**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?

**The simple substitution cipher is a cipher that has been in use for many hundreds of years (an excellent history is given in Simon Singhs 'the Code Book').**

* 1. How does it work?

**It basically consists of substituting every plaintext character for a different ciphertext character.**

* 1. What is a “key”?

**Keys for the simple substitution cipher usually consist of 26 letters (compared to the caeser cipher's single number).**

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

**This is Simon Singh’s key:**

**plain alphabet: abcdefghijklmnopqrstuvwxyz**

**cipher alphabet: phqgiumeaylnofdxjkrcvstzwb**

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

**This is an example of decoding:**

**plaintext: defend the east wall of the castle**

**cipher text: giuifg cei iprc tpnn du cei qprcni**

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?

**Letter frequencies ordered from most frequent to least frequent This means that the letter 'e' is the most common, and appears almost 13% of the time, whereas 'z' appears far less than 1 percent of time.**

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

**Application of the simple substitution cipher does not change these letter frequencies, it merely jumbles them up a bit (in the example above, 'e' is enciphered as 'I', which means 'I' will be the most common character in the cipher text).**

**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?

**Morse code is a method for transmitting**[**telegraphic**](http://www.newworldencyclopedia.org/entry/Telegraph)**information, using standardized sequences of short and long elements to represent the letters, numerals, punctuation and special characters of a message.**

* 1. How does it work?

**The short and long elements can be formed by sounds, marks, or pulses, in on off keying and are commonly known as "dots" and "dashes" or "dits" and "dahs.**

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

**International Morse code today is most popular among amateur radio operators, where it is used as the pattern to key a transmitter on and off in the radio communications mode commonly referred to as "continuous wave" or "CW."**

1. 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?
2. Provide an example of encoding a message using Morse code.
3. 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?