**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?
   2. How does it work?
   3. What is a “key”?; phqgiumeaylnofdxjkrcvstzwb the alphabet that is used to replace other letters. Thus, the key to decryption or encrypting a message

The simple substitution cipher is a cipher that has been in use for many hundreds of years. It basically consists of substituting every plaintext character for a different ciphertext character. It differs from the [Caesar cipher](http://practicalcryptography.com/ciphers/caesar-cipher/) in that the cipher alphabet is not simply the alphabet shifted, it is completely jumbled. The simple substitution cipher offers very little communication security, and it will be shown that it can be easily broken even by hand, especially as the messages become longer (more than several hundred ciphertext characters. Each character in the plaintext is replaced with the corresponding letter in the cipher alphabet. Decryption is just as easy, by going from the cipher alphabet back to the plain alphabet.

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

plain text= you are dumb

key = phqgiumeaylnofdxjkrcvstzwb

ciphertext= wdv pki gvoh

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

ciphertext=wdv pki qddn

key= phqgiumeaylnofdxjkrcvstzwb

plain text= you are cool

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 first step is to calculate the frequency distribution of the letters in the cipher text. This consists of counting how many times each letter appears

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

“A cryptanalyst has to find the key that was used to encrypt the message, which means finding the mapping for each character. For reasonably large pieces of text (several hundred characters), it is possible to just replace the most common ciphertext character with 'e', the second most common ciphertext character with 't' etc. for each character (replace according to the order in the image on the right). This will result in a very good approximation of the original plaintext, but only for pieces of text with statistical properties close to that for english, which is only guaranteed for long tracts of text.Short pieces of text often need more expertise to crack.Usually, punctuation in ciphertext is removed and the ciphertext is put into blocks such as 'giuif gceii prctp nnduc eiqpr cnizz', which prevents the previous tricks from working. There are, however, many other characteristics of english that can be utilized.”

**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?
   2. How does it work?
   3. What does it use instead of a “key”?

“Morse code is a method for transmitting [telegraphic](http://www.newworldencyclopedia.org/entry/Telegraph) 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." 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](http://www.newworldencyclopedia.org/entry/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. Morse code is transmitted using just two states (on and off) so it was an early form of a digital code.”

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 id for ‘E” as it is the most used letter

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

The longest code is for numbers because they are less common.

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

“The variable length of the Morse characters made it hard to adapt to automated circuits, so for most electronic communication it has been replaced by more machinable formats, such as Baudot code and ASCII. Use of Morse code revolutionized international communication. Ability to use a visual signal also meant that Morse code could be used to indicate distress and the need for assistance, whether from a life-boat at sea or from an isolated land location (signalling a searching rescue aircraft).”

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

hi this is bob=

.... .. / - .... .. ... / .. ... / -... --- -...

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

.... . .-.. .-.. ---

= hello

**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](https://computer.howstuffworks.com/question525.htm) 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. Similar to substitution cypher, this codes the information by replacing variables with other variables.”

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?
   2. What is AES 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. Because computers have become increasingly faster since the '70s, security experts no longer consider DES secure -- although a 56-bit key offers more than 70 quadrillion possible combinations (70,000,000,000,000,000), an attack of brute force (simply trying every possible combination in order to find the right key) could easily decipher encrypted data in a short while. DES has since been replaced by the Advanced Encryption Standard (AES), which uses 128-, 192- or 256-bit keys. Most people believe that AES will be a sufficient encryption standard for a long time coming”

1. Summarize and explain the concept of Public-key Encryption. (See Slide 4)
   1. How is it different from Symmetric-key Encryption
   2. What is an Asymmetric-Key?

“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](https://computer.howstuffworks.com/10-types-of-computers.htm), 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. The key pair is based on prime numbers (numbers that only have divisors of itself and one, such as 2, 3, 5, 7, 11 and so on) of long length. This makes the system extremely secure, because there is essentially an infinite number of prime numbers available, meaning there are nearly infinite possibilities for keys.”

1. Prime Numbers and Hashing Algorithms are used to encrypt messages. (See Slide 6)
   1. What is a Hash Value?
   2. How is a Hash Value used to encrypt a message?
   3. How is a Hash Value used to decrypt a message?
   4. 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. 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. 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, 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

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

“One very popular public-key encryption program is Pretty Good Privacy (PGP), which allows you to encrypt almost anything.”

* 1. What is SSL / HTTPS?

“SSL is an Internet security protocol used by Internet browsers and [Web servers](https://computer.howstuffworks.com/web-server.htm)to transmit sensitive information. SSL has become part of an overall security protocol known as Transport Layer Security (TLS).

In your browser, you can tell when you are using a secure protocol, such as TLS, in a couple of different ways. You will notice that the "http" in the address line is replaced with "https," and you should see a small padlock in the status bar at the bottom of the browser window. When you're accessing sensitive information, such as an online bank account or a payment transfer service like [PayPal](https://money.howstuffworks.com/paypal.htm) or [Google](https://computer.howstuffworks.com/internet/basics/google-tool.htm) Checkout, chances are you'll see this type of format change and know your information will most likely pass along securely”

* 1. What is a Digital Certificate?

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.

d. What is a Certificate Authority?

The certificate authority acts as a middleman that both computers trust. It confirms that each computer is in fact who it says it is, and then provides the public keys of each computer to the other.