Fall 2025 CIS 3362 Homework #6: Public Key Encryption
Check WebCourses for the due date

1) (10 pts) In the Diffie-Hellman Key Exchange, let the public keys be p = 101, g = 61, and the secret keys be a = 47 and b = 91, where a is Alice's secret key and b is Bob's secret key. What value does Alice send Bob? What value does Bob send Alice? What is the secret key they share? Use a program or calculator to quickly simplify the modular exponentiations that arise, but show what each calculation is.

2) (10 pts) In an RSA scheme, p = 31, q = 29 and e = 187. What is d? Show the work by hand, but for any complicated calculation, do it on a calculator or use a program. (So, show each step of the Extended Euclidean Algorithm, but feel free to use a calculator to quickly get quotients and remainders.)

3) (40 pts) The following message below was encrypted using RSA with the following public keys:

```
n = 8026065103508817081150001
e = 1423281426182392320050 93
```

To convert from numbers to text, note that the text was encoded in Radix-64.

```
321251867927762668921327
447945021814250853925165
142942690680808870807566
737615056419979196859493
545746583621299804719191
205851239514859974899456
110167313188444538715684
535120815990806445465331
1019264475605962109133 5
745490068381463823869257
257313688759441542961519
219628179338693649269029
253414784759894255746286
31382609168188763125675
130438303509992733966181
754975772391654684650376
745790577930962533327692
767936391782179357220216
733728044739400315921725
708868149777974617770 33
151670069329711845671749
125329600979515468024668
799821373136048823636548
425749956533381805774782
319659447214924103523 20
237541203185932543303463
554091769301038245250950
106947523735492603333217
417201258432292229147661
116398916319937250554705
```

Try to break the message! Show all of your work. You may use/modify any code on the course webpage or write your own code only.

4) (40 pts) The following message was encrypted via El Gamal with the following Public Keys:

```
p = 6269871280021
g = 6207687755470
Alice Public = 4055297942248
```

To convert from numbers to characters, use the usual base 26 interpretation from class.

```
687654814464 5350053305360
5397230649283 1317878981464
2194911138406 2889771503479
4853169487835 2061534955667
3084573299729 4371393384712
2435906747036 1621032121550
2177303592559 2793972295377
1290751753565 1299087795122
1100562480797 3626083404392
3410291309909 2570140654106
5827535521467 4243754188867
5993491771416 4777251329063
526921499320 953075608732
1206289282988 2218173230892
1696659787694 2528477574286
4839364611449 3525863755566
1980389186399 4304901635591
1583387701095 2595777613654
4765830854317 2319258157170
5800625108860 3220357454447
2899732640862 6094681358901
731871741108 128496861031
```

Good luck!