CO 485/685: Assignment #4 Due date: November 10 (Friday)

Some of these exercises are from the textbook. In such cases, the corresponding exercise number from the textbook is provided.

1. Recall that Schnorr signatures are obtained by applying the Fiat-Shamir transform to a zero-knowledge proof, in the following manner.

   Parameters: Group G of order q, with generator $g \in G$, and hash function $H\colon \{0,1\}^* \times G \to \mathbb{Z}/q$.

   Key generation: Choose $\alpha \leftarrow\!\$\, \mathbb{Z}/q$. The public key is $h = g^\alpha$. The private key is α.

   Signing: To sign $m \in \{0,1\}^*$, choose $r \leftarrow\!\$\, \mathbb{Z}/q$ and output $(b, r + b\alpha)$ where $b = H(m, g^r)$.

   Verification: Given a signature (σ_1, σ_2) for m, check whether the equation $H(m, g^{\sigma_2} h^{-\sigma_1}) = \sigma_1$ holds.

   Using the forking lemma, prove that Schnorr signatures are EUF-CMA under the discrete logarithm assumption for G and the random oracle assumption for H.

2. (Exercise 3.36)

   This exercise asks you to use the index calculus to solve a discrete logarithm problem. Let $p = 19079$ and $g = 17$.

   (a) Verify that $g^i \pmod p$ is 5-smooth for each of the values $i = 3030, i = 6892$, and $i = 18312$.

   (b) Use your computations in (a) and linear algebra to compute the discrete logarithms $\log_g(2), \log_g(3)$, and $\log_g(5)$. (Note that $19078 = 2 \cdot 9539$ and that 9539 is prime.)

   (c) Verify that $19 \cdot 17^{-12400} \pmod p$ is 5-smooth.

   (d) Use the values from (b) and the computation in (c) to solve the discrete logarithm problem $17^x \equiv 19 \pmod{19079}$.

3. In this problem we check that the DSA verification bounds check is mandatory. The DSA signature scheme is defined as follows.

   Parameters: Prime p, element $g \in (\mathbb{Z}/p)^*$ of prime order q, and hash function $H\colon \{0,1\}^* \to \mathbb{Z}/q$.

   Key generation: Choose $\alpha \leftarrow\!\$\, \mathbb{Z}/q$. The public key is $h = g^\alpha$. The private key is α.

   Signing: To sign $m \in \{0,1\}^*$, choose $k \leftarrow\!\$\, \mathbb{Z}/q$ and output (r, s) where

   $$r = (g^k \bmod p) \bmod q$$
   $$s = \frac{H(m) + \alpha r}{k} \bmod q$$

   Verification: Check the bounds

   $$0 \le r < q$$
   $$0 \le s < q$$

   and the congruence

   $$r \equiv (g^{\frac{H(m)}{s}} h^{\frac{r}{s}} \bmod p) \pmod q$$

   Suppose that the bounds checks are omitted in the verification algorithm. Show that the following procedure succeeds in forging signatures, and explain why bounds checking prevents such a forgery:

   - Choose $r' \leftarrow\!\$\, \mathbb{Z}/q$
   - Choose $s \leftarrow\!\$\, (\mathbb{Z}/q)^*$
   - Set $r'' = (g^{H(m)} h^{r'})^{s^{-1} \bmod q}$
   - Set $r = r' \bmod q$ and $r = r'' \bmod p$ (how is such an r constructed?)
   - Output (r, s)