Problem 3.1 They are the same. Consider the expansion:

$$\left(\frac{t}{N}\right) = \left(\frac{t}{p}\right)\left(\frac{t}{q}\right)$$

. **Lemma 3.1** shows $\left(\frac{t}{p}\right) = \left(\frac{t^{-1}}{p}\right)$ (extending to prime q as well). This means that both terms in the expansion are the same value for t and t^{-1}, implying that $\left(\frac{t}{N}\right) = \left(\frac{t^{-1}}{N}\right)$.

Proof of **Lemma 3.1** (stated above): if $t \in QR \mod p$, there exists x such that $t = x^2 \mod p$. We can plug this in: $t^{-1} = (x^2)^{-1} = (x^{-1})^2 \mod p$, implying that $t^{-1} \in QR \mod p$ as well. This (and the reverse direction) shows that t is QR $\mod p$ iff t^{-1} is a QR $\mod p$ as well. The contrapositive statement be true too: t is not a QR iff t^{-1} is not a QR $\mod p$.

Problem 3.2 When we apply encryption to a message $m = \left(\frac{t}{N}\right)$ and simplify using polynomial long division, we obtain:

$$f(x) = (x+t)^2 t^{-1} \mod x^2 - R \mod N$$

$$f(x) = (x^2 + 2xt + t^2 \mod x^2 - R)(t^{-1} \mod x^2 - R) \mod N$$

$$f(x) = (R + 2xt + t^2)(t^{-1}) \mod N$$

Now, when we decrypt, we first substitute r into $f(x)$:

$$f(r) = (r^2 + 2rt + t^2)(t^{-1}) = t^{-1}(r+t)^2 \mod N$$

Now we take the $\left(\frac{f(r)}{N}\right)$:

$$f(r) = \left(\frac{t^{-1}(r+t)^2}{N}\right) = \left(\frac{t^{-1}}{N}\right) \times 1 = \left(\frac{t}{N}\right) = m$$

The decryption is m as desired.

Problem 3.3 We prove this semantically secure by showing that this encryption scheme is essentially lossy encryption. Here, a non-lossy key is $R \in QR$. A lossy key would be $R \in QNR$. To show the scheme is lossy, we show it fulfills three properties:

1. Correctness of the non-lossy key: this was shown in Question 3.2.
2. Indistinguishability of the lossy and non-lossy key: by the QR assumption, $R \in QR$ and $R \in QNR$ are indistinguishable.
3. Indistinguishability of ciphertexts with lossy key: our ciphertext is $f(x) = t^{-1}(2xt + t^2 + R) = 2x + t + \frac{R}{t}$. We show that knowledge of $f(r)$ reveals no information about the Jacobi symbol of t. Given the previous expression for $f(x)$, it suffices to show that $t + \frac{R}{t}$ reveals no information

about $m = \left(\frac{t}{N}\right)$ (because $2x$ reveals no information about t). This is the case because the possible values of Jacobi of t is equally distributed across the two values of 1 and -1. To show this, we consider the quadratic $z = t + \frac{R}{t} \rightarrow t^2 - zt + R = 0 \mod N$. We know that R is the product of the roots in the quadratic, and $\left(\frac{R}{p}\right) = \left(\frac{R}{q}\right) = -1$ because R is a QNR. This means that the roots' Jacobi symbols $\left(\frac{t}{p}\right) = \left(\frac{t}{q}\right) = \pm 1$, since these roots multiply to R. With equally distributed possible values of $\left(\frac{t}{N}\right)$, no information is leaked about m.

Problem 3.4 Suppose for contradiction there was a PPT A that could break the CPA security of the scheme. We show a PPT B that can break the semantic security of the regular $\mathsf{Enc}_{\mathsf{PK}}$ scheme presented in Question 3.2:

1. A challenger sends B public key $(R = r^2, N)$ and challenge ciphertext $c_1 = \mathsf{Enc}(m_b)$ to distinguish in the CPA-game with plaintexts m_{b_0}, m_{b_1}.
2. We allow for A to query us any set of prepatory ID's for which we must return the valid secret key $(b, \sqrt{\pm H(ID)})$. Because we have control of the random oracle function, we can construct plausible working answers: (1) $r_{id} \xleftarrow{\$} \mathbb{Z}_N$. Randomly return either $-r_{id}^2$ or r_{id}^2 as the value of $H(ID)$, along with the corresponding private key based on the sampled r_id.
3. Now we ask A to break specific the semantic security of a specific $\bar{ID}$. This $\bar{ID}$ has the property that $H(\bar{ID}) = R$, which we can ensure by finagling with the random oracle. We pass with this challenge the encrypted ciphertext $c_1, \gamma \xleftarrow{\$} \mathbb{Z}_N$. This is a valid ciphertext tuple in the IBE scheme because encryption with a QNR is indistinguishable from random. We also pass along m_{b_0}, m_{b_1} for the CPA setup. By definition of A, it is able break the semantic security, meaning that it can return the bit b corresponding to the correct original plaintext.
4. We return this b.

B uses A to break the semantic security of the original (3.1) encryption scheme, contradiction. No such B can exist, the scheme is IND-ID-CPA secure.