**D.3**

**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’s a cipher that’s been used for hundreds of years to substitute characters for other characters.

b.      How does it work?

Substitution works by substituting characters for other characters in the cypher language.

c.       What is a “key”?

Keys give the language of the substitution

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

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.

plain alphabet : abcdefghijklmnopqrstuvwxyz

cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

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?

You can analyze the cypher through the frequency of letters in the English alphabet

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

Using common small words to analyze the cypher such as of, to, in, the, and, for, are, that, with, have, this,

**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?

Morse code is a character encoding scheme used in telecommunication that encodes text characters as standardized sequences of two different signal durations called dots and dashes

b.      How does it work?

To write in Morse code, on would have to use a series of dots or dashes in a specific pattern in order to represent specific numbers or letters.

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

Instead of being physically written, Morse code is more commonly transmitted via electrical pulses, audio tunes, or radio signals.

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 for a letter is a single dot to represent the letter “e”. This because the letter “ e” is the most common letter in the English alphabet.

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

The longest code belong to the number “0” as it has five dashes to represent itself.

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

When transmitting messages, for the more common letters, it is easier for the messenger to give away his message to the intended target, while having enough variables to make sure each letter has a unique amount of dashes or dots to let the target know what message is being sent to them.

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

–– --- ·-· ··· ·   / -·-· --- -·· ·

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

––     ---  ·-· ···    · /            -·-· --- -·· ·

M       O R        S E (space)             C O D E

**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’s similar in  that the message cannot be read without the key.

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

The difference is that the key must be installed onto the computer. You need to know which computers are sharing information as well.

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?

DES stands for Data Encryption Standard, it was made in the 1970s and uses a 56-bit key. Since computers have become more powerful it is not considered secure  anymore because computers are capable of brute forcing them by trying all combinations.

b.      What is AES and how strong is it?

AES stands for Advanced Encryption Standard, it is a new encryption standard and uses 128, 192 and 256-bit keys. It is secure because it is much harder to brute force such a long key.

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

a.       How is it different from Symmetric-key Encryption

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. ... The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link.

b.      What is an Asymmetric-Key?

Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric)

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

a.       What is a Hash Value?

The key in public-key encryption is based on 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.

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

Public keys generally use complex algorithms and very large hash values for encrypting, including 40-bit or even 128-bit numbers.

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

If you somehow knew the has value used to encrypt the message, you could use that same value to decrypt, otherwise you would spend decades going through every conceivable combination looking for encrypted data.

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

Current public keys can have up to 128-bit numbers or 3,402,823,669,209,384,634,633,746,074,300,000,000,000,000,000,000,000,000,000,000,000,000 different combinations.

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

a.       What is PGP?

Pretty Good Privacy. A public key encryption program.

b.      What is SSL / HTTPS?

Secure Socket Layers. An Internet security protocol used by Internet browsers and web servers to transmit sensitive information.

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted.

c.       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.

d.      What is a Certificate Authority?

In cryptography, a certificate authority or certification authority is an entity that issues digital certificates.