Discrete Mathematics: Homework 3

(Deadline: 8:00am, March 11, 2022)

1. (15 points) Let $a, b \in \mathbb{Z}$ with $a \geq b > 0$, and let $q = \lfloor a/b \rfloor$. Show that $\ell(a) - \ell(b) - 1 \leq \ell(q) \leq \ell(a) - \ell(b) + 1$, where $\ell(x)$ is the length of the binary representation of an integer x.

2. (25 points) Implement EEA (Extended Euclidean Algorithm). Run your program on the integers a, b to find two integers s, t such that $\gcd(a, b) = as + bt$, where

```
a=1668022384651447825852593457833359953985771134637730126520497011165389239767604
379401615050725941099565818805704071208590360722012241359542000748948840573133428
0061988395608779010713411287131295428179813333359977034173092335579409810742439 73
1878889187445253126904842513990354679981309972227336575079548411574454057133261 94
8502170654953266704862335547650976687291747849350782598464591428327947848142796 06
6981940848596121777048411057049426221708373813396661449882414643261467806037889 44
0842533384968180620271785010057924587366185944297155319798570577070773474129972 10
787162387238464340113251311657455102507133618892541 1;
```

b=1785577029987051936724205968139042441809618215534204113748879687967110747874357
2864002383145021454681629377265833889126584206834902794697518171431222912791170 44
7567040871094490052067407306798661337490592199170717969818501521767458577818192 49
9457245780503918087449739410569911194050665897532807959319750868264903299819242 75
1930003066441776015464336357481344549028678389909625259705769654505066857444104 94
7192647667108605714724299029223354866042954807541588937325411249097096068333555 97
6598698947608331063572282201472029299051787515328011628625087966449702534156436 26
64766187238978164320548965280129091222800465521335 34.

(**Remark**: Submit your program. The programming can be done with Python, C or C++.)

3. (25 points) Implement the Square-and-Multiply algorithm. Run your program to compute $a^e \bmod n$, where

a=2643001830466169822724488955091646831748945577895632859292198346969979230916366
5193972706206594036869415691968221117606771494540098970766552365207210568611105 85
2640630040412543297842462434526788081852074542946114404279053789976397875435006 09
4029065093695673255562607050336148424707698012085470002233698228862346738763599 12
0210887024055251199687451392437357330469313875769415203278005429487989371958004 06
2135384988676187092753933346466785135069682592239769739616884935612245424974736 66
6329142491909330198993521032748920319427468193197363789859738402941190883470502 93
438525193487532012236008292764491037361145992329447 6;

e=1440940598216013205825255507197539386591946416564947793531697088969116191795293

```
8338402420626169849869240199817340818785857661040902521177902522865655959315955027296333658575625679171649648237486715107874038848080146760431808160047758267886816563159460881275453304962088598750789947602763231536498803689415008248542306983990585872732303067442760485939483530499206750926623632218337793608305495353477797937055213103722548287089239675029998455237837122665431788486963392282333218897305536581935858534831705616909506614608137265328584496490209976683510539438184418619421230489065033982087166936851293061923363455338233631;

n=6454313945264858380477703362750179103894280648074641679882475733796493188829653940877532537389629620183301943333659170185060419295800903851882920771678506908477673738912708560686143515108791497878950835462108643709804848978316528866309066793095973807053237106244098640248269616792697037137207037826580927776615573507736400136484378662896553468052081722791343589348903943822231956595028500968946488659653138113699743321196084282674797868993406360468278824654992876075514546905176286602291631523433342533346644133635496466500102652351900303276417412474450899876006942532128618431090810948908047427520943091131205569637 8.
```

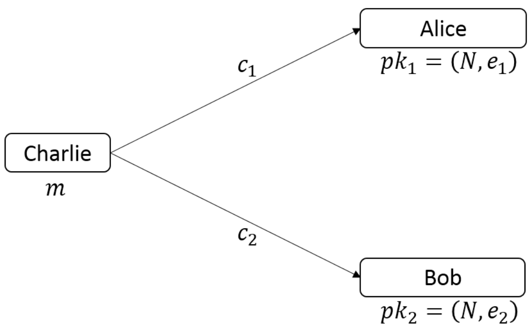
(**Remark**: Submit your program. The programming can be done with Python, C or C++.)

4. (20 points) Solve the following linear congruence equations:

   (1) $17x \equiv 11 (\mathrm{mod} 23)$;

   (2) $55x \equiv 35 (\mathrm{mod} 75)$.

5. (15 points) See the following figure. Alice and Bob trust each other very much. They set their RSA public keys as $pk_1 = (N, e_1)$ and $pk_2 = (N, e_2)$, respectively. Charlie wants to send a private message m to Alice and Bob, where $0 \le m < N$ is an integer and $\gcd(m, N) = 1$. To this end, Charlie encrypts m as $c_1 = m^{e_1} \bmod N$ and $c_2 = m^{e_2} \bmod N$; and then sends c_1 to Alice and sends c_2 to Bob.



Suppose that $\gcd(e_1, e_2) = 1$ and Eve sees all public keys and ciphertexts. Determine if Eve can learn the value of m.