**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’s a type of encryption where characters or units of text are replaced by others in order to encrypt a text sequence. It consists of substituting every plaintext character for a different ciphertext character.

* 1. How does it work?

Substitution Cypher works as a way to communicate using the alphabet in order to provide a description. It can easily be broken by hand especially when messages become longer. Furthermore, the procedure is varied depending on the key but it substitute every letter in the message with the substitution cipher for the entire message.

* 1. What is a “key”?

A key in simple substitution cipher usually consist of 26 letters. It can map every possible character in the plaintext message to any different value.

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

plain alphabet : abcdefghijklmnopqrstuvwxyz

cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

Encryption of the code:

plaintext : defend the east wall of the castle

ciphertext: giuifg cei iprc tpnn du cei qprcni

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

plain alphabet : abcdefghijklmnopqrstuvwxyz

cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

Encryption of the code:

plaintext : defend the east wall of the castle

ciphertext: giuifg cei iprc tpnn du cei qprcni

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 frequency analysis of letters determines a possible candidate for the cracked cipher. If a particular letter is popular for example A, all which must be done is to take the most popular encrypted letter (in this case A) and replace other letters with A.

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

This takes the most frequent one, two, three or four letter words to figure out what is the phrase or sentence being created with 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
   1. What does it do?

Morse code is a method for transmitting telegraphic information using a standardized sequence of short and long elements to represent many kinds of letters, numbers, punctuations and characters.

* 1. How does it work?

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.

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

It uses dots and dashes in order to replace different letters.

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 is either the letters t or e. They are usually the most frequently used letters, the shorter code will become a dot. For example, e is the most used letter the shorter code (dot).

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

The longest codes are the letters which consists of 4 dots or dashes. These are the letters which are the least used letters in the alphabet.

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

The benefit of having a variable length code, you will not have to type a long message to send long sentences or phrases. The variables length will shorten the length and they will be a less amount of dots and dashes that will be performed.

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

My name, Raakin Rishad will be: .-..-.--.-..-. .-………..--..

Provide an example of decoding a message using Morse code.

---.-…--…-. Will translate to Origin.

**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”?

Just like the substitution cipher, the Symmetric key encryption sends data between devices in which they both have the same key to encrypt information. Each computer has a secret key that it can be used to encrypt a packet of information before it is sent over to the other computer within the network. The Symmetric-key required that you know which types of computers will be talking to each other in which they Symmetric key will be installed in each one. This makes the code very similar to the secret code because each of the computers must know how to decode the information. Furthermore, the code also provides the key to decoding the message so the viewer will know what It means.

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?

DES is the first major symmetric algorithm developed for computers in the United States which was approved for use in the 1970s and used a 56-bit key which offers more than 70 quadrillion possible combinations. The AES is a encryption code which uses either 128, 192 or 256bit keys. This replaced DES as the Advanced Encryption Standard uses higher bit keys and consist over quadrillions or even more of combinations.

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?

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. 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.

1. Prime Numbers and Hashing Algorithms are used to encrypt messages. (See Slide 6)
   1. What is a Hash Value?

The Hash Value is a value that is computed from a base input number using a hashing algorithm. The hash value is the summary of the original value and one of the most important factors about the hash value is that it is nearly impossible to derive the original input number without knowing the data which is being used to create the hash value.

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

The Hash Value is used to encrypt messages by being multiplied by the input number and then the new number becomes the new encoded number.

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

The hash value is used to decrypt the message with a hash value and then you must divide the encoded message with the hash value in order to decode the message.

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

Public keys generally use complex algorithms and very large hash values for encrypting which includes 40 bit or high bit numbers like 128bit. A 128bit has 2128  combinations.

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

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

* 1. 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.

* 1. What is a Digital Certificate?
  2. What is a Certificate Authority?

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 certificate authority. This certificate acts as the middleman that both computers receiving the message can trust. 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.