Problem 1 [20 points] Let $\mathcal{K}_{\text{rsa}}$ be a RSA generator with security parameter $k \geq 1024$. Consider the key-generation algorithm $\mathcal{K}$ and encryption algorithm $\mathcal{E}$ defined below:

\[ \text{Alg } \mathcal{K} \]
\[ (N, p, q, e, d) \leftarrow \mathcal{K}_{\text{rsa}} \]
\[ \text{Return } ((N, e), (N, d)) \]

\[ \text{Alg } \mathcal{E}((N, e), M) \] // $M \in \mathbb{Z}_N^*$
\[ U \leftarrow \mathbb{Z}_N^* \]
\[ V \leftarrow \text{MOD-EXP}(U, e, N) ; W \leftarrow (U \cdot M) \bmod N \]
\[ \text{Return } (V, W) \]

1. [8 points] Specify in pseudocode an $O(k^3)$-time decryption algorithm $D$ such that $\mathcal{AE} = (\mathcal{K}, \mathcal{E}, D)$ 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 $O(k^3)$-time adversary $A$ making one query to its LR oracle and achieving $\text{Adv}_{\mathcal{AE}}^{\text{ind-cpa}}(A) = 1$. 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 $X \in \mathbb{Z}_N^*$ 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 $-2$?