**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?

It substitutes letters and characters with another to hide and secure messages. It is used to convey very private and important messages.

* 1. How does it work?

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

* 1. What is a “key”?

A key is a list of letter with the substitution before and after encoding. This can be helpful when decoding a message. Each letter is assigned a different letter and this can change a message completely. A simple key consists of 26 letters and those letter have ciper substations.

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

Ow fpoi ar Epkypx

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

My name is Harjap

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?

The cryptanalysis uses the frequency of letter found in English and checks the frequency of letters in the encoded message. As in English e is the most used letter and I n the message the most used letter is t than the cryptanalysis with know that e is encoded as t. this will happen for the other letters too.

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

It uses the frequencies of words and the number of letters in them and the words in the encoded message and compares them. If there is a 1 letter word in the encoding message then that letter will either be an a or I. Cryptanalysis is used for more number of letters with the frequency of words.

**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, using standardized sequences of short and long elements to represent the letters, numerals, punctuation and special characters of a message. 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. How does it work?

Morse code can be transmitted in a number of ways: originally as electrical pulses along a telegraph wire, but also as an audio tone, a radio signal with short and long tones, or as a mechanical or visual signal (for example, a flashing light) using devices like an Aldis lamp or a heliograph. The letters that are less commonly used have a small combination of dots and dashes.

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

Morse code uses binary and computer energy instead of a key.

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 0 and it is used to represent e. e is also the most frequent letter in English.

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

The longest code is 1101 and it is used for q. q is also the least frequent letter in English.

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

This makes it easier to send long messages as the most common letters are easy to encode.

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

11 1011 10 01 11 0 00 000 0000 01 010 0111 01 0110

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

My name is Harjap

**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”?

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. 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.

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

* 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

One of the weaknesses some point out about symmetric key encryption is that 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?

Also known as asymmetric-key encryption, 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. To decode an encrypted message, a computer must use the public key, provided by the originating computer, and its own private key. Although a message sent from one computer to another won't be secure since the public key used for encryption is published and available to anyone, anyone who picks it up can't read it without the private key.

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

This is a value that is computed from a base input number using a hashing algorithm. Essentially, the hash value is a summary of the original value. The important thing about a hash value is that it is nearly impossible to derive the original input number without knowing the data used to create the hash value.

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

The hash value is multiplied by the input number and the new number becomes the encoded number.

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

To decrypt the message with a hash value, you need to divide the encoded message with the hash value.

* 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.

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

PGP allows you to encrypt almost anything

* 1. What is SSL / HTTPS?

SSL is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information. SSL has become part of an overall security protocol known as Transport Layer Security (TLS).

* 1. What is a Digital Certificate?
  2. 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