mod \ 17$

Entrada: Representação Binária de k e um ponto P
Saída: $Q = kP$

1: $Q = P$
2: **for** $i = n - 2$ to 0 **do**
3: $\quad Q = 2Q$ {Doubling}
4: $\quad$ **if** $k_i = 1$ **then**
5: $\quad\quad Q = Q + P$ {Addition}
6: $\quad$ **end if**
7: **end for**
8: **return** Q

Algorithm 1: Double-and-Add Algorithm

Por exemplo, calcular $19P$.

$k_4 2^4 +$	$k_3 2^3 +$	$k_2 2^2 +$	$k_1 2^1 +$	$k_0 2^0 =$	19
k4	k3	k2	k1	k0	
1	0	0	1	1	
	2P	4P	8P + P	18P + P	