Suggested reading: Trappe-Washington 6.3–6.4, Koblitz V.2.

For this assignment, please write out your steps to show how you are applying the alogrithms. You are welcome to use computer software for the computations.

1. (a) Describe the Solovay-Strassen primality test (Chapter 6.3) and explain why it works.

   (b) Use the test on $n = 804\,509$. Is n composite, prime, or inconclusive?

2. (a) Describe the $(p-1)$ factoring algorithm (Chapter 6.4) and explain why it works. What must be true of the factors of n for this algorithm to succeed quickly?

   (b) By choosing a base a and testing some small values of B, use the algorithm to find a factor of 49349.

3. (a) Describe the Quadratic Sieve factorization method (Chapter 6.4) and explain why it works.

   (b) Let $n = 4181$. Find a factor of n using the following:

$$\begin{aligned} 65^2 &\equiv 44 \pmod{4181} \\ 66^2 &\equiv 175 \pmod{4181} \\ 67^2 &\equiv 308 \pmod{4181} \\ 145^2 &\equiv 120 \pmod{4181} \\ 429^2 &\equiv 77 \pmod{4181} \\ 497^2 &\equiv 330 \pmod{4181} \\ 688^2 &\equiv 891 \pmod{4181} \end{aligned}$$

4. (a) Describe the Pollard rho algorithm.

   (b) Using $x_0 = 1$ and $f(x) = x^2 + 1$, find a factor of $n = 403$. At each step i, you may compute just $\gcd(x_i - x_{i-1}, n)$ (instead of performing all computations $\gcd(x_i - x_j, n)$ with $j < i$).