Kryptografia z elementami algebry

Laboratorium 3, arytmetyka krzywej eliptycznej

(Moduł 2)

1. Zaimplementuj algorytm (funkcję), która generuje losową krzywą eliptyczną nad $\mathbb{F}_p$.
   Dane: $p = 3 \pmod 4$ duża liczba pierwsza (ok. 300 bitów)
   Wynik: $A, B \in \mathbb{F}_p$ takie, że $E : Y^2 = X^3 + AX + B$ jest krzywą nad $\mathbb{F}_p$

2. Zaimplementuj algorytm (funkcję), który znajduje losowy punkt na krzywej eliptycznej nad $\mathbb{F}_p$.
   Dane: $A, B, p = 3 \pmod 4$ takie, że $E : Y^2 = X^3 + AX + B$ jest krzywą nad $\mathbb{F}_p$
   Wynik: $P = (x, y) \in E(\mathbb{F}_p)$

3. Zaimplementuj algorytm (funkcję), który sprawdza czy punkt należy do krzywej.
   Dane: $P = (x, y)$
   oraz $A, B, p = 3 \pmod 4$ takie, że $E : Y^2 = X^3 + AX + B$ jest krzywą nad $\mathbb{F}_p$
   Wynik: `True` jeśli $P = (x, y) \in E(\mathbb{F}_p)$ w przeciwnym przypadku `False`

4. Zaimplementuj algorytm (funkcję), który oblicza punkt przeciwny do danego punktu.
   Dane: $P = (x, y) \in E(\mathbb{F}_p)$ **Wynik:** $-P = (x, -y) \in E(\mathbb{F}_p)$

5. Zaimplementuj algorytm (funkcję), która oblicza $P \oplus Q$ sumę punktów krzywej eliptycznych. Zaimplementuj wszystkie przypadki.
   Dane: $P = (x_1, y_1), Q = (x_2, y_2) \in E(\mathbb{F}_p)$
   oraz $A, B, p = 3 \pmod 4$ takie, że $E : Y^2 = X^3 + AX + B$ jest krzywą nad $\mathbb{F}_p$
   Wynik: $R = (x_3, y_3) \in E(\mathbb{F}_p)$ taki, że $R = P \oplus Q$.