Q1

(1)

The probability formula will be proved by induction. The base case is trivial: an empty set is always linearly independent, so the probability of drawing a linearly independent empty set is exactly 1.

For the induction, assume that $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1} \in \mathbb{F}_q^n$ are linearly independent, then consider the probability of drawing a t-th vector uniformly from $\mathbb{F}_q^n$ such that it is not in the linear span of the previous $t-1$ vectors: $\mathbf{a}_t \notin \mathrm{Span}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1})$.

There are a total of q^n possible values for $\mathbf{a}_t$ to draw from. On the other hand, there are a total of q^{t-1} possible combinations of coefficients (including all zeros) for $t-1$ vectors. Singe $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1}$ are linearly independent, each unique combination of coefficients corresponds to a unique element in the linear span. Thus, there are a total of $q^n - q^{t-1}$ possible values that are outside the linear span of $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1}$, and the probability of uniformly drawing a $\mathbf{a}_t$ that's outside the linear span is $1 - \frac{q^{t-1}}{q^n}$.

In other words:

$$P(\mathbf{a}_t \notin \mathrm{Span}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{t-1}) \mid \{\mathbf{a}_i\}_{i=1}^{t-1} \text{ is linearly independent}) = 1 - q^{t-1-n}$$

From here, we can recursively compute the probability of drawing m linearly independent vectors:

$$\begin{aligned}
&P(\{\mathbf{a}_i\}_{i=1}^{m} \text{ is linearly independent}) \\
&= \prod_{j=0}^{m-1} P(\mathbf{a}_{j+1} \notin \mathrm{Span}(\{\mathbf{a}_i\}_{i=1}^{j}) \mid \{\mathbf{a}_i\}_{i=1}^{j} \text{ is linearly independent}) \\
&= \prod_{j=0}^{m-1} (1 - q^{(j+1)-1-n}) \\
&= \prod_{j=0}^{m-1} (1 - q^{j-n})
\end{aligned}$$

(2)

Notice from the probability formula above:

$$\begin{aligned}
\prod_{i=0}^{n-1}(1 - q^{i-n}) &= (1 - q^{-n}) \cdot \prod_{i=1}^{n-1}(1 - q^{i-n}) \\
&= (1 - q^{-n}) \cdot \prod_{i=0}^{n-2}(1 - q^{i-(n-1)})
\end{aligned}$$

The product in the R.H.S. is the probability of drawing $n-1$ linearly independent vectors from $\mathbf{Z}_q^{n-1}$. Since $1 - q^{-n} < 1$ for all $q, n > 0$, the value of this probability strictly decreases as n increases. Therefore, we can bound the probability from below by setting n to the maximal value 1024:

$$\begin{aligned}
\prod_{i=0}^{n-1}(1 - q^{i-n}) &\geq \prod_{i=0}^{1023}(1 - q^{i-1024}) \\
&= (1 - q^{-1024})(1 - q^{-1023})\ldots(1 - q^{-1}) \quad \geq (1 - q^{-1})^{1024} \\
&= (1 - 3329^{-1})^{1024} \\
&\approx 0.735175 > \frac{2}{3}
\end{aligned}$$

(3)

For Kyber-512, the parameters are defined with $n = 256, q = 3329$. Plugging them into the formula:

```
from sympy import Rational

if __name__ == "__main__":
    q = 3329
    n = 256
    prod = 1
    for i in range(n):
        prod *= 1 - Rational(q) ** (i - n)
    print(f"Prob is {prod.evalf()}")
```

The result is 0.999699519257883