Criptografie și securitate CTI

Laborator 13

Curbe eliptice

1. Fie curba eliptică $y^2 = x^3 + 11x + 20$ peste $\mathbb{Z}_7$.
   (a) Câte puncte are această curbă eliptică și care sunt acestea? Calculați de mână aceste puncte.
   (b) Adunați punctele $A = (2, 1)$ și $B = (4, 4)$.
   (c) Calculați $2A$.
   (d) Determinați punctul A' pentru care $A + A' = \mathcal{O}$.
   (e) Pot fi adunate punctele $(4, 3)$ și $(5, 6)$?

Criptosistemul ElGamal - versiunea pe curbe eliptice

2. Fie curba eliptică $y^2 = x^3 + 11x + 20$ peste $\mathbb{Z}_{23}$.
   Cheia secretă este $a = 7$. Cheia publică este $(\alpha = (10, 16), \beta = (22, 10), E)$.
   (a) Criptaţi mesajul $(10, 16)$ folosind $k = 3$.
   (b) Decriptaţi mesajul $(y_1, y_2) = ((2, 2), (20, 12))$. Ce observaţi?
   (c) Puteți cripta valoarea $(3, 5)$ folosind cheia anterioară cripta ? Justificaţi.