Kryptografia z elementami algebry

Laboratorium 4, Kryptosystem ElGamala na krzywej eliptycznej

(Moduł 3)

Niech

$$E : Y^2 = X^3 + AX + B \pmod{p}, \qquad p = 3 \pmod{4}$$

1. Zaimplementuj algorytm generowania kluczy kryptosystemu ElGamala na krzywej eliptycznej.
   Dane: k liczba bitów p
   Wynik: $K_A = [E = [A, B, p], p, Q, P]$,- klucz publiczny, $k_A = [E = [A, B, p], p, x, Q, P]$- klucz tajny, gdzie $p = 3 \pmod 4$, $Q, P \in E(\mathbb{F}_p)$

2. Zaimplementuj algorytm, który koduje wiadomość na punkt na krzywej eliptycznej.
   Dane: M, $E = [A, B, p]$
   Wynik: $P_M = (x, y) \in E(\mathbb{F}_p)$ zakodowana wiadomość M

3. Zaimplementuj algorytm szyfrowania ElGamala na krzywej eliptycznej.
   Dane: $P_M, K_A = [E = [A, B, p], p, Q, P]$,- klucz publiczny
   Wynik: $C = [C_1, C_2]$, $C_1, C_2 \in E(\mathbb{F}_p)$

4. Zaimplementuj algorytm deszyfrowania ElGamala na krzywej eliptycznej.
   Dane: $C = [C_1, C_2]$ $P_M, K_A = [E = [A, B, p], p, x, Q, P]$,- tajny
   Wynik: $P_M = (x, y) \in E(\mathbb{F}_p)$

5. Zaimplementuj algorytm, który dekoduje punkt krzywej eliptycznej.
   Dane: $P_M = (x, y) \in E(\mathbb{F}_p)$ $E = [A, B, p]$
   Wynik: M wiadomość - zdekodowany punkt P