Kevin Lee
CS 460
Homework #2

RSA Encryption
Output & Summary

512 bits:

```
------Key Generation------
Please enter a key length: 512
[n]:
113229599506923118020049393332950423391784533130419238399760977037460500794589224437680553153013757812547881806442558343182718524552850953961409406358572 01.

[p]:
115783205427808964776896910464961021850473527277848329522309996106344963928899.

[q]:
977944936733695591059162152898623987654618104767223672879883821311473109238 99.

[d]:
666056467687783047176761137252649549363438430178936696469182217867414710556394639180526713928087821654649021013155288175324545985792635118700202844764965.

[e]: 17.


[Elapsed Time]: 0.019982s
Signing  OK
Verify Signature OK


------Encryption & Decryption------
Please enter plaintext to encrypt: Hello
[Plain Text]: Hello
```

```
Encrypting 100 times...DONE
[Elapsed Time]: 0.006735s
[Ciphered Text]:
2b9d82fba712cb8756df75b3764c25d4f22551d893b914666dfeea86df6f653f97caa7
585b8d027f820ad6ad825169ec836827d4b759251e582bda2d2909b008

Decrypting 100 times...DONE
[Decrypted Text]: Hello
[Elapsed Time]: 0.029814s
```

1024 bits:

```
------Key Generation------
Please enter a key length: 1024
[n]:
152414652832910725890968299136988109384173364672996554125838034537498048252200182675526864064569536774378943174513136349620339215202786428479518722593063573684641629699627541720097100807711366872387078606699647322140246302608670386986570978033814807828699464640415039015802906354276977193884466704569232179791.

[p]:
120803133924051418278910065205570138613753160472619036858125445812297961602418172039844182384455113186597102928057394158469152481728759076288307195893908 33.

[q]:
126167797044680461961480512104952735551123498705231623817149665648324032458232697121113105623938358484201003715418554837204399502138601340736877158413681 27.

[d]:
358622712548025237390513645028207316198054975701168362649030669499995407652235723942416150740163615939715160410619144352047856976947732772892985229630737762323643606650445923955386752365703412669932143109726070105009647624492386639763893840717679925838899729011178097460949032939008448136100621614432473931 37.
```

```
[e]: 17.


[Elapsed Time]: 0.039981s
Signing  OK
Verify Signature OK


------Encryption & Decryption------
Please enter plaintext to encrypt: Hello
[Plain Text]: Hello

Encrypting 100 times...DONE
[Elapsed Time]: 0.008954s
[Ciphered Text]:
8c6a17d6ab5e2b838575a5dc6c8689ecc5cf56f3a74fc4b19a0c11a4524d16d8eb4158
76ca7b09e68c439d72fdc2a95377dbe5e265aa8949c9cf4e9e8ac8e8457febdbb7a8c0
b418756e57f65e6e9e1b7413aeebb9a5f0bda43d2ef37584bc8e1e1fccac13bee6787f
c340c97b2e56a463770f8e180b48c7da59a8cc9e5ea1d5

Decrypting 100 times...DONE
[Decrypted Text]: Hello
[Elapsed Time]: 0.071327s
```

2048 bits:

```
------Key Generation------
Please enter a key length: 2048
[n]:
311027825221693175556475416225908236071000203805634047254898933867031905
058231527342342583477523413827104615671651296656828445512612182172540066
628715993078910808772318735560512146228129030514259096810752528393401350
919648864256972083811967675733801346947533126520888912494801094320603
686341033443406818686829241303148686618397532767229621103618377841889
752287391086574206557832765543195589468436989753349597058278447434308123
680575109933660458578503674684952861733438882276757608195289277411083
272459991116071092610987073280243790092667673043576078727074750443961
651842244393628785790041838602176434807188312312319988 61.
```

[p]:
175067881504181711933621297898863115378031746901484197079478954408031559368374288327296714120032955359987175664135893789550725211772208070528145284357741982018977247341067406253011266025967060322148273981461927810884768218591052109447327855576552359745123460322040149158043120296360999978981670796499759923049.

[q]:
177661272044503430483316277207870968916085068951378416814919853498300119579075708101512266638879762780280166495825478849113670555871034030272803487709972681941236598681360462533102497200793667200834015250835173711247649654008156175531987453340027569093860094617171165646558614393016527725089661471552035027589.

[d]:
274436316372082213726301837846389620062647238652030041695499059294439916902781824324345600957948278862171971028055587367215780524604309341770554749405657862478328516531376922481965996203394934497185958113288295309634984291991445956304677360941589423777235111636078452201295083224062076183264803006016488378739213991603939599507586341650032009589618283759198910247909016304796572429753902503660794069788649891360977070036920547813352331750611315437351644616633458940541298497691691118896711868533693572840807235548249462993164362970596108994514346151096133372563367317222600424182152377892494322994788704969230326896 1.

[e]: 17.

[Elapsed Time]: 0.130955s
Signing OK
Verify Signature OK

------Encryption & Decryption------
Please enter plaintext to encrypt: Hello
[Plain Text]: Hello

Encrypting 100 times...DONE

```
[Elapsed Time]: 0.016217s
[Ciphered Text]:
14ac41ba7ec90bd0c7f3e07ef75ae92c7cf91cbd8769b26214ada1ceb2d7e70ae10aec
cb8efbf387054f4f55386f093f5acc959a99aba89a489d6ab81ad564d547d54290e6e6
94734318f5261b9857916b2a584646c08a0b9691078fb8749e8c0ea8e94018764b4d95
756dcd5f53410655f350d090c104296468adba8e43cb588554d3ff5802d90c472205b6
e1d518d8e1fcb8039cf096a2a63c3ac1e113cd632959108677ddf6a9a0fd968187e4eb
598f552b8c4b600eb41c0b5044a934f4dfe25dd159bed6adfad37d836966824ef6cb5b
09e0b238e9ba3474e41c538ad89787e7727a8abcf9eddc345722ccd451dc9607e79949
010e4785af97eb182fed8b

Decrypting 100 times...DONE
[Decrypted Text]: Hello
[Elapsed Time]: 0.313323s
```

Between these three key lengths, decryption seems to take much longer than encryption. This might be because of the fact that the decryption method has to deal with a long ciphertext where the encryption method only has to deal with the length of the string, which in this case is much shorter than the ciphertext. Moreover, decryption is much much slower than encryption, because the decryption exponent is huge whereas the encryption exponent is typically small. It seems as that with every doubling of the RSA key length, decryption is significantly slower. With usual implementations of RSA, doubling the key length means that *encryption* will be somewhere around 4 times slower, and *decryption* will be around 8 times slower. The theory says that for a *n*-bit key, the computational effort for encryption is proportional to n^2, while the effort for decryption is proportional to n^3. We can see that here between these three key lengths.