Question 5

By the Chinese Remainder Theorem we know that

$$\frac{\mathbb{Z}_q[x]}{\langle x^{256}+1\rangle} \cong \frac{\mathbb{Z}_q[x]}{\langle x-\zeta\rangle} \times \frac{\mathbb{Z}_q[x]}{\langle x-\zeta^3\rangle} \cdots \times \frac{\mathbb{Z}_q[x]}{\langle x-\zeta^{511}\rangle} \tag{1}$$

Because of the isomorphism between the large quotient ring R_q and the product space of the smaller rings, an element in R_q is invertible if and only if its NTT representation is invertible, which happens if and only if each entry in the NTT representation is invertible.

Notice that because each of the smaller ring is quotient on a degree-1 polynomial, $\mathbb{Z}_q[x]/\langle x-\zeta^{2k+1}\rangle$ is also isomorphic to $\mathbb{Z}_q$. There are $\phi(q) = q-1$ invertible elements in $\mathbb{Z}_q$ for a prime q, so the probability of drawing an invertible element from $\mathbb{Z}_q$ is $\frac{q-1}{q} = (1-\frac{1}{q})$, and the probability of independently drawing 256 invertible elements is $(1-\frac{1}{q})^{256}$