**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?

Substitution Cyber consists pf substituting every plaintext character for a different ciphertext character. It differs from the Caesar cipher in the alphabet is not simply the alphabet shifted, it is completely jumbled.

* 1. How does it work?

It first turns the input into a random key and then translates it into ciphertext.

* 1. What is a “key”?

A key is used for the simple substitution cipher, which usually consist of 26 letters.

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

Plain Text-> i am daksha

Key-> oihfcvpgzdwyskaqxbutnremlj

Ciphertext-> z os fowugo

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

Ciphertext-> z os fowugo

Key-> oihfcvpgzdwyskaqxbutnremlj

Plain Text-> i am daksha

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 analysis the letters and which is the most common and which is the least common. The coding letters are usually frequent and are in the order 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?

Morse code is a method for transmitting telegraphic information.

* 1. How does it work?

It works by using standardized sequences of short and log elements to represent the letters, numerals, punctuation and special characters if a message. The short and log elements can be formed by sounds, marls, 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”?

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 the letter E. It corresponds to the frequency of letters as the letter E is the most used letter.

* 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 the letters J and Q. It corresponds to the frequency of letters as they are the least used letters.

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

The benefit of having a variable length code for letters is that you know what the letters are and don’t have to decode it.

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

Get to the Choppa

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

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

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

Get to the Choppa

**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”?

Rather than letters, it uses numbers. There are 128-, 192, and 256-bits, for example, in Advanced Encryption Standard(AES). A 128-bit key can have 300000000000000000000000000000000000 key combinations, which 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 developed for computers in the United States. It was approved for use in 1970s. It used a 56-bit key, which offered more than 70 quadrillion. It was strong back then, but now because of the increasingly fast computers, security experts no longer consider it secure.

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

AES is Advanced Encryption Standard which had replaced DES. IT uses 128-,192-, and 256-bit keys. Most believe that AES will be a sufficient encryption standard for a long time coming, as a 128-bit key can have, as said before, 300000000000000000000000000000000000 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 uses two different keys at once. It uses a private key and a public key.

* 1. What is an Asymmetric-Key?

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.

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

A Hash Value is a value that is computed from a base input number using a hashing algorithm.

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

A hash Value is used to encrypt a message by multiplying the input # by 143.

* 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 2128 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 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.