**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

a. What does it do?

It simply encrypts the data so that someone that doesn’t know the cypher would not be able to read the document.

b. How does it work?

It changes the order of the alphabet, so that the sender writes the rearranged alphabet, and the receiver uses the rearranged alphabet to convert back into regular words.

c. What is a “key”?

A key is the cypher that the receiver and sender would use to code and decode the document so that they can hide or read it.

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

A b c d e f

B c d e f a

bad----cbe

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

B c d e f a

A b c d e f

cbe----bad

4. Summarize and explain the concepts related how “cryptanalysis” can be used to “break” a code.

a. How does the “frequency analysis of letters” work?

It bases the frequency of the letters to determine a possible candidate for the cracked cypher. For example, e is the most popular letter. All you have to do is take the most popular encrypted letter and replace it with e.

b. How does the “frequency analysis of words” work?

This takes the most frequent one, two, three or four letter words to guess what the cracked sentence or phrase might be based on the lettering.

**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

a. What does it do?

It disguises letters as dots and dashes so the receiver needs a key to understand.

b. How does it work?

It uses dots and dashes and converts each letter into a unique pattern.

c. What does it use instead of a “key”?

Instead of regular alphabets, it uses dots and dashes in replace for different letters.

2. Compare the Morse code table to the “frequency of letters” analysis in Level 1 above.

a. What is the shortest code and how does it correspond to the frequency of letters?

The shortest code is either t or e, and they are both the most frequently used letters, with e being the most used, and is the shorter code (dot).

b. What is the longest code and how does it correspond to the frequency of letters?

The longest code are the letters with 4 dots or dashes, and they are the least used letters in the alphabet. For example, z would be --.. Y would be -.-- and so on

c. What is the benefit of having a variable length code for letters?

The benefit of having code that's a variable length, is so that when typing messages, you do not have to type a lot to send long phrases. The variable length shortens the length of the amount of dots and dashes that you have to perform.

3. Provide an example of encoding a message using Morse code.

Encoding the word Amrit Shoker would be .- -- .-. .. - ... .... --- -.- . .-.

4. Provide an example of decoding a message using Morse code.

.- -.-. . .-. Would be decoded to be acer.

**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)

a. How is it similar to a “substitution cypher”?

b. How is it different from a “substitution cypher”?

2. Encryption key strength is related to the number of bits and combinations. (See Slide 3)

a. What is DES and how strong is it?

b. What is AES and how strong is it?

3. Summarize and explain the concept of Public-key Encryption. (See Slide 4)

a. How is it different from Symmetric-key Encryption

b. What is an Asymmetric-Key?

4. Prime Numbers and Hashing Algorithms are used to encrypt messages. (See Slide 6)

a. What is a Hash Value?

b. How is a Hash Value used to encrypt a message?

c. How is a Hash Value used to decrypt a message?

d. 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)

a. What is PGP?

b. What is SSL / HTTPS?

c. What is a Digital Certificate?

d. What is a Certificate Authority?