

Cryptography Homework 8

Due April 19, 10:30m

Send your OUID number to me by using ElGamal cryptography system based on elliptic curve:

The elliptic curve $y^2 = x^3 + 9817492759375943 * x + 7358469577957$ over finite field \mathbf{F}_p with $p = 29579385439865947694694684968492467204765762471$. Use $\kappa = 30$. The base point is $B = (5, 22628679036034363552380188982145515602413799729)$.

My public key is $(15747883366601598527268816398234122460533203151, 20436308842811998600725239736561666084747562678)$.