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 = 97, g = 23, and the secret keys be a = 83 and b = 65, 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 = 41, q = 17 and e = 147. 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) (50 pts) The following message was encrypted via RSA encryption. The public keys are as follows:

n = 153535199189155511054009430409868302266002806975797 7
e = 730215628455429163275499063151379643457490494895 59

Each integer in the ciphertext corresponds to a plaintext of 28 characters. In your write up, describe in detail what steps you took and which code (if you used any of the posted code) you used, or how you adapted it. Turn in attachments of any original code you wrote or anything that had non-trivial adaptations of the code posted for the class. Here is the ciphertext:

```
74209613410074397133739562490961655593632344033729 7
10759875070311261566551052167597394824929977674703 82
37136178901187016506391578582062362009111877953861 0
16527039554841755410947604318288947923580200640535 6
23788029530914035386955677082663380642981449721503 1
34452111653937533859814646710843688867699154630088 7
47059433656921674929477576688864353985428489141812 9
12828010520733511993604930575344540972828800762460 52
34048644521542217089640587131226549853498074777866 1
```

4) (30 pts) The following ciphertext below was created with the El Gamal cryptosystem with the following public elements:

q = 1234567890133 (prime)
g = 726288716355 (primitive root)
Ya = 268931642640 (Alice's public exponent)

You also know that the plaintext was written in all lowercase letters and split into blocks of 8 characters and the value of each 8 character block is simply equal to its base 26 equivalent, treating A = 0, B = 1, …, Z = 25.

Use this information to decrypt the following ciphertext: (Note: This will also be given to you in a text file, for ease of processing and as mentioned, each line represents the encryption of one block of 8 characters.)

```
299335298747 1172223606113
889598930003 557439201934
493347324365 308563064395
89330316409 284568396280
1011600488984 284687286118
78301339268 445083507637
184420679506 945520081269
113325085374 330613800716
801254124539 2492123523
189525982163 429945730554
884843344510 169440640565
518889437424 634600793624
2248173165 323732777084
575687437463 568722795104
891109133954 753816562536
1124597795350 970569441767
608617739348 63349455224
771764120123 778305272817
181728415187 585124549217
492606809251 383617280481
458984069941 197980928842
1082309772979 255983715074
775217121216 504345290258
1114180621864 18900995437
139742778128 205760018212
1098177806924 464716156995
159086739222 63106975262
251212528964 496548036082
1207655912195 764037801281
544740425341 289356820759
1073938227507 329586495737
989432039687 1210124857313
1190570442012 1222786515110
```

Good Luck!