**CIS 406 – Information Security**

Assignment 4.3 – Ciphers

In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption—a series of well-defined steps that can be followed as a procedure. An alternative, less common term is “encipherment”. To encipher or encode is to convert information into cipher or code. In non-technical usage, a 'cipher' is the same thing as a 'code'; however, the concepts are distinct in cryptography. In classical cryptography, ciphers were distinguished from codes.

Codes generally substitute different length strings of characters in the output, while ciphers generally substitute the same number of characters as are input. There are exceptions and some cipher systems may use slightly more, or fewer, characters when output versus the number that were input.

The operation of a cipher usually depends on a piece of auxiliary information, called a [key](http://en.wikipedia.org/wiki/Key_%28cryptography%29) (or, in traditional NSA parlance, a cryptovariable). The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm. A key must be selected before using a cipher to encrypt a message. Without knowledge of the key, it should be extremely difficult, if not impossible, to decrypt the resulting ciphertext into readable plaintext.

So, long story shorter, a cipher is a way to trick others by replacing text with something else so they can’t tell what they are reading. For this lab, you will be deciphering a string of characters using one of the tools on the following linked page. The page is dedicated to simple text manipulation tools, which all can be replicated with just paper and pencil.

**For Part 1:**

1. Go to: <http://rumkin.com/tools/cipher/>
2. Review the different tools on the page.
3. Now take the following string of characters and decipher it using on the tools on the page:

Vbhs vjtfm xjt mj njp Efjimceo ahp?

(Here is a hint: Key = harmony)

1. Enter the cipher used here:

|  |
| --- |
| Keyed Caesar |

1. Enter the answer for the decipher here:

|  |
| --- |
| What would you do for Klondike Bar? |

**For Part 2: Build your own cipher and post it**

1. Review the different tools on the page.
2. Decide on a cipher tool – of course, don’t tell anyone which one you choose!
3. Take a string of characters (word, words or phrase) in raw text and list it here:

|  |
| --- |
| GRACIOUSWORDSAREAHONEYCOMBSWEETTOTHESOULANDHEALINGTOTHEBONES |

1. Enter the chosen cipher tool here along with how it works and any hints or keys that you will give to other students to help them figure it out :

|  |
| --- |
| I used the Ubichi cipher, used by the Germans in WWII, with the key deutsch. It is a double columnar transposition cipher. To use it, a key word is used to determine the number of columns and the order. The message is then entered letter by letter into the columns. The columns are then rearranged to generate the cipher text. |

1. Enter the coded message here for your chosen cipher:

|  |
| --- |
| AEEUBAOOOEDEERSLOSGGSWHIHEIECACTLTSRRTNTOOETY  WNNUBAZNSOHHMDAO |

1. Post the coded message in the Cipher Discussion Forum for other students to try.