Cryptography Homework 5
Due Mar 7, 11:00pm

Suppose that the parameters for the DSS are:

```
q=2873825735738573859476020492596948649629496249717

p=766499231300891823697721141291013080039942567070250364355147662349367989078706206354788206150569781405730505292980104026476107666249244710531735725278852
7

g=145787256720529333581447713207184963245355286403113879324409401203264166993810723395016245782686407100456148738219547600358374464929118512712216877445017
2
```

my DSS public key is:

```
y=651338314678151462503077882532789784745581815960180523820718791300666319354736453279553897541664374323404540241277219523874238424108214591386247717342852
4
```

The following list contains my DSS signatures on the SSN of the students in the class, as well as some random numbers. Find out which one is yours and briefly explain how you do that. (Hint: In Pari/GP, `Mod(23,45)^(-1)` computes the inverse of 23 mod 45, `component(Mod(23,45),2)` gives you the integer 23.)

```
1=
952658166956238299981816222139345264121795595827,
175553423056763791985036191046549124627835845891
4
2=
243195713708712686370244425556676668284318783811
4,
234554309795917662223323361950566540159035791474
3
3=
217500486141662835953054973234833471829064033839
1,
140044465647948768833416123790171076551774729587
2
```

4=
24423449228960131818563317134402917643706185962 63,
18251892631276441309326285980810959232221164240 68
5=
22561345316458160985592284306857840820242149968 65,
92534458835646429734560234796265300281436753131 0
6=
42276457444267780309092893144268656952938680650 0,
28489054820099432726870157180968900231240716571 72
7=
64668415345148171054708475291557268940380834442,
18569610450853820121768264874914221880632624335 63
8=
50418139252893987376013167894386980693335721344 6,
52143134592576062849758810400432746917227642238 5
9=
45772713668440594820582655249763321534662655092 7,
16656318811763613646366480196463427664909982156 23
10=
25366400405156550161955115367935199415593222031 5,
23053661165524116094348611229180801842979126050 16
11=
75769082114922007709605668442747218051157198912,
82984862645412417716725884325266726952846496817 6
12=
34609420824119971435673399637155766122966829396 6,
16252867390691998044676146659638244926190719731 2
13=
24572645147925375323064033396696622597113062881 3,
11429058295590241978864366748750487070998087192 26
14=
24763028484841034021470262734947864508563234560 17,
10091968586794482529306096548464727515733534901 5
15=
25130412526850491194894043603671339085301569577 39,
22443527865414709938501925219293206486606894757 5
16=
16784720358186694450017635882663205570450780428 66,
76822123050613300182966854077974332003168245602 6