Fall 2023 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 = 79, g = 48, and the secret keys be a = 36 and b = 67, 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 = 47, q = 31 and e = 119. 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) Alice and Bob both have their own RSA keys and have each sent a message to one another.

Here are Bob's Public Keys:

n = 4751614356616424867781976168280737158143706077825299390190036646711989408286996041120433429097816319
e = 4685895394525945948602630590450251030824289205

Here are Alice's Public Keys:

n = 5027378074612278683849377061501198168112765099092211588948671006054146262763926543857634165199504551
e = 57323338227899193769901534310113340374743309

You have intercepted two ciphertexts, one sent from Alice to Bob (using Bob's public key):

C = 1046284573466962387739473944807380691612565121927521278523282411305437337626467565825335153065591711

And another one sent from Bob to Alice (using Alice's public key):

C = 3325523873963550704984437728904370519830678404172921362089587136490304638487650626956531260800780164

Normally, you would be out of luck in cracking these messages, but Alice and Bob have poorly constructed their RSA keys. Determine, in text, what each of the ciphertexts decrypt to. (Note: a modified version of RSA2BigInt.java was used to create this problem. As such, this code should explain how to convert an integer plaintext to uppercase letters.)

4) (40 pts) The following ciphertext below was created with the El Gamal cryptosystem with the following public elements:

q = 208827064597 (prime)
g = 148730885957 (primitive root)
Ya = 22100313146 (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.)

```
111537273770 135478365325
135874735585 91980775319
114008480727 189673465227
51859330405 168411804286
147104771103 105548487980
1785731042 1829176754
177464475649 64097517903
31371229910 160373635219
155078142943 88685005036
92163822772 83821102277
114922855196 109868919775
139345072195 37637914660
180092093087 72241715608
54004792799 102543868605
180382625017 101039780617
52988886207 106664942086
196270659674 1848943199
35121652348 107823603240
158294360726 126547219134
84120560054 82845406333
106816610946 160475344872
109119061605 199945687440
135206784648 11466088841
104712202700 173240884045
126757086234 179687780957
```

Good Luck!