Homework # 1

Homework is due Sep 22, before 11:59pm
Submission Instructions:
email to TA
Andrew Zonenberg  zonena@rpi.edu
Jeremy White  jwhiterpi@gmail.com

PART A. (50pnts)

Please show your work to get full credit.

1.) Playfair Cipher.
    a. Construct Playfair matrix with the key “NETWORKSECURITY”.
    
    b. Encrypt the message: “OUR NEW PASSWORD IS TELECOM”.
    
    c. Decrypt the message: “AVYSTKQNSTYWFNGTKC”.

2.) Hill Cipher.
    Consider the Hill Cipher where the encryption and decryption is performed as follows:
    
    \[ C \equiv P \cdot K \mod 26 \]
    \[ P \equiv C \cdot K^{-1} \mod 26 \]
    
    Where C (ciphertext) and P (plaintext) are row vectors of size 2, and K (key) is a 2 X 2 matrix. Given the key matrix and enumeration below, answer the following questions.
    
    \[ K = \begin{bmatrix} 9 & 13 \\ 2 & 3 \end{bmatrix} \]

    a. What is the ciphertext corresponding to the plaintext “NETSEC”
    
    b. What is the plaintext corresponding to the ciphertext “YIFZMA”? 
3.) Affine Cipher.
   Affine cipher is a generalization of the Caesar cipher. For each plaintext p it substitutes ciphertext c:

   \[ c = E([a, b], p) \equiv (a \cdot p + b) \mod 26 \]

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

   a. What is wrong with \( c \equiv (13 \cdot p + 4) \mod 26 \) as the affine cipher encryption function?

   b. It is known that the ciphertext “QRPYQHRA” is encrypted with affine cipher mod 26. If the first two letters of the plaintext are “RA”, what are the affine plane parameters \([a, b]\)? What is the plaintext? (Hint: some of the inverses in modulo 26 are given below.)

<table>
<thead>
<tr>
<th>3^{-1}</th>
<th>5^{-1}</th>
<th>7^{-1}</th>
<th>11^{-1}</th>
<th>17^{-1}</th>
<th>25^{-1}</th>
<th>…</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>21</td>
<td>15</td>
<td>19</td>
<td>23</td>
<td>25</td>
<td>…</td>
</tr>
</tbody>
</table>
4.) A Cipher. 
The key “THE QUICK RED FOX JUMPS OVER THE LAZY BROWN DOG” is used to create the ciphertext:

“ABCWCQAQTCKFYABCXLISJFQXLIABSCQQFKYLLYCOCOWCIQALGSLQCABCJLLI”

a. What is the encryption algorithm?

b. How secure is it?

c. What is the plaintext?

PART B. (50pnts)

Implement Simplified DES (see the class notes and the text book)
- 8-bit blocks and uses 10-bit key
- Only 2 rounds