# Cryptology Quiz, Lessons 1 -3

1. Wired Equivalent Privacy (WEP) had many problems. Describe two of them.

Key Length was short, limited by hardware. Keys were repeated, so were broken  
WEP used RC4 with a small IV (24 bits) which was repeated over time--broken  
WEP did not prevent attackers from inserting crafted packets.

1. What is the difference between encoding and encryption?

Encoding just changes the form of the output, it does not require a key to decode. Encryption uses a secret key, which must be known to decrypt the message.

1. What is one advantage they symmetric encryption has over asymmetric encryption? What is one advantage that asymmetric encryption has over symmetric encryption?

Symmetric is much faster than asymmetric.  
Asymmetric allows for secure key exchange.

1. Consider a Caesar cipher where the possible symbols are A through Z, and 0 through 9. How many possible keys are there?

There are 26 letters plus 10 digits, so there are 36 possible shifts (including 0)

1. What is the Greatest Common Divisor? What is the GCD of 28 and 35? What does it mean when the GCD is one?

GCD is the largest number that can divide both numbers evenly.  
GCD(28,35) is 7. 7\*4 = 28, 7\*5 = 35  
When the GCD is 1 the numbers are relatively prime.

1. If we are working in Z15, {0, 1, 2, …, 14}, which of the following numbers **does not** have a multiplicative inverse? 4, 6, 11

For Z15, the number of elements is 15. 15 has factors 3 and 5. Of the numbers given (4, 6, 11), 6 shares the factor 3 with 15, so it has no multiplicative inverse.

1. What is the most important thing to remember when using either a nonce, initialization vector, or a salt?

None of these should ever be reused. Nonce means Number used ONCE.

1. What is the most common symmetric cipher in use today?

AES

1. 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?

Identical blocks of plaintext give identical ciphertext. An attacker may not be able to break the code, but they can glean some information from it. Remember the Linux penguin picture we encoded with ECB.

1. Fill in the blank. A one-bit change in the plaintext should \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the ciphertext.

change many bits in the ciphertext