**pLevel 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

a. What does it do?

It simply encrypts the data so that someone that doesn’t know the cypher would not be able to read the document.

b. How does it work?

It changes the order of the alphabet, so that the sender writes the rearranged alphabet, and the receiver uses the rearranged alphabet to convert back into regular words.

c. What is a “key”?

A key is the cypher that the receiver and sender would use to code and decode the document so that they can hide or read it.

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

A b c d e f

B c d e f a

bad----cbe

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

B c d e f a

A b c d e f

cbe----bad

4. Summarize and explain the concepts related how “cryptanalysis” can be used to “break” a code.

a. How does the “frequency analysis of letters” work?

It bases the frequency of the letters to determine a possible candidate for the cracked cypher. For example, e is the most popular letter. All you have to do is take the most popular encrypted letter and replace it with e.

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

This takes the most frequent one, two, three or four letter words to guess what the cracked sentence or phrase might be based on the lettering.

**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

a. What does it do?

It disguises letters as dots and dashes so the receiver needs a key to understand.

b. How does it work?

It uses dots and dashes and converts each letter into a unique pattern.

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

Instead of regular alphabets, it uses dots and dashes in replace for different letters.

2. Compare the Morse code table to the “frequency of letters” analysis in Level 1 above.

a. What is the shortest code and how does it correspond to the frequency of letters?

The shortest code is either t or e, and they are both the most frequently used letters, with e being the most used, and is the shorter code (dot).

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

The longest code are the letters with 4 dots or dashes, and they are the least used letters in the alphabet. For example, z would be --.. Y would be -.-- and so on

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

The benefit of having code that's a variable length, is so that when typing messages, you do not have to type a lot to send long phrases. The variable length shortens the length of the amount of dots and dashes that you have to perform.

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

Encoding the word Amrit Shoker would be .- -- .-. .. - ... .... --- -.- . .-.

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

.- -.-. . .-. Would be decoded to be acer.

**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)

a. How is it similar to a “substitution cypher”?

It is similar to substitution cypher because there are keys that you have to follow, and both the encoder and the decoder both need to have the key installed or know the key in order to handle the message.

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

There's no shifting, and you could make a symmetric key cypher without following the pattern of the alphabet. This makes the code harder to crack, as they wouldn’t know the pattern of the rest of the letters if one letter is found out. With substitution cypher, there are also 26 combinations, but the symmetric key has more.

2. Encryption key strength is related to the number of bits and combinations. (See Slide 3)

a. What is DES and how strong is it?

The Data Encryption Standard is a symmetric-key algorithm for the encryption of electronic data. It has a key length of 56 bits, but it was strong enough to have more than 72 quadrillion possible encryption keys.

b. What is AES and how strong is it?

It's the advanced encryption standard, and it is a specification for the encryption of electronic data established by the national institute of standards and technology in 2001. It is either 128, 192, or 256 bits in size. Most of the time, it is 256-bit encryption with 128-bit blocks.

3. Summarize and explain the concept of Public-key Encryption. (See Slide 4)

a. How is it different from Symmetric-key Encryption

The Asymmetric-key encryption, public-key encryption uses two different types of keys at once. It uses a combination of a private and a public key.

b. What is an Asymmetric-Key?

The private key is only available to your computer while the public key is given by your computer to many other kinds of computer and is communicated securely within it. For a text message to be decoded, the computer must use a public key in order to decode it. This key must be received from the original computer and it also needs its own private key. Furthermore, a message sent from one computer to another won’t be secure as the public key is used for encryption is published publically and is available to almost everyone. However, the individuals who receive the public key cannot read it unless they have the private key which will open it up for them.

4. Prime Numbers and Hashing Algorithms are used to encrypt messages. (See Slide 6)

a. What is a Hash Value?

The hash value is computed from a base input using a special algorithm. It is the summary of the original value, and it is nearly impossible to derive the original input without knowing the data used to generate the hash.

b. How is a Hash Value used to encrypt a message?

The hash value is used to encrypt by multiplying it by the innput, and the result is the generated hash value.

c. How is a Hash Value used to decrypt a message?

You have to divide the encoded message by the hash value to decode the message.

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

Public keys use complex algorithms and have large hash values for encrypting. They include 40 bit or high bit numbers such as 128 bit. 128-bit encryption has 2^128 combinations.

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

a. What is PGP?

PGP is a system which allows you to encrypt anything. PGP stands for “Pretty Good Privacy”.

b. What is SSL / HTTPS?

SSL is a type of internet security protocol used by internet browsers and many web servers to transmit sensitive information. SSL has become part of an overall security protocol known as Transport Layer Security. SSL stands for Secure Sockets Layer.

c. What is a Digital Certificate?

A digital certificate is a unique piece of code or a large number that says that the web server is trusted by the independent source which is known as a certificate authority. This certificate acts as the middleman that both computers receiving the message can trust.

d. What is a Certificate Authority?

This confirms that each computer is in fact who says it is and is the system which provides the public keys of each computer to each other so that there’s no interruption in who’s recieving the message.