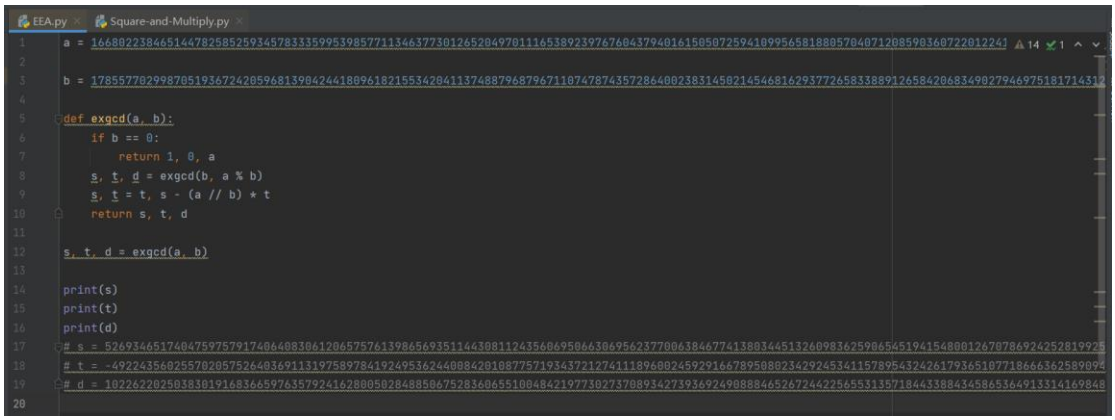
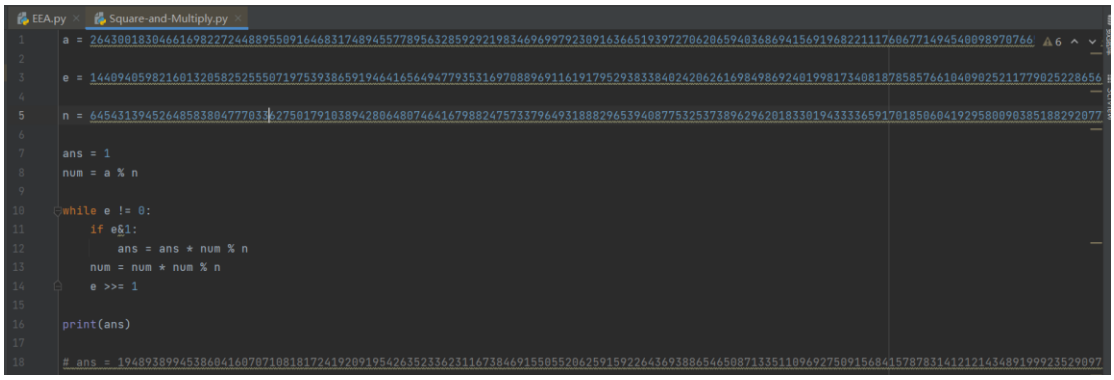
Code:




```
a =
16680223846514478258525934578333599539857711346377301265204970111653892397676043794016150507259410995658188057040712085903607220122413595420007489488405731334280061988395608779010713411287131295428179813333359977034173092335579409810742439731878889187445253126904842513990354679981309972227336575079548411574454057133261948502170654953266704862335547650976687291747849350782598464591428327947848142796066981940848596121777048411057049426221708373813396661449882414643261467806037889440842533384968180620271785010057924587366185944297155319798570577070773474129972107871623872384643401132513116574551025071336188925411

b =
17855770299870519367242059681390424418096182155342041137488796879671107478743572864002383145021454681629377265833889126584206834902794697518171431222912791170447567040871094490052067407306798661337490592199170717969818501521767458577818192499457245780503918087449739410569911194050665897532807959319750868264903299819242751930003066441776015464336357481344549028678389909625259705769654505066857444104947192647667108605714724299029223354866042954807541588937325411249097096068333555976598698947608331063572282201472029299051787515328011628625087966449702534156436266476618723897816432054896528012909122280046552133534

def exgcd(a, b):
    if b == 0:
        return 1, 0, a
    s, t, d = exgcd(b, a % b)
    s, t = t, s - (a // b) * t
    return s, t, d

s, t, d = exgcd(a, b)

print(s)
print(t)
print(d)
```

```
# s =
526934651740475975791740640830612065757613986569351144308112435606950663069562377
006384677413803445132609836259065451941548001267078692425281992503034711715362075
978960084056501348894581563254902960363363426447969584774252883983875181782658907
006563057148373685234965973219732121971442442376472912705292015 89
# t =
-492243560255702057526403691131975897841924953624400842010877571934372127411189600
245929166789508023429245341157895432426179365107718666362589094840035084251285306
016811645985979248393722436128585040024638171844869043880299712684419112198488445
907621410558133651695333611897412475655023625792574536582806138 73
# d =
102262202503830191683665976357924162800502848850675283606551004842197730273708934
273936924908884652672442256553135718443388434586536491331416984834824033197117759
304330445010455165933739427704599295260946079885114808010341303339499946231480241
490457444191096184251471380336624525729640680939684612642314760897
```

Code:


EEA.py
Square-and-Multiply.py
a = 26430018304661698227244889550916468317489455778956328592921983469699792309163665193972706206594036869415691968221117606771494540098970766
e = 14409405982160132058252555071975393865919464165649477935316970889691161917952938338402420626169849869240199817340818785857661040902521177902522865655959315955027296333658575625679171649648237486715107874038848080146760431808160047758267886816563159460881275453304962088598750789947602763231536498803689415008248542306983990585872732303067442760485939483530499206750926623632218337793608305495353477797937055213103722548287089239675029998455237837122665431788486963392282333218897305536581935858534831705616909506614608137265328584496490209976683510539438184418619421230489065033982087166936851293061923363455338233631
n = 64543139452648583804777033627501791038942806480746416798824757337964931888296539408775325373896296201833019433336591701858604192958009038518829207716785069084776737389127085606861435151087914978789508354621086437098048489783165288663090667930959738070532371062440986402482696167926970371372070378265809277766155735077364001364843786628965534680520817227913435893489039438222319565950285009689464886596531381136997433211960842826747978689934063604682788246549928760755145469051762866022916315234333425333466441336354964665001026523519003032764174124744508998760069425321286184310908109489080474275209430911312055696378

```
ans = 1
num = a % n

while e != 0:
    if e&1:
        ans = ans * num % n
    num = num * num % n
    e >>= 1

print(ans)

# ans =
194893899453860416070710818172419209195426352336231167384691550552062591592264369
388654650871335110969275091568415787831412121434891999235290979965397926547335052
787068125208309422099919003183364358024089072490207637709226822372509095139519948
147241025531424326059166502091869304438173719943244423806182390608997702096989971
134105963997915957273941960090533678167318836865046871071816483210949940976719953
054190408051208140315555905870988234774714741823035881413138114720829132874785799
104897746598426572197932459541718475031700171514407373804788401894603784580054764
847429538488131703745484558069776758207601280183 44
```

NO

DATE

homework 3

1. $a, b \in \mathbb{Z}$ $a \geq b > 0$, $q = \lfloor \frac{a}{b} \rfloor$

~~$\Leftrightarrow$ log~~ $l(x) = \lfloor \log_2 x \rfloor + 1, x > 0$

<1> $\exists r \in \mathbb{Z}$, $0 \leq r < b$

s.t. $a = bq + r$

so $l(a) = \lfloor \log_2 a \rfloor + 1 = \lfloor \log_2 (bq + r) \rfloor + 1$

$\geq \lfloor \log_2 (bq) \rfloor + 1 = \lfloor (\log_2 b) + (\log_2 q) \rfloor + 1$

$\geq \lfloor \log_2 b \rfloor + \lfloor \log_2 q \rfloor + 1$

$= l(b) + l(q) - 1$

so $l(a) \geq l(b) + l(q) - 1$

so $l(q) \leq l(a) - l(b) + 1$

<2> $\exists r \in \mathbb{Z}$, $0 \leq r < b$

s.t. $a = bq + r < bq + b = b(q+1)$

so $l(a) = \lfloor \log_2 a \rfloor + 1 = \lfloor \log_2 (bq + r) \rfloor + 1$

$< \lfloor \log_2 b(q+1) \rfloor + 1 = \lfloor \log_2 b + \log_2 (q+1) \rfloor + 1$

$\leq (\lfloor \log_2 b \rfloor + \lfloor \log_2 (q+1) \rfloor + 1) + 1$

since $a \geq b$ so $q \geq 1 \Rightarrow 2q \geq q + 1$

so $\lfloor \log_2 b \rfloor + \lfloor \log_2 (q+1) \rfloor + 2$

$\leq \lfloor \log_2 b \rfloor + \lfloor \log_2 (2q) \rfloor + 2 = \lfloor \log_2 b \rfloor + \lfloor \log_2 q + 1 \rfloor + 1$

$= \lfloor \log_2 b \rfloor + \lfloor \log_2 q \rfloor + 1 + 1$

$= l(b) + l(q) + 1$

so $l(a) < l(b) + l(q) + 1$

so $l(a) \leq l(b) + l(q) + 1$

so $l(a) - l(b) - 1 \leq l(q)$

above all $l(a) - l(b) - 1 \leq l(q) \leq l(a) - l(b) + 1$ □

NO

DATE

4. (1) $17x \equiv 11 \pmod{23}$

$d = \gcd(a, n) = \gcd(17, 23) = 1$

since $d \mid 11$ so x has a solution

notice that when $x = 2$

$17 \times 2 = 34$

$34 \bmod 23 = 11$

so 且 when $x = 2$, $17x \equiv 11 \pmod{23}$ is correct ⇒ so $x = 2$ is one of the solution

$\frac{n}{d} = \frac{23}{1} = 23$ so $x \equiv 2 \pmod{23}$

so let $x = 2 + 23z$, $z \in \mathbb{Z}$ is all the solutions

above all $x = 2 + 23z$, $z \in \mathbb{Z}$

(2) $55x \equiv 35 \pmod{75}$

$a = 55$, $b = 35$, $n = 75$

let $d = \gcd(a, n) = \gcd(55, 75) = 5$

$5 \mid 35$ so $d \mid b$ so the equation has solutions

let $t = (\frac{a}{d})^{-1} \pmod{\frac{n}{d}}$

$t = 11^{-1} \pmod{15}$

~~since~~ $\varphi(15) = (3-1) \times (5-1) = 8$

since $\gcd(t, \frac{n}{d}) = \gcd(11, 15) = 1$

notice that $11 \times 11 = 121 = 120 + 1 = 15 \times 8 + 1$

so $11 \times 11 \equiv 1 \pmod{15}$

NO

DATE

so $(11)^{-1} \pmod{15} = 11$

so $t = 11$

satisfied $(\frac{a}{d}) \cdot t \equiv 1 \pmod{\frac{n}{d}}$

so the solution

$x \equiv \frac{b}{d} \cdot t \pmod{\frac{n}{d}}$

$x \equiv \frac{35}{5} \times 11 \pmod{\frac{75}{5}}$

$x \equiv 77 \pmod{15}$

$x \equiv 2 \pmod{15}$

so $x = 2 + 15z, \ z \in \mathbb{Z}$

above all

$x = 2 + 15z, \ z \in \mathbb{Z}$

are the solutions of the equation

$55x \equiv 35 \pmod{75}$

5. Eve can learn the value m

since $\gcd(e_1, e_2) = 1$

so there exist $s, t \in \mathbb{Z}$ s.t.

$$e_1 s + e_2 t = 1$$

from RSA we know that

$$c_1 = m^{e_1} \pmod{N}$$

$$c_2 = m^{e_2} \pmod{N}$$

so $c_1^s \bmod N = (m^{e_1})^s \bmod N = m^{e_1 s} \bmod N$

$c_2^t \bmod N = (m^{e_2})^t \bmod N = m^{e_2 t} \bmod N$

so $(c_1^s) \cdot (c_2^t) \bmod N = (m^{e_1 s} \bmod N) \cdot (m^{e_2 t} \bmod N) \bmod N$

$$= m^{e_1 s} \cdot m^{e_2 t} \bmod N$$

$$= m^{e_1 s + e_2 t} \bmod N$$

since $e_1 s + e_2 t = 1$

so $(c_1^s)(c_2^t) \bmod N = m^1 \bmod N$

so $c_1^s \cdot c_2^t \equiv m \pmod{N}$

since $0 \le m < N$

so $m = c_1^s \cdot c_2^t \bmod N$

above all

we can compute m

by $m = c_1^s \cdot c_2^t \bmod N$