General Information

You are given two messages encrypted by an Elliptic Curve cryptography system. One of the messages is authentic, while the other was intentionally forged. The goal is to decrypt both messages, identify which message is forged, and explain your decision.

Elliptic Curve

Both messages were generated using the same elliptic curve E over a prime field of order equal to 13-th Mersenne prime, and coefficient a equal to -3. E was generated using Complex Multiplication method with imaginary field discriminant D > -400. Security constraints on #E: largest prime divisor > 2^{160}; second largest prime divisor < 2^{16}.

Cryptosystem

Both messages were encrypted using ElGamal scheme. Every message was encrypted using a different point on the curve E, and different private key d.

Converting text to elliptic curve points was performed using 1 byte padding.

Representation of Elliptic Curve points

Points on elliptic curves are represented in the so called "Compressed" format (see e.g. http://www.cdc.informatik.tu-darmstadt.de/TI/Veroeffentlichung/Artikel/Kryptographie/PublicKeyAllgemein/P1363-E-10-05-98.pdf, section E.2.3.1), where the x-coordinate is preceded by a "+" or "-" sign, whenever the compressed y-coordinate equals to 1 or 0, respectively.

Messages

Message 1:

EC point :
-39854059894255679671560184198458955381466341207788211832699113864712223297651504406209918236768379804
40324457306600557245758586407123663426871114407190797434

d :
27448348782958755025239908982559709389317508031370645647395171020977304234906521514359365600168914817342864913123798890151787489300101998886437815 13

Cypher : (-
25283570341156314285452570973622931552452114955113458213172475153638040134476111431514881084970388388824199251926120588824778863763753924991176044900175071 95,
+49938368138975226976303726116381107008375562097222477041826762836953124933844950351967161977191555513140861986708261125495626315333858553510520709455352972 4) (-
80758254166624930994885805808547278868718998071374807133715169194253247467455891647655174183575919667899962774286642154391884204524232270614047908160880140 3,
+48895184225146340576989096938782009425102806022592335856230935456690157697537869879840694481515998005140735254831936928651133321567530760913273058938141574 88) (-
67963017237211817379104842876036531858536954025735158867830197606550067064999293637905324395273160915824213733076760220325848160629071489922021580830736571 74,
+34100361230470345235538416213457966803859349577856572731338138608591495828776684341409852662502523611778080563937468430434959374548359626354713646599503778914) (-
56188991773561506031002117064858333989553958878011305817106070653814471141548012052043976496815678771933783293026632527596954424119846975490640040608379841 07,
+34169336482657079864211904130164242671491998507969626927159824425318473123159700897784519933424521773753987294686398999219471632328969089100404126804266856 4)
(+42357581058619648963139224795216147743995076557618780467354879022880965630936345115997449079058307748416946870392218118715534005957424366026772021430447701 41,
+19203061345990046403709866799484725008271545126069049790268849889477291786002233659394475856373581332939339123844776781598945234580742177770442459063157379 85) (-
16763992999626024496919929122995219673424527003176960629205515456329111707731122233792822964141690544700097699317336174126617617661365153810830962234607576 92,
-28230416287331726547518646043017347622686310127882715861308205747507696304971434510457084825058925403350550716609845230437680425376467775291101842227573865 29) (-
66911818541034442336596572118635109945077548911227006389970304657492550531352691084774178115954750258561755876124731124034031797703052251096707507794496493 3,
-32484351231830818188317641151119521993348787563631945721193720736270366856789020104628184103698082049444549223238271201017009946546941623547504255387641803 18)
(+14062083264626258715501530495932715271382145065874701346952810158396043336363076878676901954526949206157818578915150899253611163818542997785404152872874582 5,
-19380147320171542124863083967272001725045338172249514956232782696359364469550900712765869087738998288301190784548904107385102190999021571753129982422703091 17)
(+44633606527008311247790072577707971646000117427391072030939111973458058674688896298635246414274736 40

277704524524605946229133630958577529608000668060320168287,
-160864485458784249866279186901185734778802762455247094670215385706520354153531227142938749405399891134708916113094998521838936475600677938012620265001599741 0)
(+28184672459374788808990207900631629340390630133873381898723548375357261142756528757385733511086765268384794710474560464777749583202811753933455278317961259 3,
+37701058376807207766959963494049155910421971382886648009692030078536171177487558992942980727879562761318422033029235046711161517697909728791807362585867824 90)

Message 2:

EC point :
+27763378398786229074599115708830772870642327479889833406646465705544246755124324274528352540556237051985363387185146541233648915772426481868607758057571420 87

d :
123794667849756879018882609441862820619347438051355641442054915403254421513064391821540591374899428211018235361774574698779981971879999474525137645 4.

Cypher : (-
19754271565231337280594014238094003174791624376688602851416440343436877071919077196169594440499637496869851258309091830558354811648934354431080877402333751320,
+95061590514746985732786963002280025522979803208335512879728320095798707162338098912329950613143050605351430330274483031703374817804416364795994063951968273) (-
19712856334786039333828979662183031495286576028431945765138979124556470151244488310074921412649719032666837071744147057134771148934687500178247890541149951 68,
+16223831278461926689012958700483231917359763316171406672452424765521575461056076270064249532232111070833523703466817367268117678183988599990539240975621234 40)
(+22989040902723008851909905351119971974866681840658021624417012414908889555244476983783886323876263958134915912177966867980721713284149180349766039500448018 6,
-46794025745540458675939373124663466497396641044456593261429130651859228280690643899495340592345420998615495542856737170294705997732493668297103193852225160 48) (-
64001708938802868307329187637808278236748937389195096410357018077864233049655495075480432005441981538998463692747488010747185260171104311071949634703969610 82,
-58922837742391356223650605002042741627010917393368018011609709706664425796096597597526242849563930530513426309722278356271534975579889078771772570397590208 90) (-
42815870455164132295031357004628246482765366301725934689386857053905817664568685739391822716576659807233118216242170548701989455359323751750167788647366659 87,
+40577106785120901491056855108266549975685726997834121787137599291196152497965728709854095016879532815449412606813746014718136949737673581154085640046662766 36) (+63483727974901989399133848177893362077135584740763894680462809392466872699584573756714703689840890132246819491162175778960485025923335218404765446597885235 88,
+14005084396014793052896208402879699976925487138613446569685400470691945186808086167489112395596094426214514066551479688086044013728248110716054259295232918 9) (-
18161540973444973064031998234041085716484868285949984153321451663587642735983081634667296266276646014754177773536663125553404511400025236773526386687607925 57,
-30503472401927837051444023353362726252997828757466527410225646956800106132198647670709357144150570664476415046892723354058489069557455601783988915973570630 33) (-
33369894822621271257275464011198734003558471336759401595042077646714900261443502936152496327116418701173125041148023056994357940415576682722813736661665946 24,
+54308964856537978546895360064317087416675630862591405053679677550001463474099684771860039759192477449195154293281494160509840691271948330075562635336774023 93) (-
34491251863004435251014862564948393167122867964320119898718206830007222802564408596170393369150905941778667608121117602743562667443939601307872097864460838 36,
-15696994340682602509016388688841316949960518664515386530059717925697405291055041480639728255778087799110925790651320392347216687096445009774743675365352819 87) (+29696642037516953985564363585749170695649495228255445868577656371921291372978713114994424868842466372136725038659449090874849615525727228191689171856065984 15,
-64569954810308224840472263351302448046694976625362399661112571384139676562586573575659413287130633329817605092184285539534328644584333756352721448412469401 17)