# Quiz #1 Results by Question

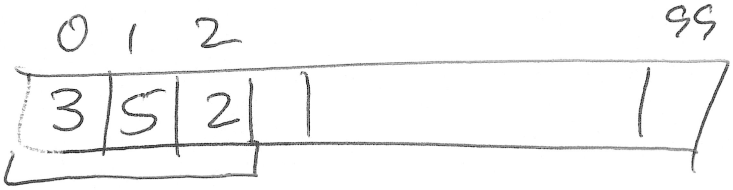
| Question | Q1-1 | Q1-2 | Q1-3 | Q1-4 | Q1-5 | Q1-6 | Q1-7 | Q1T |
|---|---|---|---|---|---|---|---|---|
| Perc | 80.56 | 66.4 | 50 | 70.8 | 69.8 | 51.2 | 100 | 61.58 |

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++) {
        ~~numcandy~~ total += numcandy[i];
        numerator += ~~{~~numcandy[i] ~~+numcandy[i]~~ *
                                    (numcandy[i]-1);
}
```

X * X − 1     5×5−1=24

and   X * (X−1)     5×4=20

CIS 3362 9/11/23

ADFGVX Cipher - Germans WWI

25 5×5

36 6×6 (26 letters, 10 digits)

key each cell has 1 item from set.

|   | A | D | F | G | V | X |
|---|---|---|---|---|---|---|
| A |   |   |   |   |   |   |
| D |   |   |   |   |   |   |
| F |   |   |   |   |   |   |
| G |   |   |   |   |   |   |
| V |   |   |   | R |   |   |
| X |   |   |   |   |   |   |

Step 1: find you plaintext letter in grid

this encrypts as row let/col let

$$R \Longrightarrow \boxed{VG}$$

so far nothing but substitution!

Step 2: use a tradition transposition cipher w/a keyword.

→ changes order of letters

2 main ways to obfuscate info

① change symbols (confusion)

② move symbols around (diffusion)

Pick a key word

| | | | | | | |
|---|---|---|---|---|---|---|
| ④ | ⑤ | ③ | ① | ② | 7 | ⑥ |
| K | N | I | G | H | T | S |

What keyword has repeated letters?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ③ | ① | ⑧ | ⑤ | ④ | ② | ⑥ | ⑦ |
| B | A | S | E | B | A | L | L |

→ for ties go left to right

Write msg from top to bottom left to right

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ④ | ⑤ | ③ | ① | ② | 7 | ⑥ | |
| Ⓚ | N | I | G | H | T | S | |
| 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!!!