Homework 5

Due: Thursday, May 12 at 12PM (noon).

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.

There are two Gradescope assignments that you need to submit. Problem 2 Part 1 is called `HW5 P2 Part1` on Gradescope; this should be a PDF writeup of your solution to Problem 2 Part 1 (no code) and Problem 3. Problem 1 and Problem 2 Part 2 is called `HW5 PlayCrypt` on Gradescope. This is for submitting your completed Python code for Problem 1 and Problem 2 Part 2, using PlayCrypt. **Do not rename your homework file from `hw5.py`**.

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 $p \geq 3$ be a prime and $g \in \mathbb{Z}_p^*$ a generator of $\mathbb{Z}_p^*$. Consider the key-generation and encryption algorithms below:

Alg $\mathcal{K}$	**Alg** $\mathcal{E}(X, M)$
$x \xleftarrow{\$} \mathbb{Z}_{p-1}$	if $M \notin \mathbb{Z}_p^*$ then return $\perp$
$X \leftarrow \text{MOD-EXP}(g, x, p)$	$y \xleftarrow{\$} \mathbb{Z}_{p-1}$; $Y \leftarrow \text{MOD-EXP}(g, y, p)$
return (X, x)	$Z \leftarrow \text{MOD-EXP}(X, y, p)$; $W \leftarrow (Z \cdot M) \bmod p$
	return (Y, W)

The message M must be in $\mathbb{Z}_p^*$, meaning the message space is $\mathbb{Z}_p^*$. We let k be the bit-length of p.

Specify an $\mathcal{O}(k^3)$-time decryption algorithm $\mathcal{D}$ such that $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ is an asymmetric encryption scheme satisfying the correct decryption property.

Problem 2 [12 points] Let p be a k-bit prime such that $q = (p-1)/2$ is also prime, and assume $k \geq 2048$. Let g be a generator of $\mathbb{Z}_p^*$. Let $h = g^2$. The quantities p, q, h are public and known. Let the family of functions $\mathcal{T}$: $(\mathbb{Z}_q^*)^2 \times \mathbb{Z}_q^* \to \mathbb{Z}_p^*$ be defined as

$$\mathcal{T}(K, M) = h^{1/K[0]+1/(M \cdot K[1])}.$$

The pseudocode is as follows:

Alg $\mathcal{T}(K, M)$ // Inputs are key $K \in (\mathbb{Z}_q^*)^2$ and message $M \in \mathbb{Z}_q^*$
$K[0], K[1] \leftarrow K$
$a \leftarrow K[0]$
$b \leftarrow (M \cdot K[1]) \bmod q$
$x \leftarrow \text{MOD-INV}(a, q)$; $y \leftarrow \text{MOD-INV}(b, q)$
$u \leftarrow \text{ADD}(x, y) \bmod q$
$W \leftarrow \text{MOD-EXP}(h, u, p)$
Return W

1. **[6 points]** This will check your understanding and also serves as a hint for the main problem in part **2**. Complete this before doing **2**; it will make the latter easier.

   (a) **[1 points]** What is the order of g? What is the order of h? (You may consider among the elements $x \in Z_p^*$, the number of x's that have $\text{DLog}_{G,g}(x)$ even, and the number of x's that have $\text{DLog}_{G,g}(x)$ odd.) (Write the numbers in terms of p and/or q.)

   (b) **[2 points]** let e be coprime to q ($e \in \mathbb{Z}_q^*$), and let $c = h^e$. Show that there exists an integer d, coprime to q ($d \in \mathbb{Z}_q^*$), such that $c^d = h$. We denote $1/e \coloneqq d$. This justifies the use of fraction notations like $1/K[0]$.

   (c) **[1 points]** Is 0 in $\mathbb{Z}_q^*$? (Use one sentence to justify your answer.)

   (d) **[1 points]** What is $\mathcal{T}(K, 1)$, $\mathcal{T}(K, -1)$, $\mathcal{T}(K, 2)$, $\mathcal{T}(K, -2)$? (You may include h, $K[i]$ in your answer.)

   (e) **[1 points]** show that with $h^{1/K[0]}$, $h^{1/K[1]}$ known, it is possible to create a valid mac.

2. **[6 points]** Specify in pseudocode a $\mathcal{O}(k^3)$-time adversary A that makes two **Tag** queries and achieves $\mathbf{Adv}^{\text{uf-cma}}_{\mathcal{T}}(A) = 1$. The messages in the **Tag** queries, as well as the one returned by A, must be in $\mathbb{Z}_q^*$. Your pseudocode should explicitly invoke algorithms from Lecture 9 Slide 32, such as those used in the pseudocode.

   Although not required in the PlayCrypt assignment, you are encouraged (both for understanding and as practice) to prove that the advantage and running time of your adversary are as required.

Problem 3 [0 points] How much time did you spend on Problem 1? How much time did you spend on Problem 2?
