## Lesson Proper for Week 8

**TYPES OF CIPHER**

What is a cipher? To put it simply, a cipher is the method in which data is converted from plaintext to cipher text format. In cryptography, there are many different methods. Each method is known as a cipher suite and has its own advantages and disadvantages. In this section, we'll discuss the different types of ciphers used to encode and decode messages.

**1. Substitution Cipher**

In a substitution cipher, also known as a **Caesar Cipher**, the secret key is the replacement of certain or all of the plaintext with another character, thus creating the cipher text. For example, let's say you are writing the sentence, ""the quick brown fox jumps over the lazy dog."" We, as humans, will see it in its natural form, plaintext. If we were to use a key such as A=Z, B=Y, C=X and so on, we would have the following:

**2. Transposition Cipher**

A transposition cipher simply manipulates the order or sequence of the message instead of trying to hide the message itself. There are many different transposition methods, one of which is known as columnar transposition. This variation uses the words of the message without spaces, where the width of the column itself is a fixed size and if there are any spaces remaining at the end of the last row, random characters are added to ensure the rows and columns are equal.

An example of columnar transposition while using the message *the quick brown fox jumps over the lazy dog* would result in the following: thequi

ckbrow

nfoxju

mpsove

rthela

zydogz

Another version of a transposition cipher is the rail fence cipher. This version hides some of the characters of a message. Once again, we'll use the *sentence the quick brown fox jumps over the lazy dog* to demonstrate how the rail fence cipher works. The following is the result of the rail fence cipher: t . . . u . . . b . . . n . . . j . . . s . . . r . . . l . . . d . .

Notice that there is a consistent thread where three characters are missing and there are no spaces between words. Each period (.) represents that a character is missing.

**3. Block Ciphers**

Block ciphers encrypt a fixed size (block) of data at a time. If you're sending a message and your computer is using a block cipher encryption algorithm, it would create blocks of a fixed size such as 64-bits or even 128-bits and encrypt all the data inside each block. Some examples of block cipher algorithms are: Data Encryption Standard, Triple Data Encryption Standard, and Advanced Encryption Standard, to name just a few.

**4. Stream Ciphers**

In a stream cipher, the algorithm encrypts each bit individually, therefore creating a continuous stream. An example of a stream cipher encryption algorithm is the **Rivest Cipher 4 (RC4)** cipher suite.

**5. Key**

A key, also referred to as the secret or even the secret key, is used to reorder the contents of a cipher text back to its original form. A simple analogy we can use is a room with a single deadbolt lock. To secure the contents of the room, we would need to lock the door using a specific key. This would be considered to be the encryption aspect. Once the room is locked, only people with the appropriate key can unlock the room to view its contents. This would be considered decryption.

**ENCRYPTION ALGORITHMS**

Furthering our discussion, we will dive a little bit deeper into understanding the different algorithms and how they are used to provide confidentiality.

**1. Data Encryption Standard**

The **Data Encryption Standard (DES)** is a symmetric encryption algorithm which uses the same key to both encrypt and decrypt data. It does this by encrypting a block of 64-bits in size using a 56-bit key. The size of the key makes a difference in the strength of the encryption itself; in this case, a 56-bit key is used per block. The smaller the key, the weaker and more vulnerable the encryption/algorithm is to being deciphered by a hacker.

**2. Triple Data Encryption Standard (3DES)**

The successor to the DES algorithm is the Triple DES (3DES), and this upgrade applies the DES three times to messages. The 3DES algorithm uses key sizes of 56-bits, 112-bits, and 168-bits, respectively. However, the block size still remains the same, 56-bits. To further explain how 3DES works, its uses a key to encrypt the plaintext, and the result will be ciphetext1, which is round 1. Next, it takes ciphertext1 and applies the algorithm again, resulting in ciphertext2; this is round 2. Once more, it runs the algorithm but on ciphertext2, giving the output as ciphertext3; this is the third round. The final output of the entire 3DES algorithm is ciphertext3.

**3. Advanced Encryption Standard**

The **Advanced Encryption Standard (AES)**has become the de facto for symmetric encryption standards due to its very strong encryption key sizes and its ability to encrypt large blocks of data at a time. AES uses various key sizes, and they are: 128-bits, 192-bits, and 256-bits, and the block size is 128-bits.