Math 308 Week 8 Problem Set

- This is a team assignment about elliptic curve encryption (Elgamal), and elliptic curve digital signature.

Assignment

Instruction: Complete and submit the following on Canvas. Please see Canvas Assignment Team Quiz 2 for detail requirements.

Alice and Bob use elliptic curve encryption schema (Elgamal) to communicate, and use the elliptic curve digital signature schema to sign messages. They use the following elliptic curve group for all activities:

- $E : y^2 = x^3 + Ax + B \bmod p$
  $A = 8722749729$
  $B = 0$
  $p = 3927849327489732742098301298309218389728937482917$

Alice's public encryption key is the following

- $P_A = [3724, 6029063420493436118204196753091780068187451946 54]$ (base point)
- $Q_A = [861353249895582217790142036793729538190030214505,$
  $1734760601653880308873616205303816003016007523211]$ (public key)
- Tolerance parameter $T = 45$.

Bob's public encryption key is the following

- $P_B = [55, 2552022818715546594530165777382068684546058213955]$ (base point)
- $Q_B = [236822613786950731013961122607930306899027178969 3,$
  $3151459300414441461488478318014699430983757085092]$ (public key)
- Tolerance parameter $T = 45$.

Alice's public signature key is the following

- $g_A = [1024893053376846362708505285152157656576664336996,$
  $3195102041918125979388046860939580729961373342395]$ (base point)
- $b_A = [3641913820209498543448466890113332485917349049728,$
  $3248144475384638502479692511929041081769252077500]$ (public key)

Bobs public signature key is the following

- $g_B = [8392708879595257733333257356633439712161817304 23,$
  $2803416021228697467998681750068158601314598184 66]$ (base point)
- $b_B = [3152020786001474940329228302416921162031149380 63,$
  $1828293803364833618111119803301786816623136360850$ (public key)

One of the two sent a message to the other, with a **digital signature** attached. The padded ASCII version of the message has two packets:

packet 1: 178197216205211210197208132184214201197215217
packet 2: 214201

The signature on packet 1 is
$x = 1985977078462597337627134881095450804747548473623$ (the x-coordinate of the point R)
$s = 814991367249546649087876465646099$

The signature on packet 2 is
$x = 1985977078462597337627134881095450804747548473623$ (the x-coordinate of the point R)
$s = 1750496888670885456506533290801827$

One of the two sent an **encrypted message** to the other (not the same message as in the previous digital signature). The encrypted message (ciphertext) is represented by two pairs (C_1, C_2) of points (one pair for each encrypted packet):

The encrypted version of packet 1 is
$[3392250666220429748352057521249133303617757145558, 1939150282495281402743909945080558858688999245361],$
$[1050636622523869006662499680251539236718340080433, 2424946592070024418655054514705348236967025679428]$

The encrypted version of packet 2 is
$[3392250666220429748352057521249133303617757145558, 1939150282495281402743909945080558858688999245361],$
$[1988696510411214582210254167304130198728973460774, 1222467321388159168322987359117953287886789562987]$

One of them by accident published also his/her **private encryption key**: 8237628684.

Questions: Determine:

(a) Whose private encryption key was accidentally published?

(b) Decrypt the message.
(Note: If you correctly decrypt the message point, you should be able to recover an English message via tools from Elliptic Curve Embedding.)

(c) Who signed the message? i.e. who's public signature keys can be used to verify the signature?