JUNE 6TH CRYPTOGRAPHY PROBLEM SET #1A

Three can keep a secret if two are dead.–Benjamin Franklin

Throughout history, people have needed to send messages in such a way that they cannot be deciphered even if intercepted. Ciphers are algorithms which let one encrypt or decrypt a message. We begin with a famous cipher, the Caesar shift (used by Julius Caesar).

1. For each letter of the alphabet, we associate a number between 0 and 25. Fix `A = 0,B = 1,C = 2` etc. When encrypting, simply add 3 to each number, and find the corresponding letter. For example, the word "`ROME`" is encrypted to "`URPH`". Of course, `X = 23,Y = 24,Z = 25` also have to be sent somewhere so we send them to `A,B,C` respectively. Make a table with each letter's number on a separate sheet and save it for later.

Encrypt the following phrases as Caesar would have by first translating them into numbers: "ET TU BRUTE", "I CAME I SAW I CONQUERED".

Decrypt the following phrase as Caesar would by first translating them into numbers: WKH GLH LV FDVW (I left the spaces in for ease of decryption).

2. While Caesar shifted his letters over by 3, you can shift by other amounts. The following ciphertext was encrypted with a shift of 1, 5, 10, 15, 20, or 25.

`TMETGXTCRTXHIWTITPRWTGDUPAAIWXCVH`

What was the plaintext and what was the shift? (I removed the spaces here) Work as a team to divide up the work load.

In general, why are Caesar shifts insecure? What strategies would you use to break them?

4. Write down the first name of each team member. Then encrypt it (choose your own key, a number between 0 and 25). Write the cipher text below and on the board in front of the class.

Your names (plaintext):

Your names encrypted (ciphertext):

5. Decrypt each of the other teams names by brute force. Write down the decrypted plaintext here. The first two teams to decrypt all the other names gets a point.