Homework 6

Due: Thursday, May 19 at Noon.

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.

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 [20 points] Let $\mathcal{K}_{\mathrm{rsa}}$ be a RSA generator with security parameter $k \geq 1024$. Consider the key-generation algorithm $\mathcal{K}$ and encryption algorithm $\mathcal{E}$ defined below:

Alg $\mathcal{K}$	**Alg** $\mathcal{E}((N,e),M)$ // $M \in \mathbb{Z}_N^*$
$(N,p,q,e,d) \xleftarrow{\$} \mathcal{K}_{\mathrm{rsa}}$	$U \xleftarrow{\$} \mathbb{Z}_N^*$
Return $((N,e),(N,d))$	$V \leftarrow \text{MOD-EXP}(U,e,N)$; $W \leftarrow (U \cdot M) \bmod N$
	Return (V,W)

1. [**8 points**] Specify in pseudocode 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 requirement, for messages that are in $\mathbb{Z}_N^*$ when the public key is (N,e). (Hint: this is similar to a problem on the previous homework.)

2. [**12 points**] Specify in pseudocode an $\mathcal{O}(k^3)$-time adversary A making one query to its **LR** oracle and achieving $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{AE}}(A) = 1$. Messages in the **LR** query must be in $\mathbb{Z}_N^*$ when the public key is (N,e).

3. [**optional points**] The following questions serve as hints to get the adversary and also to improve your understanding (you don't need to submit a writeup for these):

1. Let $X \in Z_N^*$ and Y be its modular inverse $(\bmod N)$. What will be the value of $XY \bmod N$?
2. What will be the ciphertext generated for the messages (in terms of U and e): 1, -1, 2 and -2?
