Applied Cryptography: Homework 9

(Deadline: 2:30pm, 2022/05/18)

Justify your answers with calculations, proofs, and programs.

1. (30 points, question 6.21, page 251 of the textbook) Write a program to evaluate Jacobi symbols using the four properties presented in Section 6.4. The program should not do any factoring, other than dividing out powers of two. Test your program by computing the following Jacobi symbols:
$$\left(\frac{610}{987}\right), \left(\frac{20964}{1987}\right), \left(\frac{1234567}{11111111}\right)$$

2. Applications of the Pollard $p-1$ algorithm and Pollard Rho algorithm.

   1) (10 points, question 6.26, page 253 of the textbook) Using various choices for the bound, B, attempt to factor 262063 and 9420457 using the $p-1$ method. How big does B have to be in each case to be successful?

   2) (10 points, question 6.27, page 253 of the textbook) Factor 262063, 9420457, and 181937053 using the Pollard Rho Algorithm, if the function f is defined to be $f(x) = x^2 + 1$. How many iterations are needed to factor each of these three integers?