Q4

Using the Kyber described in the definition sheet, the LWE parameters are as follows: $n = m$, $q = 3329$, $\chi_s = \mathcal{B}(n = 6, p = 0.5)$, $\chi_e = \mathcal{B}(n = 4, p = 0.5)$, where $\mathcal{B}(n, p)$ denotes the centered binomial distributions.

Since $\mathbf{s} \leftarrow \chi_s^n$ is independently sampled from identical distributions, we can describe $\|\mathbf{s}\|^2$ as the sum of I.I.D. random variables:

$$\|\mathbf{s}\|^2 = \sum_{i=1}^{n} S_i^2$$

Therefore:

$$E[\|\mathbf{s}\|^2] = E\left[\sum_{i=1}^{n} S_i^2\right] = \sum_{i=1}^{n} E[S_i^2]$$

Because S_i follows the **centered** binomial distribution, $E[S_i] = 0$, so $E[S_i^2] = \mathrm{Var}[S_i]$. On the other hand, the variance of the centered binomial distribution is identical to that of the corresponding binomial distribution: $\mathrm{Var}[S_i] = 6 \cdot p(1-p) = \frac{3}{2}$. This is true because shifting a random variable by a constant does not change its variability.

Putting everything together:

$$E[\|\mathbf{s}\|^2] = \sum_{i=1}^{n} E[S_i^2] = \frac{3}{2}n$$

On the other hand, for calculating the variance of $\|\mathbf{s}\|^2$, we take advantage of the fact that the entries of $\mathbf{s}$ are independently drawn, and the variance of sum of independent random variables is the sum of variances:

$$\begin{aligned}
\mathrm{Var}[\|s\|^2] &= \mathrm{Var}[\sum_{i=1}^{n} S_i^2] \\
&= \sum_{i=1}^{n} \mathrm{Var}[S_i^2] \\
&= \sum_{i=1}^{n} (E[S_i^4] - E[S_i^2]^2) \\
&= \sum_{i=1}^{n} \left((\sum_{j=-3}^{3} (j^4 \cdot \binom{6}{j} \cdot 2^{-6}) - (\frac{3}{2})^2 \right) \\
&= \sum_{i=1}^{n} \left(6 - \frac{9}{4} \right) \\
&= \frac{15}{4}n
\end{aligned}$$

Replacing the secret distribution with the error distribution, we can compute the expectation and variance of the norm square of the error term in similar fashion. In conclusion:

$$\begin{aligned}
E[\|\mathbf{s}\|^2] &= \frac{3}{2}n \\
\mathrm{Var}[\|s\|^2] &= \frac{15}{4}n \\
E[\|\mathbf{e}\|^2] &= n \\
\mathrm{Var}[\|e\|^2] &= \frac{3}{2}n
\end{aligned}$$