

## 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  $D > -400$ .

## 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 :

-3985405989425567967156018419845895538146634120778821183269911386471222329765150440620991823676837980440324457306600557245758586407123663426871114407190797434

d :

2744834878295875502523990898255970938931750803137064564739517102097730423490652151435936560016891481734286491312379889015178748930010199888643781513

Cypher : (-

252835703411563142854525709736229315524521149551134582131724751536380401344761114315148810849703883888  
2419925192612058882477886376375392499117604490017507195,  
+49938368138975226976303726116381107008375562097222477041826762836953124933844950351967161977191555513  
14086198667082611254956263153338585535105207094553529724) (-  
807582541666249309948858058085472788687189980713748071337151691942532474674558916476551741835759196678  
999627742866421543918842045242322706140479081608801403,  
+48895184225146340576989096938782009425102806022592335856230935456690157697537869879840694481515998005  
14073525483193692865113332156753076091327305893814157488) (-  
679630172372118173791048428760365318585369540257351588678301976065500670649992936379053243952731609158  
2421373307676022032584816062907148992202158083073657174,  
+34100361230470345235538416213457966803859349577856572731338138608591495828776684341409852662502523611  
77808056393746843043495937454835962635471364599503778914) (-  
561889917735615060310021170648583339895539588780113058171060706538144711415480120520439764968156787719  
3378329302663252759695442411984697549064004060837984107,  
+34169336482657079864211904130164242671491998507969626927159824425318473123159700897784519933424521773  
7539872946863989992194716323289690891004041268042668564)  
(+4235758105861964896313922479521614774399507655761878046735487902288096563093634511599744907905830774  
841694687039221811871553400595742436602677202143044770141,  
+19203061345999046403709866799484725008271545126069049790268849889477291786002233659394475856373581332  
93933912384477678159894523458074217777044245906315737985) (-  
167639929996260244969199291229952196734245270031769606292055154563291117077311222337928229641416905447  
0009769931733617412661761766136515381083096223460757692,  
-28230416287331726547518646043017347622686310127882715861308205747507696304971434510457084825058925403  
3505507166098452304376804253764677529110184222757386529) (-  
669118185410344423365965721186351099450775489112270063899703046574925505313526910847741781159547502585  
6175587612473112403403179770305225109670750779244964933,  
-32484351231830818188317641151119521993348787563631945721193720736270366856789020104628184103698082049  
44454922323827120101700994654694162354750425538764180318)  
(+1406208326462625871550153049559327152713821450658747013469528101583960433363630768786769019545269492  
061578185789151508992536111638185429977854041528728745825,  
-19380147320171542124863083967272001725045338172249514956232782696359364469550900712765869087738998288  
30119078454890410738510219099902157175312998242270309117)  
(+4463360652700831124779007257770797164600011742739107203093911197345805867468889629863524641427473640  
277704524524605946229133630958577529608000668060320168287,

-16086448545878424986627918690118573477880276245524709467021538570652035415353122714293874940539989113  
47089161130949985218389364756006779380126202650015997410)  
(+2818467245937478880899020790063162934039063013387338118987235483753572611427565287573857335110867652  
683847947104745604647777495832028117539334552783179612593,  
+37701058376807207766959963494049155910421971382886648009692030078536171177487558992942980727879562761  
31842203302923504671116151769790972879180736258586782490)

Message 2:

EC point :

+27763378398786229074599115708830772870642327479889833406646465705544246755124324274528352540556237051  
98536338718514654123364891577242648186860775805757142087

d :

123749667849756879018882609441862820619347438051355641442054915403254421513064391821540591374899428211  
0182353617745746987799819718799994745251376454.

Cypher : (-

197542715652313372805940142380940031747916243766886028514164403434368770719190771961695944404996374968  
6985125830909183055835481164893435443108087740233751320,  
+95061590514746985732786963002280025522979803208335512879728320095798707162338098912329950613143050605  
3514303302744830317033748178044163647959940639519968273) (-  
197128563347860393338289796621830314952865760284319457651389791245564701512444883100749214126497190326  
6683707174414705713477114893468750017824789054114995168,  
+16223831278461926689012958700482321917359763316171406672452424765521575461056076270064249532232111070  
8335237034668173672681176781839885999053924097562123440)  
(+2298904090272300885190990535111997197486668184065802162441701241490888955524447698378388632387626395  
81349159121779668679807217132841491803497660395004480186,  
-46794025745540458675939373124663466497396641044456593261429130651859228280690643899495340592345420998  
61549554285673717029470599773249366829710319385222516048) (-  
640017089388028683073291876378082782367489373891950964103570180778642330496554950754804320054419815389  
984636927474880107471852601711043110719496347039661082,  
-58922837742391356223650605002042741627010917393368018011609709706664425796096597597526242849563930530  
51342630972227835627153497557988907877177257039759020890) (-  
428158704551641322950313570046282464827653663017259346893868570539058176645686857393918227165766598072  
331821624217054870198945535932375175016778864736665987,  
+40577106785120901491056855108266549975685726997834121787137599291196152497965728709854095016879532815  
44941260681374601471813694973767358115408564004666276636)  
(+6348372797490198939913384817789336207713558474076389468046280939246687269958457375671470368984089013  
224681949116217577896048502592333521840476544659788523588,  
+14005084396014793052896208402879699976925487138613446569685400470691945186808086167489112395596094426  
21451406655147968808604401372824811071605425929952329189) (-  
181615409734449730640319982340410857164848682859499841533214516635876427359830816346672962662766460147  
541777353666312555340451140002523677352638668760792557,  
-30503472401927837051444023353362726252997828757466527410225646956800106132198647670709357144150570664  
47641504689272335405848906955745560178398891597357063033) (-  
333698948226212712572754640111987340035584713367594015950420776467149002614435029361524963271164187011  
7312504114802305699435794041557668272281373666166594624,  
+54308964856537978546895360064317087416675630862591405053679677550001463474099684771860039759192477449  
1951542932814941605098406912719483300755626353677402393) (-  
344912518630044352510148625649483931671228679643201198987182068300072228025644085961703933691509059417  
7866760812111760274356266744393960130787209786446083836,  
-15696994340682602509016388688841316949960518664515386530059717925697405291055041480639728255778087799  
11092579065132039234721668709644500977474367536535281987)  
(+2969664203751695398556436358574917069564949522825544586857765637192129137297871311499442486884246637  
213672503865944909087484961552572722819168917185606598415,  
-64569954810308224840472263351302448046694976625362399661112571384139676562586573575659413287130633329  
81760509218428553953432864458433375635272144841246940117)