Task 1. *Barr 2.8 exercise 1*

Task 2. *Barr 2.8 exercise 6*

Task 3. *Barr 2.8 exercise 7*

Task 4. *Go to*

`http://www.simonsingh.net/The_Black_Chamber/vigenere_cracking_tool.html`

This is Simon Singh's Vigenere Cracking tool. It performs the Kasiski test to determine the length of the key word. Use it to determine the length of the keyword for the following text. Please write out a justification based on the evidence of the Kasiski test for your assumed keyword length.

DzfXnxzcjqljcurgwhkbwvlvrsolkfrbyfszvctuwvySrouuvvqvusvwhbvNticknqwuebwvyigkcmvjkccegkscibzbfrajiuxrdfyt nozyuPhznjvqcoiTdifjgksnyvurUcywvyjrgwzwrutlfzhowybwvyivqzuetxoavpxgnfzvohuydkmKuhfcmruUuibqbyjrsol rghgnyrJoocfifidgksUhhlhuevwvyDnubyraghbvFhwhvfhduinwsnyrptlfzwvySrouuvBiofcgksmvgksVvyjoyrehhbvouo pvfwpytnxgykuhmuiriilkuhgnweranyrfwpzylnukvrbuequszzahayegrtileSfimvqqyragayipkohkfosujgifyhhhbnclusmf ewhikuhaueqlajfewhbffhhbzajgqyvfvnvaghivsisgzadhykuhaceqdbxkuhmuirwvyerdfyjgwcnyrJsldnqgqybgkycyessfag hbvEkwhvjlhbnuranyrbolvprbnzaxofclzoazajkuisrfqyvfvlvnvchkuhVycihhcznogijhudujfwvyirvhiwgksArhogceidzii nvhbvlfchkrqrqzgkhbvThfgravwhrypcmkqdwfpodhncrvkbvawvyprlhbveusjvywvydsucgkuhwlfjqhyielhiivhgivgksgjr ojyjjduynnuchkuhwlwerbnzrugIersolkbihbvfhkbzpkwnynvpyvavocugkonkuhUulyvcwthsmnrxhgckfesazaqwhxnwh bveljyiEkchvvwwmsbxbxvqemnyruwpveJolfaqsnyrrqyradbxkuhhyielhiivhgiwgksVvyjoyzgeclurugnfbrbnyrvwxvbih bvFheoralohugksBvyysnzvxdiegkslzihfLyvqsueqvhlvgfvyjgrkuiqwvyebuhbKuhPyctdslzfhgzibphbvrahlvzhtlfawwyibi UulyhlnvaghikuhzinruduigrtnyruwpveUvcerdbxcbrynfjdfxkuhbiigkohugkslzflbajhqOklvwohznhlnvaggzibphbveljyi TdfieahhikuhDsirqoyrapcoegdwhjnqrnfgkongnuhiwgksitrdbqyvfvcjaholJcdwhzgocibfesnnrhbnyrvsnkvquiwgksmla dbxkuhbiigkgnre

Note that if you open this pdf in Acrobat or similar you can copy and paste the text directly to save yourself the transcription errors.

Task 5. *(counts as three tasks) Using the keyword length that you found in the previous task go to*

`http://www.cs.uri.edu/cryptography/classicalvigenerecryptdemo.htm`

and use the three steps given there to analyze the ciphertext further.

- *Why might the Friedman test estimate a significantly lower keyword length than the Kasiski test? That is, what general features of a plaintext might cause the index of coincidence to be unusually high? Step 2 might be helpful here.*
- *Step three gives the dot products of the letter frequencies for each of the cosets with all 26 letters and chooses a keyletter that gives the largest dot product. Are there other close contenders when making these choices? Might there be for other texts and what would you do if there was a tie?*
- *Using the tool at*

  `http://rumkin.com/tools/cipher/vigenere-keyed.php`

  decipher the message and pick your favorite tribe. Looking at the deciphered text, what peculiar features of this text made the index of coincidence so high and as a consequence made it the Friedman test guess too short of a keyword?