Question 2

In SPX, each WOTS keypair WOTS signs the root of child XMSS tree(s). If WOTS is replaced by some k-time signature scheme, then each leaf node in each XMSS tree can sign the roots of k child XMSS tress. Fixing each XMSS tree to still have 2^t leaf notes, then each XMSS tree can have $k \cdot 2^t$ children. If the entire SPX hypertree has d layers, then it can sign a total of $(k \cdot 2^t)^d$ messages.

From the lecture notes we know that for a target security level λ, we want:

$$(k \cdot 2^t)^d = 2^{2\lambda}$$

Which solves to $d = \frac{2\lambda}{\log_2 k+t}$. With larger k (aka the signature scheme can sign more messages without losing security), **we need fewer layers in the hypertree to accomplish the same security level**. Since the signature, signing routine, and verification routine all iterate through all d layers of the hypertree, **signature size, signing time, and verification time all decrease linearly as d decreases**