Question 3

Without rounding $\mathbf{w}$, the public key is $(A, \mathbf{t} = A\mathbf{s} + \mathbf{e})$ the signature contains three components:

$$\begin{aligned} \mathbf{z} &= \mathbf{y} + c\mathbf{s} \\ c &= H(\mathbf{w}, m) \\ \mathbf{w} &= A\mathbf{y} \end{aligned}$$

Multiply $\mathbf{z}$ by A:

$$\begin{aligned} A\mathbf{z} &= A\mathbf{y} + cA\mathbf{s} \\ &= \mathbf{w} + c \cdot (\mathbf{t} - \mathbf{e}) \end{aligned}$$

Assuming that c is invertible, re-arranging the equation above allows us to recover $\mathbf{e}$ from the publis key $A, \mathbf{t}$ and a single pair of message and signature $(m, (\mathbf{w}, c, \mathbf{z}))$:

$$\mathbf{e} = \mathbf{t} - c^{-1}(A\mathbf{z} - \mathbf{w})$$

From here we can attempt to recover the secret key $\mathbf{s}$ by solving $A\mathbf{s} = \mathbf{t} - \mathbf{e}$. While this is a non-trivial instance of inhomogeneous SIS, with proto-Dilithium A is a wide matrix, which makes SIS easier to solve. In the lecture notes, we simply assume that for the choice of parameters in proto-Dilihtium, such wide ISIS is "too easy".