Discrete Mathematics: Homework 6

Name ID: Number

2020.4.23

1. 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=166802238465144782585259345783335995398577113463773012652049701116
538923976760437940161505072594109956581880570407120859036072201224135
954200074894884057313342800619883956087790107134112871312954281798133
333599770341730923355794098107424397318788891874452531269048425139903
546799813099722273365750795484115744540571332619485021706549532667048
623355476509766872917478493507825984645914283279478481427960669819408
485961217770484110570494262217083738133966614498824146432614678060378
894408425333849681806202717850100579245873661859442971553197985705770
70773474129972107871623872384643401132513116574551025071336188925411;

b=178557702998705193672420596813904244180961821553420411374887968796
711074787435728640023831450214546816293772658338891265842068349027946
975181714312229127911704475670408710944900520674073067986613374905921
991707179698185015217674585778181924994572457805039180874497394105699
111940506658975328079593197508682649032998192427519300030664417760154
643363574813445490286783899096252597057696545050668574441049471926476
671086057147242990292233548660429548075415889373254112490970960683335
559765986989476083310635722822014720292990517875153280116286250879664
49702534156436266476618723897816432054896528012909122280046552133534.

The Code is as follows:

```python
from math import gcd

def Exgcd(a: int, b: int):
    '''
        gcd(a,b)=ax+by
    '''
    if (not b):
        return [1, 0]
    x,y = Exgcd(b, a % b)
    return [y, x - a // b * y]



if __name__ == "__main__":
    a = 16680223846514478258525934578333599539857711346...
    b = 17855770299870519367242059681390424418096182155...
    a = int(a)
    b = int(b)
    print(Exgcd(a,b))
```

The Output:

$s =$ 52693465174047597579174064083061206575761398656935114430811243560695
06630695623770063846774138034451326098362590654519415480012670786924 2
52819925030347117153620759789600840565013488945815632549029603633634 2
64479695847742528839838751817826589070065630571483736852349659732197 3
21219714424423764729127052920158 9,

$t = -$ 4922435602557020575264036911319758978419249536244008420108775719343 7
21274111896002459291667895080234292453411578954324261793651077186663 6
25890948400350842512853060168116459859792483937224361285850400246381 7
18448690438802997126844191121984884459076214105581336516953336118974 1
24756550236257925745365828061387 3

2. Implement the Square-and-Multiply algorithm. Run your program to compute $a^e \bmod n$, where,

$a =$ 26430018304661698227244889550916468317489455778956328592921983469699792309163665193972706206594036869415691968221117606771494540098970766552365207210568611105852640630040412543297842462434526788081852074542946114404279053789976397875435006094029065093695673255562607050336148424707698012085470002233698228862346738763599120210887024055251199687451392437357330469313875769415203278005429487989371958004062135384988676187092753933346466785135069682592239769739616884935612245424974736666329142491909330198993521032748920319427468193197363789859738402941190883470502934385251934875320122360082927644910373611459923294476

$e =$ 14409405982160132058252555071975393865919464165649477935316970889691161917952938338402420626169849869240199817340818785857661040902521177902522865655959315955027296333658575625679171649648237486715107874038848080146760431808160047758267886816563159460881275453304962088598750789947602763231536498803689415008248542306983990585872732303067442760485939483530499206750926623632218337793608305495353477797937055213103722548287089239675029998455237837122665431788486963392282333218897305536581935858534831705616909506614608137265328584496490209976683510539438184418619421230489065033982087166936851293061923363455338233631

$n =$ 64543139452648583804777033627501791038942806480746416798824757337964931888296539408775325373896296201833019433336591701850604192958009038518829207716785069084776737389127085606861435151087914978789508354621086437098048489783165288663090667930959738070532371062440986402482696167926970371372070378265809277766155735077364001364843786628965534680520817227913435893489039438222319565950285009689464886596531381136997433211960842826747978689934063604682788246549928760755145469051762866022916315234333425333466441336354964665001026523519003032764174124744508998760069425321286184310908109489080474275209430911312055696378.

The Code is as follows:

```python
def pinbow(a: int, b: int, m: int):
    a %= m
    res = 1
    while (b > 0):
    '''
        当b的当前二进制最低位为1时，即对应着二进制指数不为0时的Xi时
            平方模m
    '''
    if (b & 1):
        res = res * a % m
    a = a * a % m
    b >>= 1
    return res


if __name__ == "__main__":
    a = 26430018304661698227244889550916468317489455778 9...
    e = 14409405982160132058252555071975393865919464165 6...
    n = 64543139452648583804777033627501791038942806480 7...
    print(pinbow(a, e, n))
```

The Output is:

1948938994538604160707108181724192091954263523362311673846915505520625915922643
6938865465087133511096927509156841578783141212143489199923529097996539792654733
5052787068125208309422099919003183364358024089072490207637709226822372509095139
5199481472410255314243260591665020918693044381737199432444238061823906089977020
9698997113410596399791595727394196009053367816731883686504687107181648321094994
0976719953054190408051208140315555905870988234774714741823035881413138114720829
1328747857991048977465984265721979324595417184750317001715144073738047884018946
0378458005476484742953848813170374548455806977675820760128018344

3. Decrypt the ciphertextcin RSA,

   where,

$$
\begin{aligned}
p = {} & 92848022024833655041372304737256052921065477715975001419347548380734496823522 \\
& 5650441779312429471225345638134159924339171084815693198941679726397367886136560 \\
& 0785371947673662561254389374813653659449400548721348578567633362118169046394241 \\
& 778176374364044740559789280733385415663116642623881571639001158683858080891;
\end{aligned}
$$

$$
\begin{aligned}
q = {} & 14960085493382551215982833152717710968911855521238517083138736580400843736791 \\
& 3613643959968668965614270559113472851544758183282789643129469226548555150464780 \\
& 2295380865904988537181020524685198767881928650922297496435467107934643052438158 \\
& 3626702477008188904720017295243800058780798609610767501228426910178511 4471;
\end{aligned}
$$

$$
\begin{aligned}
e = {} & 40998521736306818227223396602297017934844970775490230507394067442991947407942 \\
& 8584156589485718325730596209165847825640345789849625975547419907263509732739897 \\
& 1990092224918103250375455707498928712201945370461644425637423044616348028546654 \\
& 8201345320125444335191585314853004623900975927763520176673866326616786815005427 \\
& 6683546905649003992838087797971215908090534886947521793984417375169824144266261 \\
& 1990406492300411900572847532884748092860563495914734527293634873292356463076178 \\
& 2948819009683739182920645278553069258988184216460576162388732542519399531449485 \\
& 5092245625574360715601350982260594338235258225212936617077118633 7;
\end{aligned}
$$

$$
\begin{aligned}
c = {} & 19650041330069746599953145601677238965601628239920147634666762951565687801813 \\
& 2475911846635611682742243940951386582057040081038097733339789581002325451518224 \\
& 2123244875173658899005048988942666876614798046351776061310094809679938914368938 \\
& 2182898067907249926601510787188645051967549072611352212571461142898751490154313 \\
& 0156920752710863868498978972974709776665048198382274278895852859421500294064580 \\
& 6662061041825912562593269329369550470854629711422167160350497882132054038403027 \\
& 4931058558406068460630295717583862204341896109717245183304380824015928953542554 \\
& 305995152141660395951576393221441992134757424350205005188842788 54.
\end{aligned}
$$

The Code is as follows,

```
from math import gcd
import sys

def Exgcd(a: int, b: int):
    '''
        gcd(a,b)=ax+by
    '''
    if (not b):
        return [1, 0]
    x, y = Exgcd(b, a % b)
    return [y, x - a // b * y]


def pinbow(a: int, b: int, m: int):
    '''
        return a^b mod m
    '''
    a %= m
    res = 1
    while (b > 0):
        '''
            当b的当前二进制最低位为1时，即对应着二进制指数不为0时的Xi时
                平方模m
        '''
        if (b & 1):
            res = res * a % m
        a = a * a % m
        b >>= 1
    return res


def Decrypt(c: int, e: int, p: int,q: int):
    '''
        c is the Ciphertext
        N = pq
        \psi_n = (p-1)(q-1)
        The output = c^{e^{-1}} \bmod N
    '''
    N = p*q
    Psi_n = (p - 1) * (q - 1)
    e_inverse = Exgcd(e, Psi_n)[0] % Psi_n
    return pinbow(c, e_inverse, N)
```

```python
if __name__ == "__main__":

    #Enlarge maximum recursion depth
    sys.setrecursionlimit(10000000)

    p = 9284802202483365504137230473725605292106547771 59...
    q = 14960085493382551215982833152717710968911855521 2...
    e = 40998521736306818227223396602297017934844970775 4...
    c = 19650041330069746599953145601677238965601628239 9...

    print(Decrypt(c, e, p, q))
```

The Output is:

630707626510186802240116822091409100209492364754391360807849452154940380221017 3
444891094505706734673093765283572976861935581726849816923593651509857540611964 7
130187091626649259762409470638569320231136891071185699688043291732815834835920 9
538253361311176291842136227833332291602193351972829179874984249491806896274595 6
079827474452589542646246101220774107235973703726237733253085312380677531524226 6
106565351048414195371114528766268254194739349257413460892523311952497070948124 0
172977007895195652407087194986430036781784697600725075803639254836729878832248 9
84114967389998412531772964049280712531810099797369684894221629 1

4. Let $G = \{x : x \in \mathbb{R}, x > 1\}$. Define $x * y = xy{-}x{-}y + 2$ for all $x, y \in \mathbb{R}$. Show that $(G, *)$ is an Abelian group.

证明. (a) **Closure**:

$x * y = xy - (x + y) + 2 \geq xy - 2\sqrt{xy} + 2 = (\sqrt{xy} - 1)^2 + 1 > 1$

(b) **Associative**:

$x * (y * z) = x * (yz - y - z + 2) = xyz - xy - xz + 2x - x - yz + y + z - 2 + 2 = xyz - xy - xz + x - yz + y + z$

$(x * y) * z = (xy - x - y + 2) * z = xyz - xz - yz + 2z - xy + x + y - 2 - z + 2 = xyz - xz - yz + z - xy + x + y$

(c) **Identity**:

$\exists 2 \in G, \forall x \in G$, we have $2 * x = 2x - 2 - x + 2 = x = x * 2$

(d) **inverse**:

$\forall x \in G$, $\exists x^{-1} = \frac{x}{x-1}$, such that $x * x^{-1} = x\frac{x}{x-1} - x - \frac{x}{x-1} + 2 = 2$

(e) **Commutative**:

$x * y = xy - x - y + 2 = yx - y - x + 2 = y * x$

□

5. Let $(G, \cdot)$ be a multiplicative (Abelian) group of order m. Show that $o(a)|m$ for any $a \in G$, i.e., the order of any group element must be a divisor of the group's order.

证明. Let $G = \{a_1, \ldots, a_m\}$

By Eular's Theorem, we have, $a^m = 1$

$\forall a \in G$

if $i \neq j$, $a_i \neq a_j$

$aa_1 \cdot aa_2 \ldots aa_m = (a_1 \cdot a_2 \ldots)a_m$

$(a_1 \cdot a_2 \cdot a_m)a^m = a_1 \cdot a_2 \cdot a_m$

$a^m = 1$

By definition, $o(a)$ is the least integer such that $a^{o(a)} = 1$

$o(a) \leq m$

Suppose $m = no(a) + r, r \in [0, o(a))$

we have $a^m = a^{no(a)+r} = (a^{o(a)})^n \cdot a^r = 1$

Because $a^{o(a)} = 1$, we have $a^r = 1$ and $r = 0$

so, $o(a) \mid m$

□

6. Let $G = \; g$ be a subgroup of $\mathbb{Z}_p^*$ of order q,

   where,

$$p = 179769313486231590772930519078902473361797697894230657273430081157732675805500963132708477322407536021120113879871393357658789768814416622492847430639474124377767893424865485276302219601246094119453082952085005768838150682342462881473913110540827237163350510684586298239947245938479716304835356329624227998859$$

$$q = (p{-}1)/2andg = 3.$$

   Suppose that in a Diffie-Hellman key exchange protocol Alice and Bobexchanged the following information$(q, G, g; A, B)$,

   where,

$$A = 112983575163002618947589666666735428181684517845144875096902910066434723952623016603393212501214127399908823223492478725971266042754892798177781267512821607470545283059472689034731313027619864228688466438258327552045437590203790635506728603774799021127049872571983254506993921153718739796769296097404717448108$$

$$B = 111772767805210239496365191691516881043394988196297062013853646674574743401042736447328886156429629192691601526398366088012736749454626686281467579205675084461989494513294624066074137247913037330040487275346913253345733429767781900977102687185378411660147190296412313303321533586102552123457499563789255321369$$

Solution:

we have:

$$g^a \bmod p = A$$

$$< g^{ab} >=< A^b >=< B^a >= Output$$

The Code is as follows,

```python
def pinbow(a: int, b: int, m: int):
'''
    return a^b mod m
'''
a %= m
res = 1
while (b > 0):
    '''
        当b的当前二进制最低位为1时，即对应着二进制指数不为0时的Xi时
            平方模m
    '''
    if (b & 1):
        res = res * a % m
    a = a * a % m
    b >>= 1
return res


p = 1797693134862315907729305190789024733617976978942 30...
q = (p - 1) / 2
g = 3
A = 112983575163002618947589666666735428181684517845144...
B = 111772767805210239496365191691516881043394988196297...

for i in range(10000):
    if (pinbow(g,i,p) == A):
        print("a= ", i)
        print("m= ",pinbow(B, i, p))
        break
```

So, $a = 9385$

The output is,

$$10828112783453462381041707802056149866596392072243903940987459672779260675319522663099080388770903982546250524992420350200207624327420612300170620802665302905750045777684348125827484365007590718638373187936889967309324722655294992225815410914105072210725045953105019352457540772995508978315699107247398350128$$