A block cipher method called chaining can be used to make a much more secure ciphertext message. In this problem you will use the cipher block chaining method to encrypt a message. You can use any programming language that you like.

Here are the steps you should follow:

1. Convert the ascii key to a binary (10101010) representation.
2. Convert the ascii text to binary representation.
3. Break the binary text from number 2 up into some larger blocks (you will use 12 bits as your block size, but you theoretically could use anything). If the last block is less than 12, you should add alternating 1’s and 0’s to it until you have 12. Finally, if you added some padding, you should append a final block (of size 12) that contains the number of bits you added. I.e. If I added 4 bits of padding, I would append the block ‘000000000100’ as the final block to be encoded.
4. Each of the above (12 bit) blocks will now be encrypted, following this process:
   a. Take the first block to be encrypted, reverse it, Xor it with the first 12 bits of the key. (store as first block of encrypted output)
   b. Take the next block and Xor it with the encrypted output of the first block. Reverse the new block, xor it with the first 12 bits of the key. (add to encrypted output stream)
   c. repeat until all the blocks are encrypted.

Your code should take an input file with the ASCII key on the first line, the text to be encoded on the remaining lines, convert them to their binary representation, and use the cipher block chaining method as described above to ‘encrypt’ them. The resultant bitstream should then be output.

Example: ABC is my key ABCDE is the stuff I want to encrypt

This input:

ABC
ABCDE

Should produce this output:

011010010110111010100110000011100001100100101110001001001011101

Hints:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Convert ASCII key to binary (10101010) representation.</td>
</tr>
<tr>
<td>2</td>
<td>Convert ASCII text to binary representation.</td>
</tr>
<tr>
<td>3</td>
<td>Break binary text into blocks of 12 bits. If last block is less than 12, add alternating 1's and 0's until it reaches 12. Append a final block containing the number of padding bits. Example: '000000000100' for 4 bits of padding.</td>
</tr>
<tr>
<td>4</td>
<td>Encrypt each block as follows: reverse it, Xor it with the first 12 bits of the key, store as first block of encrypted output. Take the next block, Xor it with the previous encrypted output, reverse it, Xor it with the first 12 bits of the key. Add to encrypted output stream. Repeat until all blocks are encrypted.</td>
</tr>
</tbody>
</table>

Example:

- Key in binary (first 12 bits): 010000010100
- First 12 bit block (reversed): 001010000010
- XOR: 011010010110 #first 12 bits of encrypted output

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Additional steps include adding the padding block and appending the last block containing the padding count. Example: 000000000100 for 4 bits of padding.</td>
</tr>
<tr>
<td>6</td>
<td>XOR the last block with the previous encrypted output, reverse it, XOR it with the first 12 bits of the key. Add to encrypted output stream.</td>
</tr>
</tbody>
</table>

And so on...
To pass off

Demonstrate that your code works. Maybe by showing that the given input produces the expected output. Upload your code as well.