**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 encrypts the message by which units of plaintext are replaced with ciphertext

* 1. How does it work?

Units of plaintext are replaced with ciphertext. The "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above

* 1. What is a “key”?

A key is a way of decryption for substitution cypher which is 26 letters

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

Plaintext: hello world

key = cbyvqduzofxgtplnrimjhkwesa

Ciphertext: einnd tdkng

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

Ciphertext: einnd tdkng

key = cbyvqduzofxgtplnrimjhkwesa

Plaintext: hello world

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

**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?

It encodes the 26 English letters A through Z, some non-English letters, the Arabic numerals and a small set of punctuation and procedural signals

* 1. How does it work?

It encodes text characters as standardized sequences of two different signal durations called dots and dashes or dits and dahs.

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

Morse key or CW key- A telegraph key is a specialized electrical switch used by a trained operator to transmit text messages in telegraph systems, usually in Morse code. Keys are used in all forms of electrical telegraph systems, such as landline or "wire" electrical telegraphy, and "wireless", or radio telegraphy:

- Straight Morse key

- Sideswiper Morse key

- Semi-automatic mechanical keyer or "bug" key

- Fully automatic electronic Morse keyers or "El-bugs"

- Iambic keyer

- Morse paddles

- Morse keyboards and automatic Morse code generators

- Choice of Morse 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?

Morse code

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

Simple substitution Cypher

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

The longer the code the harder to hack/decript/protected

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

••••

•

•-••

•-••

---

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

H

E

L

L

O

**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 also swamps the letters with other letters

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

The letters are in encrypted using certain mathematical equation

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?

Data Encryption Standard (DES), approved for use in the 1970s. The DES uses a 56-bit key. It had 70,000,000,000,000,000 possible combinations which is not so strong now because you could just try a all the possible combinations and easily read the message.

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

Advanced Encryption Standard (AES), which uses 128-, 192- or 256-bit keys. This encryption standard is believed to be a sufficient encryption standard for a long time because it has more than 300,000,000,000,000,000,000,000,000,000,000,000 key combinations

1. Summarize and explain the concept of Public-key Encryption. (See Slide 4)
   1. How is it different from Symmetric-key Encryption

its different from the symmetric key encryption because it is not secret it could be accessed by anyone you give to but it needs to be used with the private key to work which is in your computer

* 1. What is an Asymmetric-Key?

Asymmetric-Key is a encryption using two keys the private key and the public key.

The public key is not secret it could be accessed by anyone you give to but it needs to be used with the private key to work which is in your computer

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?

Some data is used to create the hash value which is a summary of the original value and so the hash value is added to the original value encrypting the message

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

Some data is used to create the hash value which is a summary of the original value and so the hash value is subtracted to the original value decrypting the message

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

Current Public Keys (Hash Values) have 40-bit or 128-bit numbers. A 128-bit number has a possible 2128, or 3,402,823,669,209,384,634,633,746,074,300,000,000,000,000,000,000,000,000,000,000,000,000 number of different combinations

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

Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

* 1. What is SSL / HTTPS?

SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. ... Your web server will match your issued SSL Certificate to your Private Key.

* 1. What is a Digital Certificate?

A Digital Certificate is used to encrypt online data/information communications between an end-users browser and a website. After verifying that a company owns a website, certificate authority will sign their certificate so it is trusted by internet browsers.

* 1. What is a Certificate Authority?

In cryptography, a certificate authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate