Applied Cryptography: Homework 11

(Deadline: 10:00am, 2020/12/09)

Justify your answers with calculations, proofs, and programs.

1. (10 points, question 8.1, page 334 of the textbook)

   Suppose Alice is using the *ElGamal Signature Scheme* with $p = 31847, \alpha = 5$, and $\beta = 25703$. Compute the values of k and a (without solving an instance of the **Discrete Logarithm** problem), given the signature $(23972, 31396)$ for the message $x = 8990$ and the signature $(23972, 20481)$ for the message $x = 31415$.

2. (20 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 $k_i = k_0 + 2i \bmod (p-1)$. Therefore,

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

   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

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

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

3. (15 points, question 8.7, page 336 of the textbook)

   Suppose Alice uses the *DSA* with $q = 101, p = 7879, \alpha = 170, a = 75$, and $\beta = 4567$, as in Example 8.4. Determine Alice's signature on a message x such that SHA3-224$(x) = 52$, using the random value $k = 49$, and show how the resulting signature is verified.

4. (15 points, question 8.8, page 336 of the textbook)

   We showed that using the same value k to sign two messages in the *ElGamal Signature Scheme* allows the scheme to be broken (i.e., an adversary can determine the secret key without solving an instance of the **Discrete Logarithm** problem). Show how similar attacks can be carried out for the *Schnorr Signature Scheme*.