Applied Cryptography: Homework 10

(Deadline: 10:00am, 2020/12/02)

Justify your answers with calculations, proofs, and programs.

1. (15 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 $\mathbb{Z}_{458009}^*$.

2. (15 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. Find the smallest integer i such that $x_i = x_{2i}$, and then compute the desired discrete logarithm.

3. (15 points, question 7.5, page 303 of the textbook)

   Implement the POHLIG-HELLMAN ALGORITHM for finding discrete logarithms in $\mathbb{Z}_p^*$, where p is prime and α is a primitive element. Use your program to find $\log_5 8563$ in $\mathbb{Z}_{28703}^*$ and $\log_{10} 12611$ in $\mathbb{Z}_{31153}^*$.

4. (15 points, question 7.6, page 303 of the textbook)

   Let $p = 227$. The element $\alpha = 2$ is primitive in $\mathbb{Z}_p^*$.

   (a) Compute $\alpha^{32}, \alpha^{40}, \alpha^{59}$, and α^{156} modulo p, and factor them over the factor base $\{2, 3, 5, 7, 11\}$.

   (b) Using the fact that $\log 2 = 1$, compute $\log 3, \log 5, \log 7$, and $\log 11$ from the factorizations obtained above (all logarithms are discrete logarithms in $\mathbb{Z}_p^*$ to the base α).

   (c) Now suppose we wish to compute $\log 173$. Multiply 173 by the "random" value $2^{177} \bmod p$. Factor the result over the factor base, and proceed to compute $\log 173$ using the previously computed logarithms of the numbers in the factor base.