**Level 1: Simple substitution Cypher**

Use this resource to answer the following questions.

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

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

Substitution cypher consists of substituting every plain text character for a different cypher text character.

* 1. How does it work?

It changes the input into a random key and then translates it into cypher text.

* 1. What is a “key”?

A key is used for the substitution cypher, which usually consist of 26 letter.

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

Plain text->Hi my name is Pritpal Jangla

Key-> ukwivzqmxrgbenopsjclathdyf

Cipher text-> mx ey nuev xc pjxlpub runqbu

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

Cipher text-> zm cs xncg mj rumtrne

Key->ndhiglozmpbecxyrqujtvfkwsa

Plain Text-> Hi my name is Pritpal

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?

It checks all the letters and ranks them from least to most common. The coding letters are usually from a to z.

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

The frequency analysis of words find the most frequent words used in real life.

**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 Morse code is used to send coded information. It is sent coded so if someone intercepts the message, they will not be able to decode it. This is because to decode the   
Morse code, you will need a key which the sender and receiver of the message will have. You use the key to decode the message. It uses dots and dashes, or “dits” and “dahs”.

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 one dot which is E. This corresponds to the frequency of letters as E is one of the most used letters.

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

The longest code is one dot and three dashes which is J and Q. It corresponds to the frequency of letters and they are the least used letters.

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

The benefit is that you know what the letters are and you don’t have to decode it.

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

My name is Pritpal

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

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

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

My name is Pritpal

**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”?

It has a secret code for it.

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

Instead of letters, it uses numbers.. There are 128-, 192, and 256-bits, for example, in advanced encryption standard. A 128-bit key can have 30000000000000000000000000000000000000000 key combinations. This is a lot.

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?

DES was the first major symmetric algorithm introduced to computers in the US. It used a 56-bit key, which offered more than 70 quadrillion. It was strong before, but because of rapid computer growth, security experts no longer consider it secure.

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

AES stands for Advanced Encryption Standard which had replaced DES. It uses 128-,192- and 256-bit keys. Many believe AES be a sufficient encryption standard for a long time coming as a 128-bit key can have 30000000000000000000000000000000000000000 key combinations.

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

Public-key Encryption allows you to send a public and private key which both are mathematically related.

* 1. What is an Asymmetric-Key?

An Asymmetric-Key uses a public a private key to encrypt and decrypt coded messages.

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

Hashing is the practice of using an algorithm to map data of any size to a fixed length. This is called a hash value . Whereas encryption is a two-way function, hashing is a one-way function.

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

Hashing is an ideal way to store passwords, as hashes are inherently one-way in their nature. By storing passwords in hash format, it's very difficult for someone with access to the raw data to reverse it.

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

You divide the hash value by 143 to get the input #.

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

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 2^138 combinations.

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

PGP is a short for Pretty Good Privacy, which allows you to encrypt almost anything.

* 1. What is SSL / HTTPS?

SSL is short for Secure Sockets Layer. It is a popular implementation of public-key encryption. It was originally developed by Netscape and is an internet security protocol used by internet browsers and web servers to transmit sensitive information.

* 1. What is a Digital Certificate?

A digital certificate is an electronic “password” that allows a person, organization to exchange data securely over the internet using the public key infrastructure.

* 1. What is a Certificate Authority?

Certificate authority is an entity that issues digital certificates.