Math 259 - Spring 2019
Review for Final Exam
RSA and DLP

For each of RSA and DLP you should be able to

- Set up the cryptoscheme (either explain the elements of the scheme, or generate an instance of the scheme)
- Encrypt some data
- Decrypt some data

You could also be asked a "simple proof" using the formulae for encryption and decryption (as in Quiz 1, problem 5 for example).

In addition, you could be asked about the log rules for the discrete log.

Finally, you could be asked problems that apply the ideas covered in Homework 1, problems 3, 4 and 5. Here are some sample problems in that vein:

1. (Homework 1, problem 3) Someone who cares very much about you tells you that

$$71^2 \equiv 12^2 \pmod{4897}.$$

   Use this information to factor 4897.

2. (Homework 1, problem 4) Suppose that three individuals set up an RSA problem, each with encryption exponent $e = 3$, but with different values of N. Specifically, let $N_1 = 51$, $N_2 = 65$ and $N_3 = 77$. Suppose that the same message m is sent to each of these three people, resulting in the respective ciphertexts

$$\begin{aligned} c_1 &\equiv 23 \pmod{51} \\ c_2 &\equiv 60 \pmod{65} \\ c_3 &\equiv 48 \pmod{77}. \end{aligned}$$

   A person who cares very much about you tells you that

$$\begin{aligned} 125 &\equiv 23 \pmod{51} \\ 125 &\equiv 60 \pmod{65} \\ 125 &\equiv 48 \pmod{77}. \end{aligned}$$

   What is the message m?

3. (Homework 1, problem 5) Suppose that two individuals set up an RSA problem, both with modulus $N = 39$, but with different encryption exponents e and f. Specifically, let $e = 3$ and $f = 5$. Suppose that the same message m is sent to each of these two people, resulting in the respective ciphertexts

$$\begin{aligned} c_1 &\equiv 31 \pmod{39} \\ c_2 &\equiv 37 \pmod{39}. \end{aligned}$$

   A person who cares very much about you tells you that

$$2 \cdot 3 - 5 = 1.$$

   What is the message m?