Homework 7: Cryptography

Homework Problems.

There are two texts here. Pick one and decode it. The first is encoded with a simple substitution cipher; the second with a Vigenere cipher with relatively small keyphrase. A tool to count characters can be found here: https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html. Frequency tables can be found here: www.cryptograms.org/letter-frequencies.php. www.onelook.com is great for filling in words where you know some but not all of the characters. http://cobalt.rocky.edu/ ulrich.hoensch/CryptoApplets/main.html has some nice applets to run Kasiski tests for you.

1 Substitution Cipher: encrypted text

Va vh j sltt-xrosr lhajutvhglb ijma agyocngoca agl fjrd-bvflrhvorjt soytbh oi agl fctavklyhl agja foha yljttd nylja bvhmoklyvlh jyl oslb ao orl uyvli foflra oi vrhwvyjavor. Tglyl'h j toa oi hwjblsoyx ivyha, oi mocyhl, uca sgja mtvrmglh agl sgotl agvrn vh agl hvnga oi, hjd, j ijttvrn jwwtl oy j uovtvrn xlaatl oy agl sjaly htvwwvrn okly agl lbnl oi agl ujag. Hoflagvrn nolh mtvmx vrhvbl agl ouhlykly'h gljb jrb aglr lklydagvrn ijtth vrao wtjml. Agl hgjwl oi BRJ, va vh wowctjytd hjvb, oslh vah bvhmoklyd ao agl mgjrml hvnga oi j hwvyjt hajvymjhl sglr agl hmvlravha'h fvrb sjh echa ja agl yvnga ylmlwavkl alfwlyjacyl. Gjb gl chlb agl ltlkjaoy, agl sgotl hmvlrml oi nlrlavmh fvnga gjkl ullr j noob bljt bviilylra.

Agvh vh agocnga oi jh hoflgos sorblyict. Va vhr'a. va vh ayjnvm. Tvaatl wjyavmtlh oi vrhwvyjavor htlla agyocng agl crvklyhl jtt agl avfl ayjkltttvrn agyocng agl blrhlha fjaaly vr agl hjfl sjd agja j rlcayvro wjhhlh agyocng j mjrbditohh gjdhajmx, jrb foha oi aglf fvhh.

Lklr soyhl, foha oi agl orlh agja gva agl lpjma mlyluyjt ajynla, gva agl syorn orl.

Ioy lpjfwtl, agl slvyb byljf juoca j tljb bocngrca or j fvtl-gvng njrayd, sgvmg vr agl yvnga fvrb soctb gjkl ullr agl mjajtdha ioy agl vrklravor oi ylwylhhlbnyjkvajavorjt ltlmayvmvad nlrlyjavor (j mgljw jrb vrlpgjchavutl jrb aoajttd ror-wottcavrn soyf oi wosly sgvmg agl soytb vr zclhavor gjb ullr hllxvrn ioy mlracyvlh, jrb ioy agl tjmx oi sgvmg va sjh wtcrnlb vrao j alyyvutl jrb woirratlhh sjy) sjh vr ijma gjb ud j hfjtt jrb ulsvtblylb bcmx.

Ud jroagly hayoxl oi ujb tcmx, agl hvnga oi j glyb oi svtb goyhlh njttowvrn agyocng j ivltb oi svtb gdjmvragh hoctb gjkl tlb j haycnntvrn mofwohly ao syval agl ijfoch Itbvan Nob Hcval, uyvrnvrn hcmmoy jrb ujtf ao agl hocth oi fvttvorh, gjb gl roa ullr ja gofl vr ulb svag hgvrntlh. Agl vrhwvyjavor aglylud iltt ao j rljyud iyon, sgo sjh roa vr fcmg oi j wohvavor ao fjxl j hajyatvrn morayvucavor ao agl ivltb oi aorl woladf.

Fjrd mvkvtvqjavorh gjkl ylmonrvqlb agvh hgomxvrn sjhal jrb ayvlb kjyvoch flagobh ao wylklra va, foha oi aglf vrkotkvrn lrodjutl uca vttlnjt jaalfwah ao aycl agl fvrb vrao agl yvnga sjklrlrnag ud agl chl oi lpoavm glyujtd oy dljha wyobcmah. Va rlkly soyxh wyowlytd.

2 Vigenère Cipher: encrypted text

Dorukfu ukjqh widu jpw grsjpwuho zbv ukf ibfu widu dhdjqtw bom ssrcdclmlub b vqhsp xkbof kbg txegfqmb chfq ddmofg jqur fajvuhoff vfyfubo nlmht dcrwh ukf vvugddh pi bq bojho smdohu.

Dog tloff wilt lt qpw b qbwvubomb uhodcof spvjwjro ipu b zidmh, ukjv qrpu jqordhow dufduxsh ide yfuz ojwuof wjpf wp fppf wp wfunv xluk jwt lehowjwz dt d xkbof efipuf lu wiho kbg ur drnh ur uhspt zjwi qpw chjqh d xkbof dob nrsh.

Ukjv jv b fppqofwf uffpue rg luv ukpxhkuv gupp ukf pppfqu lu efjbq jwt ojif wjom wih nrnhow jw fqehe lu.

Di ! Ziduv idqsfqjqh? lu wirvjiw.

Fu, fadxth nh, xkp dn L?

Ihmop?

Zib bp J kfuf? Ziduv nb qxsspvf lo ojif?

Zidu gp L nhbq cb xkp dn L?

Ddmp erxq, hhu d hujs orx ri! wilt lt do lowfufvuloj thovbwjro, zidu lt lu? Luv b vpuu rg bbzoloj, ulojmloj thovbwjro lo pz pz zfom L txqspvf Le efwuhs vudsw glogjqh qbpfv grs wilojt lg L xdow ur ndlh bqz kfdezbb jq xkbw grs wih tdlh pi xkbw J vidmo ddmo bq buhxnhow J vidmo ddmo ukf zpumg, tr mhuv ddmo jw nb twppbfi.

Jpre. Rprpk, jwt jfwuloj rxjwf vuupqh. Dog ihz, ziduv bepxu wilt ziltwmloj srbujqh vpxog hrjqh sbvu zidu Ln vvgehooz jploj ur ddmo nb ihbg? Qhskbst L ddo fbom widu zjqe! Lt widu d hrpg odnh? Jwmo er qhskbst L ddo ijqe d chuwfu odnh grs lu obwfu xkfq Jyf ipxog pxu zidu luv grs. Lu pvvu ef vppfwiloj whsb jpqrswbqu effbxth ukfuf ffuudjqmb thfpt wp ef d ihmo pi b opw pi jw. Ihz! Ziduv ukjv ukjqh? Wilt ofwt fbom lu d udjo zhbk, udjo. Ihz! L ddo fbq shbomb uksdtk jw bepxu sshuwz jpre fbqu L? Xrx! Zpz! Ukbw ghfot jshbw! Erfvow thfp ur bfilfyf yfuz pvfi evw Jom ssrcdcoz ijqe rvw xkbw jwt ipu mduhs ro. Qpz idwh J evlmw vs bqz fpkfufqu sjfuxsh pi ukjqhv zhu?

Qp.

Qfyfu nlog, ihz, wilt lt ufdmoz hyfjwjqh, vp pvfi wp ijqe rvw bepxu, vp pvfi wp oprl ipuxdsg ur, Jp rxjwf gjcab xluk bquldlqdulpq

Pu jv jw ukf zjqe?

Wihsh shbomb jv b opw pi ukbw orx ltqu lu?

Dog xrx! Kfb! Xkbwt wilt wiloj txegfqmb drnloj urxdsgt pf yfuz ibvu? Yfuz yfuz ibvu. Vp ejj bqe imdu dog srvqe, lu qfhev b ejj xleh trvqeloj odnh mllh pz pxog srvqe jsrvqe! Widuv jw! Ukbwt d hrpg odnh hupxog!

J zpqehs lg lu zjom ef islfqev xluk nh?

Bqe wih shtw, biuhs d txegfq xhu wixe, zbv tlmhoff.

Fvujrvvmb fqpxhk, ukf rooz wiloj ukbw xhow uksrvji wih nlog pi ukf epzm rg sfwvqjdt dt lu ifom zbv Pk or, oru dhdjq. Ndob qhpsmh idwh tsffvobwfg ukbw ji xh lqfz fabfuoz zib ukf epzm rg sfwvqjdt kbg ukpxhku widu zf zpxmg lqpz b opw nrsh bepxu wih oduxsh pi ukf xolwhsvf wido zf gp qpz.