Math 495R Homework 10

In this lab you will write a program to crack the Vigenère Cipher that you programmed in Lab 8. For background, read the material available in Learning Suite on the Content page. You will need the programs you wrote in the previous 2 labs.

(1) Write a function that takes a string S and an integer K, and returns an array of K strings $S_0, S_1, \ldots S_{K-1}$ where S_i contains the letters of S at positions $j \equiv i \pmod{K}$ (So S_1 contains the letter at positions $1, K+1, 2K+1$, etc).

(2) Write a function that takes a string S of capital letters, and returns an array of length 26 whose entries count the number of occurrences of each letter in the string (so the first entry is the number of As, the second is the number of Bs, etc.)

(3) Write a function that takes a Vigenère cipher text and returns the most likely key and the translated message using that key. Test your function on the cipher text on the next page. Additional cipher texts can be found at `https://math.byu.edu/~doud/Vigenere/`.

The process for cracking the Vigenère cipher is as follows.

- The most likely key length K is the distance with the most coincidences in the cipher text. (See Lab 9 problem 1 and Sections 2.3.1-2 in the background material.) Calculate this value using the function built in problem 1 of lab 9.
- Use the function from problem 1 of this lab to split the text into strings $S_0, S_1, \ldots, S_K$. Assuming K is the key length, the letters of each one of these strings should have been encrypted using the same letter from the key.
- For each $0 \leq i \leq K$, use the function from problem 2 of this lab to calculate the vector W_i which contains the occurrences of each letter in the string S_i.
- Use the function built in problem 3 of Lab 9 to find the value k_i which gives the maximum dot-product $W_i \cdot A_{k_i}$, where the A_j are the arrays used in that problem. The table for A gives the frequencies of each letter in standard written English. The most likely i-th letter of the key is the letter corresponding to k_i (See Section 2.3.3 in the background material). For instance, if $W_3 \cdot A_j$ achieves its maximum at $j = 0$, then the third letter of the key is most likely A.
- Once the most likely key is determined, the original text should be decrypted using this key and the function written in Lab 8.

Cipher text:

```
XUKBVQIGXIIIPYKZSSVFUQGAMYRJRGSABMAMIAZBBWTRGSBJLVSENWIKVWHRHVTONVIPUVQMXRSIG
XIEZWHWLVYOEICREMFWLBTMNRHGCQAOPRJIAHLVYCFYEYRGCEPRLIPIANYNYYWUKLNRHNTQZEXRJB
UIJVXMOYVAKLOVMTNBYCEAJBUIWBLBEEHVGVPISSZPRMRPGVQIWPKVGPMTNBFMRGNMYMPVKABJWVR
DRVGNAOUXXUKJHFFYKAGLEGLTNWLRJIAHTNYARHMAUCEKPNYARWSHXKUEMEYJRMRTNQFTEGKVGWIZ
HZNGIQGVQGEEKAFIHHYZNXLRXBUERFAJZMXGKLGSFRYIGYTBTIAHXUKZRAEFZPNXPHDCEMSHYISXI
EJQARIEGBZSWCNMEIAUKVGLSHMPGVSNSATVEPKNHPPLLZRISSZPRXVNSURPWBLXEIGVYQBREAJPRT
YGOBGSYFOVGLMFCILQEEQQAKXUKXBMRGYEVXLNRMNRJBXMSMRTKZNWARYIGERQRIMMPLGLZMVRJPV
WINXVRWXAKAFSZRXBUMWAKECEVNJWKEWJKBUSYTNBVXEAJPVWJRICAHMGEGBYQHYBSSPYUEZIGNXM
```

SYPYEQFLEYRPNZIGUKBRXEUDRVXBTMBVXJUQQIEFZPNXEEKIYQSFZCAMZRXANPPLGKPITGKLGLITK
WZIXEENBVMAYBNRGRZPRCXNAOUXCBAIGWGUUWYMWSUCAHIQUVNQMFIWAGICZQBRMFTWGXLNZZNXLR
XIYEVTKBUMRTZWRBTRIBHWXBHMTMRHVWAWEVJNVPFLGVNVKHSMAXEGODRTIEYWAAMGNZRHLNOZVHS
AUBZIEAZWNWOLUCGSEPIMCXEAEBUMRTCQGLSHZZREWBTIOPITXWHRHSUZVXCBAEVPPFUWAEHZOBNW
QHIPNWMAKMQJVBSGBYCBASASABLKBYVFKBUEXNSIGLIZGBVGEYRQAIEYOVRSJGNQPORRYAAMPUGAA
SVRGTRBMFZMAGIGNMLXEHMPGCSHZPNXRROBUIVUGANQEGNMZEXVIIYTPNTMGLIFKBUMRTYIEIQRXM
NFWGXIPXMBTAGLEGOANPPEOOUXWNOLGLICYGPLSYUOVWXAUZUEZVTOBRPLRMAKXUHZREHGNIAHXUO
KXRIFYKNREPAJRLEIKIEIEYKFVWXRTKRXLRXMVSFWKKGWEVJNVPFLUNPSYEYMNWSYOLOSHLSILIBV
YBNPPEKIYXLVTOFWSZUAGTIBVTRXLVTSOYXJGQGEQBSMAXGNTIAMRFZIAXEAKWHWGHHMRBMFZLBRX
SUTYSALUCFEMQLQYFCPGVNGYOKBUEXQUMFRSGRIFXJBXIACXVSMNXEYRPNZINXMNPIKOAGIRPKNVP
FLHMPEQRVMAWMIKKYIEERGGLIGOURXVNBMYPIEVZBGIRJMQERLXMNPFBJGZYWGNIIIIKZMAWMBTQA
JSHXLVVIPZQBRWVZUHWXUGDRPIAMBUFVRGLGLXUOKXRIFYIAHHHXIGMSAHCGXLEUCTLEAGBHVEYOV
SMVZOBLSJGNMSPIFNEUMGUOEVPPRDXYEMAZWLSYVTIZSQRTBJIMAITVRIGUWIIVYUWXXLVYNNGXGN
MEIEEKZREPYENBYVQOURRWVUVFXLEKMJLMPNERGEYRBUIXUXMRTPNTMFSJFVIPIEAJISSYEZPGMQR
ZPRVIVYPBAIIKZNXIAJMAGCGULEEANTCAVINRLVWXVTKGMSAHMGAIRTBUIJBXURVXUXMRHMZKVFMS
AYIAHXUKTNXXRXJRGEHYMVXLNVXRRWGNIGSYEIWAWGVUCFRIFYUBZIFOVGIVZOBGIRGRGVRSAKLVV
IPZQBREYUVTXLRRIGXIELZBQXUKJRKMATQAKXBZPRIRQUNBYVYODRWXUGBFEMQGDRVCLUCAKQNTUN
OMAMACEWZULVGISLWEXWGUZRPMTNBUMWPOONVSIKZGLIYGUCXLNZDRVCPRMNVMAJMRHRBCQGMWIKZ
LVIZGZXEFYKBUEXGNQFMWFUMKXIAYQIIPLUDRVPBUSRHGBTBVRYRJBUIXVSMGVEIKTYIVJOBUEWYO
OUXEPIMFWMBTWSGLRKZSYPAKAFVINRTLXLVYQFALNZQFQINTBOCXUKNBYVGNLVQIAYQBRXUUCTLWB
SMCISCRMJLSGGTXEFBABGLISUCEXLQOURRWVUVQSRBZSASAGNMLQINTQGMXVYWAPCNTWGLIECILSJ
YUWXMRTGBGMQRZPRVIVYVBHMSLMEIRPKJRXARKVGMQRGVQERLUNGLIGNZRIHVSMAWMBTABJWCGKRI
BPKXGXLNZWHVGBTAPMSHYVRWWZUDRWEYUVTMXOABFSQRLWBPMFNXRSTYKPNZITUBUSPQUNGLIJXWA
KWVJMBJXUGBVHINEWHLEIKIYPLRGZQALNZBUICUGDRXSFGGNFSHZBUMWSUCEXLQOURRWVUVVLEIKV
BXWNOLGLICXWIMRPOIYQELUZVXMFYQZTPLZPVWXUGBFTEPKIFSYESIGLIZGBVGMNTAUEZROBVWWCU
SRRSSGAUEZVTOGLVRKLVQIAYQBRWJNQPLSAKUNCGNRTYIRTZPOVINJBUERQZPVGOAKAFERQOANPAN
EAQIJVTIOPIOEZRJIEKVPIXBZPEIICRIAIWRGKUEXEOOUXEAMTRWXBZPRSXUKZFFYGYWZITUOTBWS
CNQPEPCKWCPIUGDRFIRTIFOMAMEUCXUXMRHMZKVFMSAYXNVXVICYEVYEEUCRBZIASXUKZQMVRIBVS
RNZZVKLGGVTPIFZWGLIBZPRVXUXMRERQNIIIIIKVGVMRJBBGSAYBEYGGGNBYVQOURRWVUVTISZKBE
CTEUNRWWBXAVQSATMJGSZHENWIKVWHRHVTOGLMFZWGLIAKELSVXSIGLIZGBVGEYYWPMIGEWAPCNSW
AXLBXABEKBEWHORBCPBASAGNYEXFAZSEGRCPVGLUGABRPLZEBHMZKVFMSAYERGEAXMCVIFKVGEJVM
CEISSGBUVIRJQZIRFOWAEPFUTVHEAJAVQMYGZYCXUKGGLMAQBUEXOEUBHIYYWSXLEKMQMQRTAVSRF
ZPRCGBATQVICXMFIRGUVRSJSUCEMJGNMLGSHRLZEWGKZGLICKZFTIPZQIISSZPRXLVTOFIIVZPVRO
FUUHVQHXMQXLRVZBZMAIQNPQNEWEERQQVVXXVTOUMWOXWJWLRRICWIQOVGSEAOVGVSFVMPXMIKAGE
XRNQFPMCYUBZMAMIFSRRCPBVICKIGWQLYBVGABXLFCIFOBUMRXOARIMGTWJLIFGQQEJGKZFSQRZQZ
IFEOOUXIAOVTMRNWCVXIGXIAWMGUZLQEATMEAIYRQQSRBZUVRHGKTYMRTEWHMLNBMOIIAGBJSVXAX
BRXUOATISZKBECSSLWHVHVSMAWMBTASSVFUURXMZKABQIBLULVIFATGWEEKKHVMBAASSVVTAGERPK
PRVIVYICSVGXIVXSSGUNREGKQTLXLKIEWSYJIASXUKZNXJVLBRIRNTWGLIEGBFIZRTBRIRNTWGLIE
GBGAIAZGGLVRKIAHWBUVNPPGNMFIEEKMIMHRTBYCWRIBVSRFGAVXARXMGLVRKLVQIAYQBREYXMCVI
FKVGEXVUVFSJUOASSYEJQZIRFOWAIHOKQAKAUOKUMWNLQKIHNTLHREYZMEEFYKBUMRTYKVIRGONVG
TRUXYITEUKRIHRJBUIXVSMGVEIKTYIVNLBRVXUKXNYWRXMDYMEKLSSVGNMCVSCKZNWWVSQYEXVUVB
JXUOAXRSJBMECARRTGLEGZQZIMFUVYCEXOVQSJFVIPILRXMVWECUXHPEEYKVIRGONVGHVGOEEQNCM
NXLRXZRGSEJBUMWYOVRMXEGKRAMGNULJMAMMEWLBCAGLIZUDRQIAZWSXLRHIESQRZMECIFZMEHELO
BJEWFUPVKLLKAGIVQGGAMKUZQGJIYRBUIRGNQFQSETQAKMGXWFIETGQAERQYWTIRGRGHTANXLGSLR
XMFYVRRGGLIZKZPYVLJQQRSGZZNGIGNQFPMAKQAERLUNGLIQOURRWVUVFSJFVIPIKRTMEEPYEZRGS
TTQMIHOABPIVGGQAPCVZBEEGRJAHGLNRQAIEAJBUEXYOVRXLRXMSSVRCMZYWGIWAGPHJMJEWNRWAK

XUKBVQIQOURRWVUV