This week’s readings


1. What is the main pitfall of using a stream cipher that WEP falls victim to?

2. What is the main design flaw of WEP?
3. What would a easy and effective incremental implementation change be to patch WEP’s keystream reuse?

4. What’s wrong with how WEP uses a CRC?

5. Express the vulnerability to authentication spoofing using the rules and message meaning from the logic of authentication paper, and note the difference between the goal and the result. (If you can’t do this, explain in words using the vocabulary of the BAN logic).