1. (Simpler version of Exercise 9.1, pp. 161) Investigate the random number generator built into the Java system that is available in the linux lab. Would you use this random number generator for cryptographic purposes? Justify your answer.

2. (Exercise 9.6, pp. 161) Implement a naive approach for generating random numbers in the set $0, 1, \ldots, 191$. For this naive approach, generate a random 8-bit value, interpret that value as an integer, and reduce that value modulo 192. Experimentally generate a large number of random numbers in the set $0, 1, \ldots, 191$ and report on the distribution of results.

3. (Exercise 10.3, pp. 179) Compute the result of $12358 \times 1854 \times 14303 \pmod{29101}$ in two ways and verify the equivalence: by reducing modulo 29101 after each multiplication and by computing the entire product first and then reducing modulo 29101.

4. (Exercise 10.9, pp. 180) Compute $27^{35} \pmod{569}$ using the exponentiation routine described in Section 10.4.2. How many multiplications did you have to perform?

Undergraduates are required to solve at least one of the following two questions. Graduate students must solve both.

5. (Exercise 10.8) Give pseudocode for the exponentiation routine described in Section 10.4.2. Your pseudocode should not be recursive but should instead use a loop.

6. (Exercise 11.3, pp. 193) Why is a number $r$ a square modulo $p$, $p = 2q + 1$ and $p$ and $q$ both prime, if and only if $r^q \equiv 1 \pmod{p}$. 