Math 7H | Professor: Padraic Bartlett

Homework 3: Cryptography

Due Tuesday, week 4 | *UCSB 2015*

Homework Problems.

There are two problems here: one piece of text encoded with a **substitution cipher**,and another with a **Vigenère** cipher. Try to solve them! Write down your observations and methods as you break the codes. You don't need to translate the entirety of either text; you can just translate some of it until you recognize the base text, and then you can tell me what it is.

Here are some tools that you may find useful:

- https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html.
  This counts characters and will create a frequency table for you.
- www.cryptograms.org/letter-frequencies.php.
  This link contains a number of useful frequency tables.
- The website www.onelook.com is great for filling in words where you know some but not all of the characters.
- http://math.ucsb.edu/ padraic/ucsb_2014_15/math_honors_s2015/math_honors_s2015_hw3.txt.
  This is a link to a plaintext version of this HW, which will make copy-pasting easier.
- http://cobalt.rocky.edu/ ulrich.hoensch/CryptoApplets/Java/KasiskiTest.html.
  This is a link to an applet that will run Kasiski tests for you.

Text Sample 1

Bo. mca Ygp. Pjoeabk, dc zjjnto rdrd, Eoukbf Soukb, itoq eoaja fd pmn qtpq fwbk lbdt mqgcqrqxn kagjma, qtpkw nlg kbdn jgre. Fwbk lbdt qtt imhq btlbab kdr'p tubtzf il nt fzklxkbp xk mcvfwfzv pfgxzvb ag jkhqqgfajp, ntzmjpq ieqn gghq pxaz'i eaaa ixqt hrow kacpqcpq.

Bo. Pjoeabk lxe ieq sfdtzfdo au x rxoy rxxabp Vogckucde, leure ypaq souaie. Wb ipp m qfs, qbquv ypk ixqt wxdsik pkk cboz, xxieajdt wb pxa tpsq p sqgv xpost jghqmreq. Boe. Srdhiqn tmh qtxk mca nalzsb mca tpa ztxdav flfot qtt rejxx pjajkf dc ztzw, leure opjq xk htok jpqurx pp ewb eebzi pa brow lr wbd ifyt zdpkucd akbd vxdsbz ubzrbe, hmkxks dk fwb ztfswyagp. Fwb Pjoeabkh ems x ebxxa pac zmaiqs Agsiqn xzs fz ieqxo aefzxlz ieqgb ipp zd cucbd qlk pkkleqgb.

Fwb Pjoeabkh ems bhtokieucd fwbk lxzibp, qrf ieqn xxhl tpa m hbogbf, pkp ieqxo sgbmibei cqpo ipp fwxf hlytyasv idrxs auhzakbd xq. Fwbk sfpc'q fwfzz qttv odrxs yqpo ui fr pkkdkq ulgca ajq mqlgi qtt Maiqqgp. Ygp. Bdqfto ipp Ygp. Pjoeabk'h puhqqg, ygi qttv tpaz'i jqi cag pqkbdpi ktxdh; fz uxoi, Jdh. Aggpxtv bgbftkpta ewb pxaz'i emkb m hfeibd, qbopret eqg puhqqg xzs eqg dada-rdo-zdqtxks wreqxzs tqgb mh rzSrdhiqnfew xe xq ipp bdpexyxt qa qb. Fwb Pjoeabkh ptjaptoqs qa ieuch iwxf ieq cbuvendoe llgaa epv uu qtt Maiqqgp mgoukbp xk fwb eioqtq. Fwb Pjoeabkh hztt fwxf ieq Elfibdh ems x ebxxa pac, qad, ygi qttv tpa ztsqg bhtk etbz wfy. Ieuh yan tmh xzdqtto sdlp gbmhlz uld zbqefzv qtt Maiqqgp mlxk; ieqn ausk'f lxzi Agsiqn jumfzv tuie m reuaa xxhq iemi.

Text Sample 2

Stz xl ug zitf, ngx qfr O,
Vitf zit tctfofu ol lhktqr gxz quqoflz zit lan
Soat q hqzotfz tzitkomtr xhgf q zqwst;
Stz xl ug, zikgxui etkzqof iqsy-rtltkztr lzkttzl,
Zit dxzztkofu ktzktqzl
Gy ktlzstll fouizl of gft-fouiz eitqh igztsl
Qfr lqvrxlz ktlzqxkqfzl vozi gnlztk-litssl:
Lzkttzl ziqz ygssgv soat q ztrogxl qkuxdtfz
Gy oflorogxl ofztfz
Zg stqr ngx zg qf gctkvitsdofu jxtlzogf...
Gi, rg fgz qla, Viqz ol oz?
Stz xl ug qfr dqat gxk coloz.

Of zit kggd zit vgdtf egdt qfr ug
Zqsaofu gy Doeitsqfutsg.

Zit ntssgv ygu ziqz kxwl ozl wqea xhgf zit vofrgv-hqftl,
Zit ntssgv ldgat ziqz kxwl ozl dxmmst gf zit vofrgv-hqftl
Soeatr ozl zgfuxt ofzg zit egkftkl gy zit tctfofu,
Sofutktr xhgf zit hggsl ziqz lzqfr of rkqofl,
Stz yqss xhgf ozl wqea zit lggz ziqz yqssl ykgd eiodftnl,
Lsohhtr wn zit ztkkqet, dqrt q lxrrtf stqh,
Qfr lttofu ziqz oz vql q lgyz Gezgwtk fouiz,
Exkstr gfet qwgxz zit igxlt, qfr ytss qlstth.