Encryption Assignment 1

Until modern times cryptography referred almost exclusively to *encryption*, which is the process of converting ordinary information (plaintext) into unintelligible gibberish (i.e., *cipher text*).[2] Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. A *cipher* (or *cypher*) is a pair of algorithms which create the encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and in each instance by a *key*.

Caesar Encryption - First we describe the Julius Caesar encryption by alphabet shifts. We start by choosing a fixed integer, such as 5. To encipher a message, each letter is replaced by the letter 5 places down the alphabet. To encrypt V, W, X, Y, or Z, we return to the beginning of the alphabet. For instance, the message ``YES'' gets transformed to ``DJX.'' The mathematical concept here is addition in a cyclic group. Schematic wheels provide a vivid way to illustrate this simple but important idea. In fact, actual wheels with gears were used at various times in history.

Using this chart as a guide:

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

AND NOW Try this:

1. Key is +7 (so move seven letters right in the alphabet) and with the key create a code using that key for the phrase: “To be or not to be, that is the question”

2. Key is -2 (so move two letters left in the alphabet) and with the key create a code using that key for the phrase: “ Education is a progressive discovery of our own ignorance.”

3. Now come up with a three word phrase and using your own cipher key, encrypt the message. Give someone in the class your encrypted message (cipher text) and the key. Ask them to decode it.

Vigenère Encryption - Next, we introduce Vigenère ciphers, which work like the Caesar method, except that an entire block of 2, 3, 4, or 5 letters is shifted by a *key-word*. For example, if the key-word is ``dog,'' consisting of the 4th, 15th, and 7th letters of the alphabet, then the first letter of the message is shifted by 4, the second letter is shifted by 15, the third by 7, the fourth by 4 (here we return to the beginning of the key-word), the fifth by 15, and so on.

Using this chart as a guide:

A	B	C	D	E	F	G	H	I	J
0	1	2	3	4	5	6	7	8	9
K	L	M	N	O	P	Q	R	S	T
10	11	12	13	14	15	16	17	18	19
U	V	W	X	Y	Z				
20	21	22	23	24	25				

AND NOW Try this:

4. key-word is big, so this consists of the **1st, 8th, 6th** letters of the alphabet. So create a code using that key-word for the phrase: “People think computers will keep them from making mistakes. They're wrong. With computers you make mistakes faster.”

To start: **QMU**….fill out the rest

5. key-word is sun. Create a code using that key-word for the phrase: “He that would live in peace and at ease must not speak all he knows or all he sees.”

Final Problem: Find a famous quote and encrypt it using both methods above, therefore you should have two coded messages. List the key number and the key-word for each respective message. Turn in the assignment on a new sheet of paper with your name on it. This assignment should be done individually and there should be no duplicate messages, codes or keys. Tomorrow you will test the encrypted messages and keys with each other.