**Problem 1 [20 points]** Let $K_{rsa}$ be an RSA generator with security parameter $k$, and let $\ell$ be an additional parameter. We require that $k$ and $\ell$ are both multiples of 8, and that $\ell \leq k - 8$. Consider the key-generation algorithm $K$ and encryption algorithm $E$ defined below:

```
Alg K
(N, p, q, e, d) \xleftarrow{\$} K_{rsa}
Return ((N, e), (N, d, p, q))
```

```
Alg E((N, e), M) // M \in \{0, 1\}^{k-\ell-8}
R \xleftarrow{\$} \{0, 1\}^{\ell/2}
Z \leftarrow 0^{\ell/2}
X \leftarrow (M \parallel R \parallel Z)
m \leftarrow \text{int}(X)
c \leftarrow m^e \mod N
Return c
```

The notation $\text{int}(X)$ indicates that we are converting the binary string $X$ to an integer. In particular, we would like to ensure that $m \in Z_N^*$, when $N$ is a $k$-bit integer. Note that we could also compute $m$ by $m \leftarrow \text{int}(M) \cdot 2^\ell + \text{int}(R) \cdot 2^{\ell/2} + 0$.

1. **[8 points]** Specify in pseudocode an $O(k^3)$-time decryption algorithm $D$ such that $A_E = (K, E, D)$ is an asymmetric encryption scheme satisfying the correct decryption requirement. Note that your algorithm $D$ must return $\bot$ (None in Python) if the input ciphertext could not have been produced by the $E$ algorithm.

2. **[12 points]** Show that $A_E = (K, E, D)$ is not IND-CCA-secure by presenting an $O(k^3)$-time adversary $A$ making one $LR$ query, one $Dec$ query, and achieving $\text{Adv}_{\text{ind-cca}}^A(A) \approx 1$.

**Optional.** Here are a few questions that may help you think about these problems. You do not need to include answers in your code.
• What modification to the above scheme would make it trivially not IND-CPA-secure?
• What is the maximum bit length of \((M \parallel R \parallel Z)\)? Why does (or doesn’t) this guarantee that \(m \in \mathbb{Z}_N^*\)?