Question 6

Comparing to McEliece

1. Classic McEliece checks that the norm (Hamming norm in this case) of the error term is exactly t as defined by the security parameters. Any codeword with strictly fewer than t bits of errors can still be correctly decoded, but the decryption routine will detect that the ciphertext has been tempered with and will appropriately reject the ciphertext as invalid.

2. Kyber will accept any ciphertexts whose error term's norm is no more than the threshold for decryption failure, which allows substantially more ciphertext malleability. This increased tolerance for ciphertext malleability is what makes the IND-CCA attack above work for Kyber, but not for McEliece.