Homework 5

Due: Wednesday, November 10 at 9PM.

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 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 $g \in \mathbf{Z}_p^*$ a generator of $\mathbf{Z}_p^*$. Consider the key-generation and encryption algorithms below:

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

The message M must be in $\mathbf{Z}_p^*$, meaning the message space is $\mathbf{Z}_p^*$. 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 q be a k-bit prime such that $p = 2q + 1$ is also prime, and assume $k \geq 2048$. Let g be a generator of $\mathbf{Z}_p^*$. The quantities p, q, g are public and known. Let the family of functions $\mathcal{T}$: $\mathbf{Z}_{p-1}^* \times \mathbf{Z}_{p-1}^* \to \mathbf{Z}_p^*$ be defined as follows:

Alg $\mathcal{T}(K, M)$ // Inputs are key $K \in \mathbf{Z}_{p-1}^*$ and message $M \in \mathbf{Z}_{p-1}^*$
$w \leftarrow (M \cdot K) \bmod (p-1)$; $x \leftarrow \text{MOD-INV}(w, p-1)$; $Y \leftarrow \text{MOD-EXP}(g, x, p)$
Return Y

1. **[Warm-up question]** This will check your understanding and also serves as a hint for the main problem in part **2**. Justify your answers carefully, and check them with us! Complete this before doing **2**; it will make the latter easier.

M	$\gcd(M, p-1)$	Is M in $\mathbf{Z}_{p-1}^*$?	Justification
0			
1			
2			
3			

2. Specify in pseudocode a $\mathcal{O}(k^3)$-time adversary A that makes one **Tag** query and achieves $\mathbf{Adv}_{\mathcal{T}}^{\text{uf-cma}}(A) = 1$. The message in the **Tag** query, as well as the one returned by A, must be in $\mathbf{Z}_{p-1}^*$. Your pseudocode should explicitly invoke algorithms from Lecture 9 Slide 35, such as those used above.

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?
