Quiz #1 Results by Question

<table>
<thead>
<tr>
<th>Question</th>
<th>Q1-1</th>
<th>Q1-2</th>
<th>Q1-3</th>
<th>Q1-4</th>
<th>Q1-5</th>
<th>Q1-6</th>
<th>Q1-7</th>
<th>Q1T</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perc</td>
<td>80.56</td>
<td>66.4</td>
<td>50</td>
<td>70.8</td>
<td>69.8</td>
<td>51.2</td>
<td>100</td>
<td>61.58</td>
</tr>
</tbody>
</table>

Key observations:

1) Best score was on decrypt shift → to be expected. Most points lost were due to lack of showing work. Please show work.

2) For the three "blue" questions, the EEA is definitely much harder than Vigenere but these averages are nearly the same. So kudos for studying the EEA, but I do think a question like #4 can get a higher class average if ALL students prepare. The latter is the key...I believe all students who adequately prepare got 9 or 10 out of 10 on that question...

3) Question 6 seemed very difficult for some and very easy for others. Questions like this one reward students who do some of their codebreaking work on their own and ahead of time. If you had started working on the Vigenere code break, this is something you would have coded up.

```
for (int i = 0; i < 100; i++) {
    numerator += numCandy[i];
    total += 1;
}

numerator += (numCandy[i] + numCandy[i-1]);

x = x - 1  
5 * 5 - 1 = 24

and: x = (x-1)  
5 * 4 = 20
```
ADFGVX Cipher - Germans WWI

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>D</th>
<th>F</th>
<th>G</th>
<th>V</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Step 1: Find your plaintext letter in grid.
This encrypts as row letter / col letter.
R \rightarrow VG

So far nothing but substitution!

Step 2: Use a traditional transposition cipher w/ a keyword.
2 main ways to obfuscate info:
1. Change symbols (confusion)
2. Move symbols around (diffusion)
Pick a key word

K N I G H T S

What key word has repeated letters?

B A S E B A L L

→ for ties go left to right

N I G H T S

Write msg from top to bottom left to right

F X A X X F F
V F D G X D A etc.

then read the message off by columns
all column label 1
all column label 2, etc

This is the final cipher text !!!