HW 5 which is LAST YEARS MIDTERM

NOTE- This is Last Years Midterm BUT I omitted one problem which is on material we have not covered.

NOTE- THIS HW IS TWO PAGES LONG. DO NOT MISS THE SECOND PAGE.

1. (25 points) The alphabet is $\{a, b, c, \ldots, z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Alice wants to use the shift cipher where she shifts by 2. She wants to send

   Bob for prez in 2016

   What does Alice send? (Make all of the capital letters small, break it into blocks of 5, and then do the shift.)

2. (25 points)

   (a) Alice wants to use a linear cipher, that is $f(x) = ax+b \pmod{36}$. Are there any restrictions on what a, b are aside from $a, b \in \{0, \ldots, 35\}$? If so, why do we need that restriction? Given an example of an (a, b) that works and an (a, b) that does not work.

   (b) Alice wants to use a 2×2 Matrix cipher with matrix

   $$\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

   Are there any restrictions on what a, b, c, d are aside from $a, b, c, d \in \{0, \ldots, 35\}$? If so, why do we need that restriction? Given an example of an (a, b, c, d) that works and an (a, b, c, d) that does not work.

3. (25 points) READ THIS ENTIRE QUESTION BEFORE ANSWERING IT. REALLY. I MEAN IT!!!!!!! In this problem you will explain Diffie-Helman and, at the same time, do an example. Your explanation of each step will be COHERENT, CLEAR, and CONCISE!!!!!!!!! They use the prime 11. Note that 11 is a safe prime since $\frac{11-1}{2} = 5$ which is prime. (The page after this one is blank in case you need it.)

   (a) Explain how they can find a generator quickly given a safe prime p (Recall that a prime p is safe if $\frac{p-1}{2}$ is also a prime.) Use this method to find the smallest number that is a generator mod 11. For the rest of the problem we call the generator you found g.

(b) Recall that Alice picks a random number a in $\{2, \ldots, p-2\}$. Explain what Alice sends to Bob given this number. What does Alice send to Bob if $p = 11$, g is the g you found in part 1, and $a = 5$.

(c) Recall that Bob picks a random number b in $\{2, \ldots, p-2\}$. Explain what Bob sends to Alice given this number. What does Bob send to Alice if $p = 11$, g is the g you found in part 1, and $b = 6$.

(d) Once Alice and Bob have send each other messages, what do they do to determine the shared secret key? What is the shared secret key when $p = 11$, g is as in part 1, Alice's random number is $a = 5$, and Bob's random number is $b = 6$.

4. (25 points) (For this problem the alphabet is $\{a, b, c, \ldots, z\}$.) In this problem you will end up giving a description of a modification of the VIG cipher where we use a set of five 2×2 matrix ciphers as the key. We denote those matrices M_0, M_1, M_2, M_3, M_4.

(a) Write the psuedocode for the following:

Input: the matrices M_0, M_1, M_2, M_3, M_4 and a text T.

Output: the ciphertext T' that Alice sends using VIG-matrix with M_0, M_1, M_2, M_3, M_4.

Also explain in English. BE COHERENT AND CLEAR!!!!!!!!!!!!!!

(b) Assume Eve knows the LENGTH of the key. Explain how she can then CRACK the message.

(NOTE- be very clear in your answer. Someone should be able to read your answer and know just what to do if they are Alice or Eve.)