**Written Problems:**

1. Using a standard M3 enigma machine from 1938, how many possible start conﬁgurations are there for encrypting a message? Explain explicitly what contributes to the number of possible options and which component contributes the most to this value.

A: For M3, there are 26x26x26x26x60 = 27,418,560 (60 is because )

I think rotors contributes most to M3.

1. Imagine you are working for the Polish Cipher Bureau before 1938 and you manage to uncover the ﬁrst three letters of a message encrypted using enigma. What information does this give you about Enigma’s corresponding settings?

A: Perhaps the first three letters can tell me some kind of format in the enigma. And if the three letters have the same letter I may know that even the same letter can be encrypt to different letters. So the settings may be change every time maybe they have something like rotors in it?

1. Cryptography, and security in general, is a ﬁeld where the past seems to repeat itself. Do some research into how the Allies broke ciphertexts encrypted using Enigma machines. Choose one speciﬁc kind of analysis done by the Allies and describe it in detail. When was it used? Did the Germans counter the attack and if so how? Lastly, at a high level, can you ﬁnd an analog to this form of attack in modern encryption protocols? Why or why not?

A: Allies can broke it is depend on three important basics. The first is that the allies have chance to see how enigma exactly looks like by getting commercial enigma machine and get some of the mechanisms in it. Second is that the message send by Germans have some format and it can use to speculate the words and the cypher mechanism. Third is that because the same letter in cannot be encrypt to itself again so that allies can use this to exclude some possibilities and finally get the right plain text. German counter this attack by using more rotors and adding a plugboard which can make the break more difficult.

I think this is kind of semantic attack. I think in URL, we can use this kind of attack.

However, if we only try brute force, it will be very difficult to do this because nowadays people use more complicated and more longer keys. It is very difficult to calculate every possibilities.