



Question Number 7

- Find out why the IV for CTR can be a nonce
- While for CBC it must be randomized (unpredictable)
- Give short justification for both

Solution.