Kryptos 2020 Challenge 1 solution:

Observations:

- The ciphertext comes in pairs, so maybe a Polybius or playfair cipher was used.
- The first letter of each pair always come from: I, L, A, C, E [five choices]
  
  Second letter of each pair come from: A, O, B, N, D [five choices]

  This makes one think of a 5 X 5 Polybius square.

- Assuming that each pair of ciphertext letters corresponds to one plaintext letter, one could begin to use frequency analysis on the letter pairs to get a good idea of what the substitutions are (i.e. just treat as a MASC).
- Alternatively, one could begin to build the key:
  - The letters forming the first letters of each pair can be rearranged as: ALICE
  - Which means a reasonable rearrangement of the second letters are: ANDBO[b]
  - We have Alice and Bob!
  - The unencrypted part of the text messages indicate a key using three characters. Since we have Alice and Bob, maybe the third character is EVE

The above observations should allow one to reconstruct the Polybius square used:

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>N</th>
<th>D</th>
<th>B</th>
<th>O</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>a</td>
<td>n</td>
<td>d</td>
<td>e</td>
<td>v</td>
</tr>
<tr>
<td>L</td>
<td>b</td>
<td>c</td>
<td>f</td>
<td>g</td>
<td>h</td>
</tr>
<tr>
<td>I</td>
<td>i/j</td>
<td>k</td>
<td>l</td>
<td>m</td>
<td>o</td>
</tr>
<tr>
<td>C</td>
<td>p</td>
<td>q</td>
<td>r</td>
<td>s</td>
<td>t</td>
</tr>
<tr>
<td>E</td>
<td>u</td>
<td>w</td>
<td>x</td>
<td>y</td>
<td>z</td>
</tr>
</tbody>
</table>

Plaintext:

1: I have the javascript code ready to go
2: we are all set with a cross site scripting attack
2: we need to upload payload by tomorrow
1: ok. I can do this at six twenty tonight. Luck
2: luck