**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

a. What does it do?

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

b. How does it work?

The encrypting procedure is varied depending on the key but what it basically does is substitute every letter in the message with a cipher for the whole message.

c. What is a “key”?

The key for a substitution cipher is a table that maps every possible character in the plaintext message to a different value.

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

plain alphabet : abcdefghijklmnopqrstuvwxyz

cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

So:

plaintext : defend the east wall of the castle

ciphertext: giuifg cei iprc tpnn du cei qprcni

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

cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

plain alphabet : abcdefghijklmnopqrstuvwxyz

So:

ciphertext: giuifg cei iprc tpnn du cei qprcni

plaintext : defend the east wall of the cast

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?

“frequency analysis of letters” works better in longer pieces of text than shorter ones because in the English alphabet, the letter frequencies are very consistent and easy to identify. In order to decrypt the ciphertext, the frequencies of of the letters can simply be replaced by the corresponding letters already known to have higher frequencies. This is mainly for longer pieces of text (over 100 words). For shorter text (less than 100 words), this method becomes less efficient because there can be more different changes in the frequencies since there are less words and because the English alphabet frequency also become less efficient.

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

It works because in a similar way to the method above but it is more guessing because the method is to replace the ciphertext with some of the words already known to be used often. There is a list of some of the most popular 1 words, 2 words, 3 words, 4 words known and they can be used to decipher a ciphertext.

**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?

b. How does it work?

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

Morse code is a method of transmitting telegraphic information by using standardized sequences of elements to represent letters, numbers, punctuation as well as special characters. The short as well as long elements can be formed using by marks, sounds or pulses. It can be transmitted in a number of ways, it originated from electrical pulses from telegraph wires and a radio signals with short and long tones. Another original method was through mechanical or visual signals like a flashing light. Morse codes are transmitted using just two states which are on and off. It is an early form of digital code and it is not technically binary. The pause lengths are required to decode the information. Instead of a key, it is commonly known as “dots, dashes, or dits and dahs”.

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?

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

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

The shortest code is “e” because it only has one dot. This is because in the frequency of letters, the letter “e” has the highest frequency. The letter “t” only has one dash so this means that it is also used a lot. This is proven correct because in the frequency of letters, the letter “t” is the second most frequent. There are a lot of letters which have a combination of 4 elements and they are “b”, “c”, “f”, “h”, “j”, “l”, “p”, “q”, “v”, “x”, “y”, and finally “z”. These letter have the longest code because in frequency of letters, these letters are not used as often as others. There are multiple benefits of having variable length code because you will not need to type a long sentence to deliver your message. The variable lengths of specific letter will help in shortening the light of the total message. Some other benefits could be that it is cheap, it is wireless and it has no interuptions.

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

My name is Jasjot = (-- -.-- / -. .- -- . / .. ... / .--- .- ... .--- --- - /)

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

(.-- .... .- - / .. ... / -.-- --- ..- .-. / -. .- -- .) = What is your name

**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”?

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

In symmetric-key encryption, computers have a secret code/key that they use to encrypt information before they send over the network to another computer. Symmetric-key encryption requires us to know which computers will be talking to each other so the key can be installed onto each one. It is basically like a secret code that computers must know in-order to share information with each other. The code also provides the key to decode the message.

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?

b. What is AES and how strong is it?

DES is Data Encryption Standard and this is the first major symmetric algorithm developed for computers in the United States. DES uses a 56-bit key and it offers more than 70 quadrillion possible combinations. Now, security experts no longer consider using DES because an attack that tries every combination could easily decipher this data. An AES is Advanced Encryption Standard and it uses either 128, 192 or 256-bit keys. Most people including some security experts believe that AES will be a sufficient encryption standard for a long time in the future. For examples, a 128-bit key can have more than 300, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000, 000 key combinations. This is why DES has been replaced by AES.

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

a. How is it different from Symmetric-key Encryption

b. What is an Asymmetric-Key?

Public-key Encryption is different from symmetric key encryption because two users attempting to communicate with each other need a secure way to do so. Otherwise, an attacker can easily steal the necessary data from their conservation. In November 1976, a paper published called "New Directions in Cryptography," addressed the problem and provided a solution which is called public-key encryption. Also known as Asymmetric-key encryption, public-key encryption uses two different keys at once which is a combination of a private key and a public key. The private key is only known 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 which is provided by the original computer, and its own private key. The key pair is based on prime numbers which are long in length. This makes the system extremely secure because there are an infinite number of prime numbers available resulting in nearly infinite possibilities for keys.

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

a. What is a Hash Value?

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

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

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

The key in public-key encryption is based on a hash value and this value is generated from a base input number using a hashing algorithm. Basically, the hash value is a summary of the original value and the important thing about it is that it is nearly impossible to figure out the original input number without knowing the data used to create the hash value. To encrypt a message, the input in changed by a hashing algorithm and the result is a hash value. To decrypt a message, it would be very difficult because we would need to change the hash value by the hashing algorithm to find the initial message. Public keys generally use complex algorithms and very large hash values for encrypting, including 40-bit or even 128-bit numbers. A 128-bit number has a possible 2128 different combinations and this is like trying to find one chosen grain of sand in the Sahara Desert.

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

a. What is PGP?

b. What is SSL / HTTPS?

c. What is a Digital Certificate?

d. What is a Certificate Authority?

A PGP is called “Pretty Good Privacy” and it is a very popular public-key encryption program which allows you to encrypt almost anything. SSL is called a “Secure Sockets Layer” and it is an Internet security protocol used by Internet browsers and Web Servers to transmit important information. SSL has now become a part of a security protocol known as TLS. Because of this, the “hhtp” in the address line will become “https”. This means that the page had become secure. A digital certificate is a unique piece of code or a very large number that says that the Web Server is trusted by an independent source which is known as a certificate authority. The certificate authority is treated as a thing that both computers trust because it confirms that each computer is actually who it says it is and it also provides the public keys of each computer to the other one.