last name **first names** **id#**

c210W2016qz2 45min alloweddevices:Vsquare,cipherdisc closedbook page 1/1

1. About how many civilians died in the sinking of the Lusitania?

   In WWI, how did the British gain access to German transatlantic telegrams?

   What was Zimmermann's response when asked if he had sent the telegram?

   Roughly how long did the Germans take to realize the Brits had cracked their cryptosystem? Explain.

2. Using the `ADFG` cipher (the `ADFGVX` cipher with a 16 letter alphabet), encrypt plaintext `retreat` with keyword `car` and this grid:

```
E T A O
I N S H
R D L C
U M W G
```

   ciphertext after 1st phase:

   final ciphertext:

3. Here are two one-time pad ciphertexts from the same key. If 1st trigram of 1st plaintext is `a s k`, then 1st trigram of 2nd plaintext is `_ _ _`. Show your work, and explain whether this is likely.

```
p r y k w v b j l t l
s n b l b c h t u r k
```

4. Language Q has letters `e o r t` with typical frequencies .4 .2 .1 .3. Here is some Q Caesar ciphertext, where the shift was 1 (`eort` to `orte`) or 3 (`eort` to `teor`): `o e r t r t t r`. For each shift, give the plaintext and index of mutual coincidence of plaintext with typical Q text. Show your work.

shift	plaintext	IMC plaintext-Qtext
1		
3		

5. Decrypt this book ciphertext. 14 27 17 8 27 2 15 11 17 5 2 0 13 24 27. Count from 0.

```
The vast sun was past its zenith, hot like an xray.  Giant pandas raced back and forth.
A mangy cat jumped on the kid, until then quietly eying the dozing newt.  He yelped.
```

   Why is this a bad choice of key for the book cipher? Explain briefly.