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

cmput 210 W'16 **asn 2** **due 15:30 Th Mar 3**

You can work in groups, but hand in only 1 assignment per group. For each page (1,2), put those answers on one page (so hand in 2 pages), each with your name and id. Show your work.

1. (i) At one point the Germany Navy had an Enigma with 8 rotors and 5 slots. Give the number of possible rotor/slot assignments. (ii) Give the number of ways to assign 5 rotors to 3 slots in which rotor I is not in slot 1, rotor II is not in slot 2, and rotor III is not in slot 3. (iii) Initially, the number of plugboard cables was 12. Later, the number of plugboard cables was increased to 20. Give the number of ways to cable 10 pairs of letters, from a 26-character alphabet. What is the ratio of this number to the number of ways to cable 6 pairs of letters ? (iv) In the text (paperback: page 136), Singh gives the number of keys for a particular version of the Enigma as roughly 10^{16}. What would this number be if there were 4 rotors, and each could be placed in any position?

2. For the Speiss Enigma simulator, rotors V-IV-III, start YEG, compute the 1-4, 2-5, and 3-6 Rejewski cycle decompositions. Hint: encryption of prefixes `AAAAAA, BBBBBB, ..., WWWWWW` is shown below. Find encryption for `XXXXXX, YYYYYY, ZZZZZZ`, then do as Rejewski did.

   `NICPZM CRFOIP BJAEJF INJNWX KWICTR SYBXPC QUTRXW JTWMSO DAESBQ HCDTCZ ESLZVV`

   `XZKUUY VVZHQA ADYDRT TPVBYH YORAFB GXSVMI WBPGNE FKQIHU OHGJEN ZGXLLS MMOQKK REHYDG`

3. To construct a Rejeswki permutation of an Enigma setting, say the 3-6 permutation, one first needs to collect 26 message prefixes, each with a different letter in position 3. Explain why it is sufficient to have 25 such messages.

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

---

cmput 210 W'16 **asn 2** **due 15:30 Th Mar 3**

4. (i) By design, the Enigma never mapped a plaintext character to the same ciphertext character. Below is a possible alignment (start position 5) of a plaintext crib with some Enigma ciphertext. Give all other possible starting positions for the crib in this ciphertext.

```
. . . . w e t t e r n u l l s e c h s . . . . . . . . . . . .
P M M H I Y K P N X O K M J D O Y Y G E E A X C Z N G J E S H
1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
```

   (ii) Give the Turing graph for (i). Find a cycle. What positions does it use?

   (iii) Turing's Enigma bombe malfunctions: it tells you `rotors I-II-III setting HDX` but not the letter that starts the cycle. Use Speiss's Enigma simulator to find the starting letter: at 1st cycle position, enter a letter a, and read $b = \text{encrypt}(a)$; at 2nd cycle position, enter b, and read encrypt(b). Continue like this, and find whether a yields a cycle. Show your work for $a = A$; then try other choices for a until you find a cycle.

   (iv) Find the plugboard settings that led to the above ciphertext.

   (v) Decrypt the complete message.

5. On the morning of 1 March 1940, Bletchley Park receives the following Enigma-encrypted message prefaces, all sent between 0300 and 0900 that day.

```
LUIMLW XVGNFF YIPVOT MOLFPD ZZDYCY JTQDYO UJCIKV QDOWSU
THWGWR FXFZHS PMYSBB ALZOZZ DYJAVH SEEBDX RAHLEA KWVRRK
HSTXQL ORSPIE NGXKXJ IBRUAI GCKTNC WQUCJP VKMHTG BNNQGN
CFBEMQ EPAJUM
```

   At Bletchley, do you think they would compute the cycle length vectors for all three permutations (1-4, 2-5, 3-6), or just for one? Justify.

   Explain how cryptanalysis changed at Bletchley on 1 May 1940.

6. Write `windtalker` in the Navajo alphabet code. Use Singh Tbl.12 (p196).

7. Using the Navajo alphabet code to write encrypted words is time-consuming. Why was this not a problem for the code users?