Applied Cryptography: Homework 11

(Deadline: 3:00pm, 2022/06/01)

Justify your answers with calculations, proofs, and programs.

1. (25 points, question 7.6, page 303 of the textbook) Let $p = 227$. The element $\alpha = 2$ is primitive in ${\mathbb{Z}_p}^*$.

   (a) Compute α^{32}, α^{40}, α^{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.

2. (25 points, question 8.3, page 334 of the textbook) Suppose that Alice is using the *ElGamal Signature Scheme*. In order to save time in generating the random numbers k that are used to sign messages, Alice chooses an initial random value k_0, and then signs the ith message using the value $k_i = k_0 + 2i \mod (p-1)$. Therefore,

$$k_i = k_{i-1} + 2 \mod (p-1)$$

   for all $i \geq 1$. (This is not a recommended method of generating k-values!)

   (a) Suppose that Bob observes two consecutive signed messages, say $(x_i, \mathbf{sig}(x_i, k_i))$ and $(x_{i+1}, \mathbf{sig}(x_{i+1}, k_{i+1}))$. Describe how Bob can easily compute Alice's secret key, a, given this information, without solving an instance of the **Discrete Logarithm** problem. (Note that the value of i does not have to be known for the attack to succeed.)

   (b) Suppose that the parameters of the scheme are $p = 28703$, $\alpha = 5$, and $\beta = 11339$, and the two messages observed by Bob are

$$\begin{aligned} x_i &= 12000 \qquad \mathbf{sig}(x_i, k_i) = (26530, 19862) \\ x_{i+1} &= 24567 \quad \mathbf{sig}(x_{i+1}, k_{i+1}) = (3081, 7604). \end{aligned}$$

   Find the value of a using the attack you described in part (a).