Homework 8

Due: Thursday, June 2 at 12PM.

You may discuss the problems in general terms in a group of size at most three. You are expected to write up your solutions yourself. Please credit your collaborators on your submission. You may use your course notes and slides to solve these problems.

This complements the PlayCrypt version of this problem set. You need turn in only the latter, on Gradescope. This version is being given out so that you can see what the problems look like in mathematical notation. **Do not rename your homework files from `hw8.py`**. Submit the file in one Gradescope submission.

We suggest that you start with this version. Work out a solution using pencil and paper. Move to implementation in PlayCrypt only after that.

As usual our convention is that the running time of an adversary does not include the time taken by game procedures to compute responses to adversary queries.

Problem 1 [8 points] Let p be a prime of bit length $k \geq 1024$ such that $(p-1)/2$ is also prime, and let g be a generator of the group $G = \mathbb{Z}_p^*$. Let $q = p - 1$. Consider the digital signature scheme $\mathcal{DS} = (\mathcal{K}, \mathcal{S}, \mathcal{V})$ whose component algorithms are below, where the message m is in $\mathbb{Z}_q^*$:

Alg $\mathcal{K}$
$x \xleftarrow{\$} \mathbb{Z}_q$; $X \leftarrow \text{MOD-EXP}(g, x, p)$
$y \xleftarrow{\$} \mathbb{Z}_q$; $Y \leftarrow \text{MOD-EXP}(g, y, p)$
return $((X, Y), (x, y))$

Alg $\mathcal{S}((x, y), m)$
If $(m \notin \mathbb{Z}_q^*)$ then return $\perp$
$z \leftarrow (y + xm) \bmod q$
return z

Alg $\mathcal{V}((X, Y), m, z)$
if $(m \notin \mathbb{Z}_q^*)$ then return 0
if $(z \notin \mathbb{Z}_q)$ then return 0
if $((Y \cdot \text{MOD-EXP}(X, m, p)) \bmod p = \text{MOD-EXP}(g, z, p))$ then return 1
else return 0

1. Present in pseudocode an $\mathcal{O}(k^2)$-time adversary A making at most two queries to its **Sign** oracle and achieving $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{DS}}(A) = 1$. For operations other than integer addition, multiplication and mod, your adversary should invoke algorithms from Lecture 9 Slide 44, such as those used above.

Optional. Here are a few questions that may help you think about these problems. You do not need to include answers in your code.

m	$\gcd(m, q)$	Is m in $\mathbb{Z}_q^*$?
0		
1		
2		
3		

a	What is az in terms of x and y for a given m?
1	
2	
3	

Problem 2 [12 points] Let p be a prime of bit length $k \geq 8$ such that $(p-1)/2$ is also prime. Let g, h be two different generators of the group $G = \mathbb{Z}_p^*$. Let $\mathcal{CS} = (\mathcal{P}, \mathcal{C}, \mathcal{V})$ be the commitment scheme whose constituent algorithms are as follows, where the message M is in $\mathbb{Z}_{p-1}$:

Alg $\mathcal{P}$	**Alg** $\mathcal{C}((g,h), M)$	**Alg** $\mathcal{V}((g,h), (C_1, C_2), M, K)$
$\pi \leftarrow (g, h)$	$K \xleftarrow{\$} \mathbb{Z}_{p-1}$	If $(\{K, M\} \not\subseteq \mathbb{Z}_{p-1})$ then return 0
Return π	$C_1 \leftarrow (g^K \cdot h^M) \bmod p$	$C_1' \leftarrow (g^K \cdot h^M) \bmod p$
	$C_2 \leftarrow (M + K) \bmod (p-1)$	$C_2' \leftarrow (M + K) \bmod (p-1)$
	Return $((C_1, C_2), K)$	If $((C_1 = C_1')$ and $(C_2 = C_2'))$ then return 1
		Return 0

1. **[6 points]** Present in pseudocode an $\mathcal{O}(k^3)$-time adversary A making one query to its **LR** oracle and achieving $\mathbf{Adv}^{\text{hide}}_{\mathcal{CS}}(A) = 1$.

2. **[6 points]** Present in pseudocode an $\mathcal{O}(k)$-time adversary A such that $\mathbf{Adv}^{\text{bind}}_{\mathcal{CS}}(A) = 1$.

[**Optional.**] Here are a few questions that may help you think about these problems. You do not need to include answers in your code. You may start answering the questions by considering a smaller p, $p = 7$, $g = 3$, $h = 5$.

- Consider the powers of a generator g in $\mathbb{Z}_p^*$. What is the order of $\mathbb{Z}_{p-1}$?
- Given the theorem that for a finite cyclic group of order n, there exists exactly one subgroup of order d, for any divisor of n. (Wikipedia: `https://en.wikipedia.org/wiki/Subgroups_of_cyclic_groups#Finite_cyclic_groups`)
  What are the subgroups of $\mathbb{Z}_{p-1}$? (Are they cyclic, and why?)
- What is the order of $(p-1)/2 \bmod p-1$? Which subgroup(s) does it belong to?
- What is the value of $g^{(p-1)/2} \bmod p$, and why?
