**Level 1: Simple substitution Cypher**

Use this resource to answer the following questions.

<http://practicalcryptography.com/ciphers/simple-substitution-cipher/>

1. Summarize and explain the concept of a substitution cypher
   1. What does it do?

It encrypts the message by which units of plaintext are replaced with ciphertext

* 1. How does it work?

Units of plaintext are replaced with ciphertext. The "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above

* 1. What is a “key”?

A key is a way of decryption for substitution cypher which is 26 letters

1. Provide an example of encoding a message using a substitution cypher key.

Plaintext: hello world

key = cbyvqduzofxgtplnrimjhkwesa

Ciphertext: einnd tdkng

1. Provide an example of decoding a message using a substitution cypher key.

Ciphertext: einnd tdkng

key = cbyvqduzofxgtplnrimjhkwesa

Plaintext: hello world

1. Summarize and explain the concepts related how “cryptanalysis” can be used to “break” a code.
   1. How does the “frequency analysis of letters” work?
   2. How does the “frequency analysis of words” work?

**Level 2: Morse Code**

Use this resource to answer the following questions.

<http://www.newworldencyclopedia.org/entry/Morse_Code>

1. Summarize and explain the concept of Morse code
   1. What does it do?
   2. How does it work?
   3. What does it use instead of a “key”?
2. Compare the Morse code table to the “frequency of letters” analysis in Level 1 above.
   1. What is the shortest code and how does it correspond to the frequency of letters?
   2. What is the longest code and how does it correspond to the frequency of letters?
   3. What is the benefit of having a variable length code for letters?
3. Provide an example of encoding a message using Morse code.
4. Provide an example of decoding a message using Morse code.

**Level 3: Encryption**

Use this resource to answer the following questions.

<https://computer.howstuffworks.com/encryption.htm>

1. Summarize and explain the concept of Symmetric-key Encryption. (See Slide 3)
   1. How is it similar to a “substitution cypher”?
   2. How is it different from a “substitution cypher”?
2. Encryption key strength is related to the number of bits and combinations. (See Slide 3)
   1. What is DES and how strong is it?
   2. What is AES and how strong is it?
3. Summarize and explain the concept of Public-key Encryption. (See Slide 4)
   1. How is it different from Symmetric-key Encryption
   2. What is an Asymmetric-Key?
4. Prime Numbers and Hashing Algorithms are used to encrypt messages. (See Slide 6)
   1. What is a Hash Value?
   2. How is a Hash Value used to encrypt a message?
   3. How is a Hash Value used to decrypt a message?
   4. How strong are current Public Keys (Hash Values) in terms of bits and combinations?
5. We use encryption every day when we use the internet and the following services. (See Slides 4 & 5)
   1. What is PGP?
   2. What is SSL / HTTPS?
   3. What is a Digital Certificate?
   4. What is a Certificate Authority?