Assignment 3 extension tasks

Menu Analysis

The length of the menu affects the building of the steckerboard but, as long as the menu covers all the letters in the steckerboard this can be built. Using the examples from the assignment page, we can see this more clearly:

Using the following crib:

- Plain = TURINGBOMBEHASKELLSIMULATIONSTOP
- Cipher = LKFMTWMTVKDEIVXHFHMNFDAZDRLMYQFR

Running longestMenu and breakEnigma on this crib gives us the following:

- longestMenu = [26,22,12,19,4,0,17,11,15]
- offset = (2,0,10)
- steckerboard = [('B','E'),('Q','H'),('W','T'),('S','N'),('J','I'),('X','A'),('Z','L'),('O','M')]

I wrote the function 'checkCorrectness :: Crib -> String' that given a crib, it returns valid if it can successfully decode the cipher to the plain, and returns an unfinished decode otherwise, using the same crib this confirms that the breakEnigma has succefully found all the pairs in the steckerboard and was able to decode the cipher successfully

Now looking at the following crib:

- Plain = COMPUTERSCIENCECALIBRATIONSTRINGTESTINGONETWOTHREE
- Cipher = QWAVMZPNGFQVGWGYCKCXXHMEXTCGWPFOCWCSYXAEFUNXQFIZJW

We get:

- longestMenu = [7,25,42,12,31,39,14,38,21,46,23,41,4,2,16,13,43] of length 17
- offset = (0,0,0)
- steckerboard = [('Q','C'),('W','I'),('S','H'),('X','A'),('U','E'),('G','T'),('R','M')]

Using checkCorrectness however returns us the partial decode:
COMYUTWRSCIZNCECAPIBRATIONSTRTNGTESTINGONETWOTHREE.

The plain was encoded using the following steckerboard:
[('L','P'),('C','Q'),('M','R'),('H','S'),('G','T'),('E','U'),('D','V'),('I','W'),('A','X')].

The two pairs missing are ('P','L') and ('D','V'). If we look at the plain text we will find that the letters P and L occur only once and the letters D and V are not in the string at all. From this we can conclude that a longer menu can be useful but as long as it covers every letter we should be able to obtain a steckerboard. Further evidence of this is given by the 2 short examples given in the assignment page, which can be deciphered even though they are only 7 characters long, this being thanks to the difference in letters.

Testing Results

Test 1:

- Plain: COMPUTERSCIENCECALIBRATIONSTRINGTESTINGONETWOTHREE
- Cipher: QWAVMZPNGFQVGWGYCKCXXHMEXTCGWPFOCWCSYXAEFUNXQFIZJW
- Result: Just ((0,0,0),[('Q','C'),('W','I'),('S','H'),('X','A'),('U','E'),('G','T'),('R','M')])

Test 2:

- Plain: AFJEQTMC
- Cipher: FJEQTMCF
- Result: Just ((0,0,0),[('I','C'),('P','M'),('U','T'),('L','Q'),('D','E'),('B','F')])

Test 3:

- Plain: TURINGBOMBEHASKELLSIMULATIONSTOP
- Cipher:
  FDLQIYHKFXSYEEXAYTWJBNNMFCHUACVMERSLXIXVWCCOBSVUESKCQGKSCXSQUMCWLWXCW
  NDEKHCGRKAUWLSCNUUROQVOTZCWUICNEXDCQPKQKHSTFTCQJXEFKDLKOTH
- Result: Just ((1,2,14),[('V','Y'),('C','H'),('J','M'),('N','A'),('B','E'),('S','X')])

Test 4:

- Plain: COMPUTERSCIENCESHEFFIELDUNIVERSITYSTOP
- Cipher:
  YZCSDCVUFVJAAEMVILWRVSQZFCBPJFVYHUUPHLAPJMTMFNLURRADJFCBRBXBCUSSXVYWAPQI
  RCUVVNODKELDMNNQHYFEFOZPBUIPWKPXIYPKQHMVOAVXFVDCKMZOULMTQNUFBVHFUSXY
  CYPWFKBYW
- Result: Just ((4,3,7),[('B','Z'),('L','D'),('G','R'),('X','F'),('J','U'),('K','C'),('O','M'),('E','N')])