Applied Cryptography: Homework 10

(Deadline: 3:00pm, 2022/05/25)

Justify your answers with calculations, proofs, and programs.

1. (20 points, question 6.28, page 253 of the textbook) Suppose we want to factor the integer $n = 256961$ using the RANDOM SQUARES ALGORITHM. Using the factor base

   $$\{-1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31\},$$

   test the integers $z^2 \bmod n$ for $z = 500, 501, \cdots$, until a congruence of the form $x^2 \equiv y^2 \pmod{n}$ is obtained and the factorization of n is found.

2. (10 points, question 7.9, page 304 of the textbook) Decrypt the ElGamal ciphertext presented in Table 7.4 (page 305 of the textbook). The parameters of the system are $p = 31847, \alpha = 5, a = 7899$ and $\beta = 18074$. Each element of $\mathbb{Z}_n$ represents three alphabetic characters as in Exercise 6.13 (page 247 of the textbook).

   The plaintext was taken from *The English Patient*, by Michael Ondaatje, Al- fred A. Knopf, Inc., New York, 1992.

3. (10 points, question 7.1, page 302 of the textbook) Implement SHANKS' ALGORITHM for finding discrete logarithms in ${\mathbb{Z}_p}^*$, where p is prime and α is a primitive element modulo p. Use your program to find $\log_{106} 12375$ in ${\mathbb{Z}_{24691}}^*$ and $\log_6 248388$ in ${\mathbb{Z}_{458009}}^*$.

4. (10 points, question 7.3, page 303 of the textbook) The integer $p = 458009$ is prime and $\alpha = 2$ has order 57251 in ${\mathbb{Z}_p}^*$. Use the POLLARD RHO ALGORITHM to compute the discrete logarithm in ${\mathbb{Z}_p}^*$ of $\beta = 56851$ to the base α. Take the initial value $x_0 = 1$, and define the partition (S_1, S_2, S_3) as in Example 7.3 (page 261 of the textbook). Find the smallest integer i such that $x_i = x_{2i}$, and then compute the desired discrete logarithm.