Cryptography: A1

Syeda Kazmi-Shah 02/22/2016

Problem 1:

Vigenere Cipher

The solution to this problem begins with first finding the key length for each block of the ciphertext. This is key in the Vigenere cipher because it will be one step to finding the key word. To do this I started by noticing common key patterns of ciphertext.

Pattern 1: $RUN_1 \rightarrow RUN_2$ = 44 letters apart.
Pattern 2: $RUN_2 \rightarrow RUN_3$ = 133 letters apart
Pattern 3: $TPR_1 \rightarrow TPR_2$ = 49 letters apart
Pattern 4: $QGZ_1 \rightarrow QGZ_2$ = 14 letters

The GCF of all these patterns were ~ 7. I then began splitting the cipher letters into blocks of seven since the keylength was a factor of 7:

YYKAEXR| QJCXONG| JYLGIBR| FMKTTMF| KHFKDME| VIWHRUN| OIIXPME| HYTMUVV| QHVLTIO | NCJAJCF| VCTXIVF| WLVWOUR| UNZVTZN| PKLBLQG| AJIHVQQ| GZFKTPR| EIDFO VQ| GZVGSMC| TIDHTMG| JYXXNME| CFNXLNN| TYRGDAR| EO IXTPR| DFVLSQA| IMFYLQO| GLKRTWB| WLJXLDR| UUEWOC E| RIJMEZV| VSUHOZQ| CCETNLR| UNRULQF| JNYBSKB| PMK BTCG| KIEHFBU| GOEBTMQ| UNRMEAB| HUDXRQP|C

Then by using the frequency chart, I noticed that for the first column, each had a different frequency for certain letters. I matched the highest frequency cipher letter to the most common letters used in the English language (E,T,A,N,O,I). From there, I found the distance between those letters and then from that distance I matched it to the number of the alphabet. For example, looking at the first column from the frequency table we noticed the letters "U" and "G" appearing the most amount of times from the first letter of each "block". From there I found the distance from both "U" and "G" to the most common used letters in English language, in this case being E. You can also test "T" if "E" doesn't work. So the distance from "U" to "E" is 17 and from "G" to "E" is 3. The 17^{th} letter of the alphabet is "Q" and the 3rd letter of the alphabet is "C". So the CHANCES of the first letter from the keyword being a "C" or "Q" is likely. We repeat this process for 6 more times since the keylength is 7. After accumulating all the probable letters, we determined the keyword to be "CURTAIN". We must understand that the keyword can be just random letters, this example is just to understand the way to figure out or break the keyword. Since we determined the keyword to be "curtain", now we look at the Vigenere square or the tabula recta. We can just say that the keyword is on the x-axis, all the letters inside the square

are the cipher-letters and the plaintext is on the y-axis. From there, we match the keyword and the cipher to obtain the plaintext.
The plaintext came out to:

WE THE PEOPLE OF THE UNITED STATES IN ORDER TO FORM A MORE PERFECT UNION ESTABLISH JUSTICE INSURE DOMESTIC TRANQUILITY PROVIDE FOR THE COMMON DEFENSE PROMOTE THE GENERAL WELFARE AND SECURE THE BLESSINGS OF LIBERTY TO OURSELVES AND OUR POSTERITY DO OR DAIN AND ESTABLISH THIS CONSTITUTION OF THE UNITED STATES OF AMERICA

Problem 2

Monoalphabet Cipher

The solution to:

CIJUQCIZQFIZALSBPUFCRLIPBFIEIHYLX QIHYLOLILEIBFQXBZJSXDJXXDLSOLILELIPLNX ASUBICJAXDJUMSBFYLISCFNDXDLSOLILXDLAJZXELBEALSBF QLKELNXXBRLHUYBAYLQ HUJUSXDHUWZXIJUWLBICSZXLIHBFZRLNJFZLXDLSVFZXQHQUXDBAQOHXDZFNDUBU ZLUZL

Is mostly based on frequency analysis. I first began by seeing if this was based on a key shift, and came to a conclusion that it was not: no words were being formed with any of the key shifts I used. I then, began noticing repeating cipher letter and looking at the letters which were repeating the most times. I found "L" to be the letter repeating the most. I associated "L" with one of the most common English letter: E. I linked every "L" with "E" and moved on to the next frequently appearing letter in the cipher-text, which was X, and ended up linking it with one of the other commonly used letters in the English alphabet: "T". The next common appearing letter in English letter is "A" but was not consistent or did not make any sense when I matched the third most frequent appearing letter in the cipher to the letter "A". So I moved onto some other method. Next, I tried associating certain repeating patterns in the text such as "XD" and "XDL" with commonly used English words, which is the word "the". I then filled in those letters with the the cipher-text associated with them. I concluded that the same cipher-text letters were associated with the same plain-text letters. I repeated the process until I deciphered the entire cipher-text to be:

MR AND MRS DURSLEY OF NUMBER FOUR PRIVET DRIVE WERE PROUD TO SAY THAT THEY WERE PERFECTLY NORMAL THANK YOU VERY MUCH THEY WERE THE LAST PEOPLE YOUD EXPECT TO BE INVOLVED IN ANYTHING STRANGE OR MYSTERIOUS BECAUSE THEY JUST DIDNT HOLD WITH SUCH NONSENSE