**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?
   2. How does it work?
   3. What is a “key”?
2. It consists of changing every plaintext character for a different ciphertext character. Providing communication security when necessary.
3. It works when each character is replaced with another character.
4. Keys for the simple substitution cipher usually consist of 26 letters
5. Provide an example of encoding a message using a substitution cypher key.

plain alphabet : abcdefghijklmnopqrstuvwxyz

cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

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

plaintext : defend the east wall of the castle

ciphertext: 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?
   2. How does the “frequency analysis of words” work?

They work by the first step is to calculate the frequency distribution of the letters in the ciphertext. This consists of counting how many times each letter appears.

**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. Morse code is a method of sending short and long elements used to represent letters and numbers.
3. Morse code works through electrical pulses through electrical poles, audio, radio, through lights and many more.
4. Instead of using keys, morse code uses dots and dashes.
5. 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?
6. The shortest code is one dot, which is letter E. It corresponds to the frequency of letters as E is the most used letter in Morse Code.
7. The longest code are one dot and three dashes, which are the letters J and Q. It corresponds to the frequency of letters as they are the least used letters.
8. The benefit is that you know which letter is which without having to decode it.
9. Provide an example of encoding a message using Morse code.

.... . .-.. .-.. --- / -- -.-- / -. .- -- . / .. ... / -... .- .-.. -.- .- .-. .- -.

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

hello my name is balkaran

**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. They have a secret code for it in this version.
3. 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?
4. The DES uses a 56 bit key.
5. AES uses 128-256 bit keys.
6. 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?
7. Public-key encryption uses two different keys. It uses the private and public key.
8. Asymmetric-Key is just another word for public-key encryption. It uses a private key and a public key. The private key is known to your computer only, while the public key is given by your computer to any computer that wants to communicate securely with it.
9. 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?
10. Hash value is computed from a base input number.
11. A hash Value is used to encrypt a message by multiplying the input number by 143.
12. If you want to decode you should divide the input number by 143.
13. Public Keys generally use complex algorithms and very large hash values for encrypting, including 40-bit or even 128-bit numbers. A 128-bit has a possible 2128 combinations.
14. 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?

1. PGP (Pretty Good Privacy) is a service which allows you to encrypt almost anything.
2. SSL (Secure Sockets Layer) is a popular implementation of public-key encryption.
3. Is an electric password which enables you to safely exchange data over the internet.
4. Issues Digital certificates.