Homework 3

Question 1:

Encoded Message:

**UBQBKDVOUKNDQNQOKFNENDNT**

My process to do this started with the playfair grid. First, I determined the order of the grid, since GREENDAY has a duplicate E, the first part of the grid looks like this

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **G** | **R** | **E** | **N** | **D** |
| **A** | **Y** |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Then, I inserted the rest of the alphabet, ignoring letters I have already used

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **G** | **R** | **E** | **N** | **D** |
| **A** | **Y** | **B** | **C** | **F** |
| **H** | **I/J** | **K** | **L** | **M** |
| **O** | **P** | **Q** | **S** | **T** |
| **U** | **V** | **W** | **X** | **Z** |

Now, I looked at the keyword. Observing if there are any repeating letters in “WAKEMEUPWHENSEPTMBERENDS”, we see that there are actually none! The last check is to see the length of the plaintext, which when calculated is 24. Since it is even, we don’t need to add a padding character to the end! All that is left is to use the grid to encrypt.

By hand, I followed all of the playfair steps, ensuring that for example, “WA” gets mapped to “UB” since it is a “box” case (no shared row/column). For the other 2 cases, for example, “KE” gets mapped to “QB” since “KE” have the same column in the matrix. For the last case, for example, “EN” gets mapped to “ND”, since “EN” have the same row in the matrix. Doing this process allowed me to produce the Encoded message at the top.

Question 2:

Decryption key for :

For this problem, since it asks us for the inverse of the hill matrix, we need to apply a slight modification of the inverse matrix formula. The formula used in this was , all under mod 37, as instructed in the problem. First, we obtain the value of , which is equivalent to . Upon further simplification,

Now, we must look for the inverse of 34 mod 37, upon some observation, we see that , and . Since we can express this as , and rewrite this as , we see that the modular inverse of 34 is 12 under mod 37.

The last step is to multiply this value to the matrix . Doing so:

By applying the formula to find the inverse hill cipher, we have obtained this result, upon observation, we can see that

Which is required condition, proving that this matrix is the inverse of the original.

Question 3: Yeah I didn’t do it

Question 4:

Since this question asked for a code file, it is added with my solution

My general process was to first fill in a playfair grid. I did this by used a used Boolean array to keep track of what characters I already placed in the keyword. This way, if we have a word such as “bananas”, the letters that get inserted in order are “bans”. My next process was to fill the rest of the playfair grid, by using this used Boolean array.

After I got the playfair grid, I went through the plaintext and inserted ‘x’ whenever there was a double character present. If the double character was ‘x’, I would insert a ‘q’ between them instead. My last check for the plaintext was to if the length was odd or even after the insertions, if it was odd, I inserted ‘x’ at the end unless the last character was an ‘x’, in this case I inserted ‘q’.

Lastly, I built up an answer string by using the playfair grid. With the used array, I also kept track of what indexes each letter had when I was filling the grid, so it came down to a matter of identifying whether two letters make a box or shared a row/column. If the shared a box, I would append the opposite corners of the “box” the characters make, if they shared a row, I would append the two characters directly to the right of the originals, and if they share a column, I would append the two characters directly downward compared to the originals. All of these were done using the mod operator to ensure I don’t go out of bounds on my grid.