Topics in Data Science, Data Protection — Spring 2020
CS 4364 — L. Longpré

Assignment 1, due 2/13/2020

In this assignment, you will create an RSA key pair, and you will practice encrypting and decrypting.

1. Create an RSA key pair. It could be 512, 1024 or 2048 bits.
2. Access the web page http://cssrvlab01.utep.edu/Classes/cs5339/longpre/. You probably have to VPN to UTEP if you're not at UTEP. (cs5339 was created the first time I set up a web site for a course, and was used since then to all my courses that need a website.)
3. Click on "Message Request".
4. A password was assigned to you for this course.
5. Enter your UTEP username, the password we assigned to you for the course, and the public key you generated and submit.
6. The next page should display a base64 encoded encrypted message.
7. Use your RSA private key to decrypt the message.
8. Go back to http://cssrvlab01.utep.edu/Classes/cs5339/longpre/.
9. Reenter your username and password, paste your decrypted message, and submit.
10. The next page will tell you if the decrypted message is correct.
11. The back-end database will keep track of your success, so you don't need to submit anything. Please copy and save the successful page just in case something goes wrong in our tracking.