EE 418 - Assignment 5

Total Points: 100
Autumn Quarter, 2021
Prof. Radha Poovendran
Department of Electrical and Computer Engineering
University of Washington, Seattle, WA 98195

Due: 11:59 pm (PST) on Dec 9 (Thur), 2021 via Canvas

Notes:

- This homework contains both computation questions (marked as **[Com]**) which are required to do by hand calculations and programming questions (marked as **[Pro]**) which are required to write Python /MATLAB codes. Zero points will be awarded if **[Com]** questions are solved via Python/MATLAB scripts and if **[Pro]** questions are solved by hand calculations.
- **Your answers to this homework must be submitted through canvas as a single zip file containing the following:** *i*) **hand written and scanned or word or pdf answers to all the computational and discussion questions as single pdf file.** *ii*) **Python/MATLB codes for programming questions as in filename.py or filename.m respectively.**
- **Name of your submission zip file should follow the following format. "*#_$_EE418_HW5.zip*", where "#" and "$" should be replaced with your first name and last name, respectively.**
- Show the computation steps and/or justify your answers in all the **[Com]** questions. Failure to show computation steps in **[Com]** questions will result zero points.
- You can use and modify the Python functions provided in the file section of the EE 418 canvas page when answering the **[Pro]** questions below.
- You can discuss with others but you need to write your own computation steps for **[Com]** questions and Python/MATLAB codes for **[Pro]** questions.

1. **[Com]**(Digital Signatures, 20 pts): Here we consider a variation of the *ElGamal Signature Scheme*. The key is constructed in a similar manner as in the original *ElGamal Signature Scheme*: "A" chooses $\alpha \in \mathbb{Z}_p^*$ to be a primitive element, $0 \leq a \leq p-2$ where $\gcd(a, p-1) = 1$, and$\beta = \alpha a \bmod p$. The key $K = (\alpha, a, \beta)$, where α and β are the public key and a is the private key. Let $x \in \mathbb{Z}_p$ be a message to be signed. "A" computes the signature $\mathbf{sig}(x) = (\gamma, \delta)$, where

$$\gamma = \alpha^k \bmod p$$

and

$$\delta = (x - k\gamma)a^{-1} \bmod (p-1)$$

The only difference from the original *ElGamal Signature Scheme* is in the computation of δ. Answer the following questions concerning this modified scheme.

   (a) (10 pts) Provide a verification equation for the modified scheme and show how a signature (γ, δ) on a message x would be verified using "A"'s public key and your suggested verification equation.

   (b) (5 pts) Describe a computational advantage of the modified scheme over the original scheme.

   (c) (5 pts) Briefly compare the security of the original and modified scheme.

2. **[Com]**(Digital Signatures, 10 pts $\times$ 3 = 30 pts):

   (a) Suppose "A" uses the *DSA* with $q = 101, p = 7879, \alpha = 170, a = 75, and \beta = 4567$. Determine "A" 's signature on a message x such that SHA-1$(x) = 52$, using the random value $k = 49$, and show how the resulting signature is verified.

   (b) In Quiz 14, Question 3, 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* and the *DSA* when the same value k is used to sign two messages.

   (c) Here, we describe a potential attack against the *DSA*. Suppose that the message x is given, let $z = (\text{SHA-1}(x))^{-1} \bmod q$, and let $\epsilon = \beta^z \bmod p$. Now suppose it is possible to find $\gamma, \lambda \in \mathcal{Z}_q^*$ such that

$$\gamma = \left((\alpha\epsilon^\gamma)^{\lambda^{-1} \bmod q}\right) \bmod p \bmod q$$

   and

$$\delta = \lambda(\text{SHA-1}(x)) \bmod q$$

   Show that (γ, δ) is a valid signature for x.

3. **[Com]**(Digital Signatures, 10 pts $\times$ 2 = 20 pts): Consider the El-Gamal signature scheme. The public key is given as (p, α, β), where p is a large prime number, α is a generator of $\mathbb{Z}_p^*$, and $\beta = \alpha^a \bmod p$ where a is the secret signing key. Recall that in El-Gamal signature scheme, signature consists of (γ, δ) where $\gamma = \alpha^k \bmod p$, and $\delta = (m - a\gamma)k^{-1} \pmod{p-1}$, where k is a randomly chosen integer in $\mathbb{Z}_{p-1}^*$.

   (a) Let the public key be $(p, \alpha, \beta) = (13, 7, 5)$. "A" signs $m_1 = 2$, yielding $(\gamma_1, \delta_1) = (11, 1)$ and signs $m_2 = 1$, yielding $(\gamma_2, \delta_2) = (11, 8)$. "E" is able to observe these two messages and the corresponding signatures. Show that "E" can recover the secret key a without solving the discrete log problem. What is a?

   (b) Suppose that "A" accidentally chooses $k = a$. Explain how "E" can immediately notice this and retrieve the secret key a given a single signature (m, γ, δ).

4. **[Com]**(Digital Signatures, 10 pts $\times$ 2 = 20 pts): This question deals with the variants of El-Gamal and Schnorr's signature schemes.

   (a) We consider following variation of the El-Gamal signature scheme. In the modified version, the public and private keys are same as the original El-Gamal, so that the public key is given as (p, α, β), where p is a large prime number, α is a generator of $\mathbb{Z}_p^*$, and $\beta = \alpha^a \bmod p$ where a is the secret signing key. Recall that in the original El-Gamal, $\delta = k^{-1}(m - a\gamma) \pmod{p-1}$. In the modified scheme, however, we let $\delta = a\gamma + km \pmod{p-1}$. Signature for message m is given as $sig(m) = (\gamma, \delta) = (\alpha^k \pmod p, a\gamma + km \pmod{p-1})$. How is a signature verified in this scheme? Draw the schematic diagram of the verification process.

   (b) We consider the following variation of the Schnorr signature scheme. In the modified version, the public and private keys are same as the original Schnorr, so that the public key is given as (p, q, α, β), where p is a large prime number, q is another prime number such that $q|(p-1)$. α is a generator of $\mathbb{Z}_p^*$, such that $\alpha^q = 1 \bmod p$. $\beta = \alpha^a \bmod p$ where a is the secret signing key. Recall in the original Schnorr scheme, $\gamma = h(m||\alpha^k \bmod p)$. In the modified scheme, we let $\gamma = m^{-1}\alpha^{5k} \bmod p$. δ is same as the original Schnorr signature scheme where $\delta = k + a\gamma \bmod q$. The signature is given as γ, δ. How is a signature verified in this scheme? Draw the schematic diagram of the verification process.

5. **[Com]** (Digital Signatures, 10 pts): "A" wants to prove to "B" that she knows that value x such that $g^x = y \bmod p$, where p is a large prime number. "B" knows values of g, y, p. However, "A" does not want to reveal the secret x to "B". Instead, "A" and "B" do the following

   (I) "A" chooses a random integer r, and sends $t = g^r \bmod p$ to "B".

   (II) "B" chooses a random integer c and sends it to "A".

   (III) "A" computes $s = r + cx \pmod{p-1}$ and sends it to "B".

   How can "B" verify that "A" knows x such that $g^x = y \bmod p$?