cmput210 asn3 (revised) due in class 930am march 7 40 marks

Late assignments (under the door of Athabasca Hall 301 within 24 hours of the due date) will be docked 10%. Later assignments will not be marked: their weight will be transferred to the final exam.

Each group should hand in one (1) only assignment.

1. **If you leave any part of this question blank, your assignment will not be marked and its weight will be transferred to the final exam.** In alphabetic order by first name, print first name, last name, and ID number of each group member (at most 5) for this assignment:

   ____

   ____

   ____

   ____

   ____

   Acknowledge **all** sources, including all references and all people not in your group with whom you discussed any part of any question (for each discussion, list the relevant questions) (continue on the back of this page if there is insufficient space):

   Each group member must read, agree to, and sign this statement:

   I am familiar with the Code of Student Behaviour. I understand that there are significant penalties for any infraction of this Code. Regarding the questions on this assignment, I have not shared or received any detailed information regarding any of these questions with anyone outside my group, and any non-detailed communications have been cited above by both parties.

   ____

   ____

   ____

   ____

   ____

2. Use the Speiss enigma simulator at `http://enigmaco.de/enigma/enigma.html`.

   i) [2] Use this key: rotors II-III-I (to move a rotor out of position, move an unused rotor in); no plugboard pairing; initial rotor settings ZYX. How many letters do you have to type in before the second rotor changes from Y to Z? Explain briefly.

   ii) [2] Give the first three letters of your first name. Use the key from i), except initial rotor settings should be these 3 letters. Give the ciphertext for plaintext `wettervorhersage`. (Eg. if your name's first 3 letters are ZYX, the ciphertext is `BPIOWFIWPFHFYDSN`).

   iii) [2] Repeat ii), but change the key to use plugboard pairings AB CD EF (so 3 cables: now with initial setting ZYX the ciphertext is `AJIODEIWPEPEYOSC`).

   iv) [2] Give a simple rule which describes which ciphertext characters will be the same in your answers to ii) and iii).

   v) [2] In combat, the above initial rotor settings are a bad choice: why? In your answer, define the word *cilly*.

3. i) [2] For the Speiss Enigma simulator, key rotors II-III-I, start ROT, no plugboard cabling, give ciphertext for XXXXXX. Repeat for YYYYYY. Repeat for ZZZZZZ.

ii) [4] For the same key, below are ciphertexts for AAAAAA BBBBBB ... WWWWWW. Using your answer from i), for this key, give the Rejewski 1-4 fingerprint, 2-5 fingerprint, 3-6 fingerprint.

```
FYMEYI CGVQZP BXIWMT NELHJM TDSAFN ASKJEY KBRMUL XIUDWZ
LHCRSA QNOFDO GRFYTU IVDVRG OQAGCD DJYTPE MTJUQJ RUWSNB
JMZBOX PKGILS VFEPIR EOXNKC WPHOGK SLBLXW UZPCHV
```

4. i) [2] In what war were (single) cipher discs used? Did the group that used them win the war?

ii) [2] Which of these two encryption systems is harder to break: fixed-position cipher disc, fixed-position code-o-graph? Justify briefly.

5. i) [2] Let k_0 be the number of keys of the Enigma with 3 slots, 3 rotors, and 6 plugboard cables (so 12 plugs). Give k_0, roughly. Explain briefly.

ii) [2] Let k_1 be the number of keys of the Enigma with of the Enigma with 3 slots, 4 rotors, and 5 plugboard cables (so 10 plugs). Give the ratio of k_1/k_0. Explain briefly.

iii) [2] True or false: given the large number of keys, the Enigma is practically unbreakable. Explain briefly

6. i) [2] Name the two people who developed the Enigma. Name two others who developed similar machines around the same time, and their countries.

ii) [2] Explain why the Enigma was commercially successful, but the other machines were not.

7. Below is Enigma ciphertext. The crib for the plaintext is `erwarterommelspaetdienstag`.

```
LZJPQFHHMFJCOWUBPREDTNBUZUCMUCMMRMQN
```

i) [2] Among $\{1, 2, 3, \ldots\}$, which positions are **not** possible as a starting position for this crib? Explain briefly

ii) [1] For each letter x of the alphabet, define $f(x)$ as the distance of that letter from a. So $f(a) = 0$, $f(b) = 1$, $\ldots$, $f(z) = 25$. Let t be the first letter of your last name. Let $y = f(t)$ mod 3. Give t and y.

iii) [4] If your $y = 0$ (respectively 1,2) : give the Turing graph obtained by aligning the crib starting at position 6 (resp. 9,7).

iii) [3] The correct alignment is 6. The Spiess Enigma setting is I-II-III HDX. Find the correct cabling. Show your work.