**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”?

It basically consists of submitting every character for a different cipher text character, the alphabet is not shifted it is complete jumbled. Simple ones offer very little communication security and can be easily be broken by hand, keys for the cipher consist of 26 letters and is basically the message.

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

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?

They see which letter is used most frequently like for example “e” is used 13% of the time, whereas “z” is used less than 1% of the time.

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

This sees which words are more frequently used, like most frequent words are “of”, “to”, “it”, “as”, “be” and etc.

**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”?

A method for transmitting telegraphic information, using sequences of short and long elements to represent the letters, numbers, punctuation and special characters in a message. It uses dots and dashes for characters. It was transmitted using electrical pulses along a telegraph wire, an audio tone, or as a machine or visual signal for example flashing lights. It was usually transmitted using on and off, making it an early form of digital code

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?

The shortest code is e and it corresponds to the frequency of letters because the most commonly used letters have shorter codes.

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

The longest is code is of letters that are not commonly used like Y or W, it corresponds to the frequency of letters because the uncommonly used letters have the longest code.

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

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

Provide an example of decoding a message using Morse code.

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

A cookie in the jar

**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”?

Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know in order to decode the information. The code provides the key to decoding the message. in symmetric-key encryption, each computer has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key requires that you know which computers will be talking to each other so you can install the key on each one.

1. Encryption key strength is related to the number of bits and combinations. (See Slide 3)
   1. What is DES and how strong is it?

The DES uses a 56-bit key. The first major symmetric algorithm developed for computers in the United States was the Data Encryption Standard (DES), approved for use in the 1970s.

* 1. What is AES and how strong is it?

DES has since been replaced by the Advanced Encryption Standard (AES), which uses 128-, 192- or 256-bit keys

1. Summarize and explain the concept of Public-key Encryption. (See Slide 4)
   1. How is it different from Symmetric-key Encryption?

In symmetric key encryption two users attempting to communicate with each other need a secure way to do so; otherwise, an attacker can easily pluck the necessary data from the stream. The solution to this is Public-Key Encryption.

* 1. What is an Asymmetric-Key?

public-key encryption uses two different keys at once -- a combination of a private key and a public key. The private key is known only to your computer, while the public key is given by your computer to any computer that wants to communicate securely with it. This is called a asymmetric-key encryption.

1. Prime Numbers and Hashing Algorithms are used to encrypt messages. (See Slide 6)
   1. What is a Hash Value?

A value that is composed using a hashing algorithm, it is basically the synopsis of the original value. It is almost impossible to figure out the original value without the data that is used to create the value.

* 1. How is a Hash Value used to encrypt a message?

Hash value is multiple by input number and that number becomes the encoded number.

* 1. How is a Hash Value used to decrypt a message?

You need to divide the encoded value by the hash value.

* 1. How strong are current Public Keys (Hash Values) in terms of bits and combinations?

Public keys can be 40bits to 128 bit numbers allowing for extremely complex and large encryption.

1. We use encryption every day when we use the internet and the following services. (See Slides 4 & 5)
   1. What is PGP?

PGP or pretty good protection, provides cryptographic privacy and authentication for data communication like emails, texts and etc.

* 1. What is SSL / HTTPS?

SSl is a security protocol used by internet servers to transmit important data.

* 1. What is a Digital Certificate? What is a Certificate Authority?

A digital certificate is basically a unique piece of code or a large number that says that the Web server is trusted by an independent source known as a certificate authority