Please write your hackerrank username somewhere on your problem set.
Written problems are due at the beginning of class on Friday, October 23. Programming problems must be electronically submitted by 10:50am according to the instructions on problem set 1. The submission page for the programming questions is the following.

`https://www.hackerrank.com/math158-problem-set-5/`

You should use a calculator or computer for the arithmetic in several of the written problems.

Written problems

1. Textbook exercise 3.1 (same in first edition).
2. Textbook exercise 3.2 (same in first edition).
3. Textbook exercise 3.7 (3.6 in first edition).
4. Textbook exercise 3.8 (3.7 in first edition).
5. Textbook exercise 3.13 (3.12 in first edition).
6. The textbook mentions that choosing $e = 3$ as the encryption exponent can help increase the efficiency of RSA encryption, likely without compromising security. If Bob chooses $e = 3$ in his public key, what conditions should he be sure to satisfy when choosing his modulus in order to have a valid public key?
7. Textbook exercise 3.11(a) (3.10(a) in first edition). You should also solve part (b), but you don't need to write it up; instead you will write a program to break the cryptosystem in the first programming problem.

Programming problems

8. Write a program to break the cryptosystem described in problem 3.11 (3.10 in first edition). Your program will receive a public key (but not the corresponding private key) and a cipher text, and it should print the original plaintext.
9. Write a program which determines the two prime factors p, q of an RSA modulus $N = pq$, given N and $\phi(N)$. This demonstrates that computing phi is not any easier than factoring.
10. Implement the Pohlig-Hellman algorithm. You have written all of the main ingredients in previous programming problems. Specifically, you will be given a discrete logarithm problem for with the modulus p is a "weak prime" in the sense that $p - 1$ factors into small prime powers (all 16 bits or smaller).
11. Write a program to print the last five digits of F_n, the n^{th} Fibonacci number. These are defined by $F_0 = 0,\ F_1 = 1$, and the recurrence $F_n = F_{n-1} + F_{n-2}$ for $n > 1$.

    Hint. Express the *vector* $\binom{F_n}{F_{n+1}}$ in terms of the vector $\binom{F_{n-1}}{F_n}$ using a matrix equation. Using this equation, try to reformulate the problem in terms of one of the programming problems from last week.