Math 116 Spring, 2012

Professor K. A. Ribet

Assignment due January 26, 2012

This part of the assignment does not have to be turned in; the aim is to get people to learn a bit about sage.

First, learn about `ShiftCryptosystem` and `SubstitutionCryptosystem` by "introspection": typing the command, followed by a question mark, and then evaluating the cell. You can also search for "sagemath SubstitutionCryptosystem" (for example) on google.

Next, take the string `enemyfallingbackbreakthroughimminentlucius` that's introduced at the very beginning of Chapter 1 of the book. Using the shift ciphersystem of sage, shift it 5 letters forward (thereby getting `jsjrdkf`...) and shift the resulting ciphertext back 5 letters to recover the original message.

Finally, do an example of the substitution cipher: Introduce the key `CISQVNFOWAXMTGUHPBKLREYDZJ` at the top of page 4 of the book and use sage to compute the inverse key `JRAXVGNPBZSTLFHQDUCMOEIKWY` in the second table at the top of page 4. Then encrypt `NEEDNEWSALADDRESSINGCAESAR` and decrypt the resulting ciphertext `GVVQGV`... to recover the urgent request in the original message.

Problems from Chapter 1 of the book:

1.5, 1.7 (using sage as your calculator), 1.8 (ditto), 1.9d (use sage to do the long divisions and continue your calculations to carry out an "extended gcd"—then do an `xgcd` with sage to check your calculations), 1.11, 1.13, 1.17efg, 1.18