Project 3 (20 points)

INSTRUCTIONS: You may use any computer language or mathematical software for this project. Submit well-commented source code or computer algebra system code along with your output. Avoid submitting zipped files. **You should submit your files as separate unzipped files. Output file should be in a pdf file format.** Your program need not create pdf files directly. But in that case, you should convert them into pdf file and submit.

Project should be typed. Any handwritten files will not be graded.

Consider the ciphered text which is encrypted by using Vigenère Cipher:

```
XCIUIHTVOQVRLHJEYJXAVICEJFWXRVRUAAEPVPNEQLFZGFQEBXOIUXGIVJXVGLBRBXYIDB
FZVKCSGHNITYJBXTSWXZHWZAYSEPINIIZWBRMITIFMQJRKLKASRIMIJPICEMIGGEIINWUT
PZWVIFFEDRJXJXEHTISVNGOWRRVLIMZZGWLHZWZKFXHDRRASRXCEKKAOINYJIJLWJPVGGG
XMSCSNXVVGTIKLXJXYIAKHVXREKTVZWLPLEERIEJGKGZQVRLBWNSDILBQZWLRSUPZXFVWV
SQIIXZXGJRKIFMSAICIUMVJRZGUHQHYEMUTXDSEWXKSHXYILXGCRFPGZCKVFZAWIMIMIFB
RMIJTGGWZXFEUHYMXFVVXVJVUYDREPXYSJBDZHNEJKEIXZWKNIYFPEXXHZVRPBNHBIWSJX
BVQGPWFEICTSEFYIMTELBSIWJIJOMXIJRGPIIGICHMGZVKEAGGJQDYFBGVXZSFLFTHVJSN
POAZXZMLZOVCFXGZWJEJRXJHVGJRTOXYIUHQHYEMUTXDSEWKHPZPPMFMLZLRRVLSAXYIWG
HPWVVLAMNEGTDBINFFXZPLZRKLWWEOEZWAGQJXZSFHZZVVPWVXMSEMUGIOAFVCLSMEKVWL
XJRRRWEIXXISFBGYIMMUXMAXYIUHQHYEMUTXDSEWHKSQMUIJBWNIIZWWADXYEOTVMEEXKX
IFMEKLASNITSEFYIMTELBSIWKLWIVJZZHWKGVRESLIVJZZHWMLZHRXSUIXELWWBXCEJHWL
MBRVHLAIOITLFHPJKPWMVLOLRXAMGVRESLUIVGTIKLIYFPEFRXCMIHHTVOCNIVHRJXYENX
EICJMDOIMFLPDXXNEEHLAIYMJGMLWDSEWOBXCMEXZXISITYLBZZFIEFVLVVVWLBPGSEKGB
RBAYMDXXCIIIZTWISKCWMFZIEEVXGDWZSFPLZXYIJMSNIVODXKDWCELBSIAVQMLXRSIOOB
XCGFRYKINWZRVNWOVPEUTHZQZGKIVDZRGQZVJYGWSGHJXYIJLXJGIEXMEIEGTJHEXLKLSM
EYHIIKLINECPGYXCIDYDMMKPVGGFTZXZRYVSIGVVFLXCEKLSOIWIVRLAIASTYKHJNSDYUA
HZFRXWUYOAVGSGEGPRKJXIOLRXOXADPCRWXHJRXSAGKCSEIKMEIHZRXHVHIUTMUPDGUITT
XZESSMMLJASIKMXJTISLXGOPZFWKXTEEHKXGPVZXQBRWSKLGNVGENWSGHJYIXWVLISCSYR
```

Part 1: Suppose we made a guess by other methods that the key word length is 7. Calculate the index of coincidences for the above ciphered text by assuming $m = 4, 5, 6, 7, 8$ and verify that the index of coincidences method supports our guess that $m = 7$. You may manually type the reason why your calculations below support our guess.

- Step(1): $m = 4$, Split the cipher text into four substrings y_1, y_2, y_3, y_4 as explained in the class, and calculate the index of coincidence for each substring. You will have to get four numbers here.
- Step(2): $m = 5$, Split the cipher text into five substrings y_1, y_2, y_3, y_4, y_5 as explained in the class, and calculate the index of coincidence for each substring. You will have to get five numbers here.
- Step(3): $m = 6$, Split the cipher text into six substrings $y_1, y_2, y_3, y_4, y_5, y_6$ as explained in the class, and calculate the index of coincidence for each substring. You will have to get six numbers here.
- Step(4): $m = 7$, Split the cipher text into seven substrings $y_1, y_2, y_3, y_4, y_5, y_6, y_7$ as explained in the class, and calculate the index of coincidence for each substring. You will have to get seven numbers here.
- Step(5): $m = 8$, Split the cipher text into eight substrings $y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8$ as explained in the class, and calculate the index of coincidence for each substring. You will have to get eight numbers here.
- Step(6): From your output, verify that $m = 7$ is the correct guess.

Part 2: Create a table with 7 columns (one for each substring $y_1, y_2, y_3, y_4, y_5, y_6, y_7$ as given in slide 26 of sec2.4.pdf in class notes. By using the table, find the keyword. If your keyword is correct, it should lead you to a meaningful plaintext. You should explicitly state your keyword.

Part 3: By using your keyword, decrypt the given cipher text. You should include spaces between words and insert period (.) at the end of each sentence and capitalize the first letter of each sentence so that the grader should be able to read your plaintext easily. Otherwise, points will be reduced. Your plaintext should typed and neatly formatted to receive full credit.