# Cryptology Quiz, Lessons 1 -3

1. Wired Equivalent Privacy (WEP) had many problems. Describe two of them.
2. What is the difference between encoding and encryption?
3. What is one advantage they symmetric encryption has over asymmetric encryption? What is one advantage that asymmetric encryption has over symmetric encryption?
4. Consider a Caesar cipher where the possible symbols are A through Z, and 0 through 9. How many possible keys are there?
5. What is the Greatest Common Divisor? What is the GCD of 28 and 35? What does it mean when the GCD is one?
6. If we are working in Z15, {0, 1, 2, …, 14}, which of the following numbers **does not** have a multiplicative inverse? 4, 6, 11
7. What is the most important thing to remember when using either a nonce, initialization vector, or a salt?
8. What is the most common symmetric cipher in use today?
9. The simplest mode for applying a symmetric cipher is just to break the input into blocks that match the block size the cipher needs, and then apply the cipher on one block after the other without any other changes. (This is Electronic Code Book (ECB) mode.) What is a problem that this mode presents?
10. Fill in the blank. A one-bit change in the plaintext should \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the ciphertext.