Question 1. Marks: 6.0

Consider a CCA-secure public-key encryption scheme $\Pi = (Gen, Enc, Dec)$ over the message space $\mathcal{M}$ and ciphertext space $\mathcal{C} = \{0,1\}^n$. Let $\tilde{\Pi} = (Gen, \tilde{Enc}, \tilde{Dec})$ be a scheme over he message space $\mathcal{M}$ and ciphertext space $\mathcal{C} = \{0,1\}^{n+1}$ defined as follows:

- $\tilde{Enc}(pk, m) = Enc(pk, m)||0$
- $\tilde{Dec}(sk, c) = Dec(sk, c')$ where $c' \in \{0,1\}^{n-1}$ is the first $n-1$ bits of c

Show that this scheme is not CCA-secure and that the adversary $\mathcal{A}$ succeeds with just one query to the decryption oracle.

Question 2. Marks: 4.0

Consider the following key-exchange protocol:

- Alice chooses uniform $k, r \in \{0,1\}^n$ and sends $s := k \oplus r$ to Bob.
- Bob chooses uniform $t \in \{0,1\}^n$ and sends $u := s \oplus t$ to Alice.
- Alice computes $w := u \oplus r$ and sends w to Bob.
- Alice outputs k and Bob outputs $w \oplus t$.

Show that Alice and Bob output the same key. Analyze the security of this protocol against a passive eavesdropper.