MATH 3375 (Theory of Cryptology) – Fall 2013

Homework Assignment 5

Due: October 17

For both questions below, you are allowed to use any web tools you can find. However, you need to let me know which website you used.

1. Section 2.5 Exercise 9 (except 9b) (on Message 2)
2. Answer the questions of Section 2.5, Exercise 9 for the following message. What book does this come from? [**NOTE:** The text below includes the proper spacing and the punctation. You do not need to decrypt the entire passage, but just the first paragraph. I have given you a lot of extra text to help you with the analysis.]

```
Shfdxe dok wkhr: lh hluag cphz.  Mnlfw by uc vhaih oagasnxx hpgnz avsm.  Zos jxmpglxx
vt zby iijbgs ksl ypufxj im lak jzwkmfasg, zos uekyy, lak bbvxxaocxx, hbv mnl qzbkm
agnxusj.  Liycgzk zwygkk wl: ttk Gukuvuw'l thaw pgz ughj bdgg 'Ioofzk, mcj ttfhzbtn vw
vnvgw mu wil aoz vsgj ac.  Gej Tojekf ksl gz rwtj hg s wuvf-ftos.

Aagj!  P rgg'z tssg zv gsr zool B quco, hl tm gpt rbgprlryx, cool mnlfw by wojmojidtxsm
vxgk othaa o vhuy-bsbr.  P aazna vsok iswg ouqdbtlr, erylzx, mu ysytxk o uhlmwf-ggpz sl
zos vxgkskm vpsux um wjhttcfzkym ag zos lkgks.  Tnz avw pozrgf um cmk guqwlzvfk by pb lak
 zwebrl; ofw sf ifagszgpkk vsgjz gztrs bgm jpglnxi wl, hx avw Vubblke'z rggk mcj.  Rub
 kaer avwkkmcjx vlfebz ts lh xldwtz, lahagawutrsm, laga Askrlm oty hg vxgk ok t jvcj-ggpz.

Kvxvcyx quso ak dok wkhr?  Gy ivijlk os vbj. Oco vubzv bz is gmnlfobyl?  Gukuvuw ttk vw
pkys htxabwky mcj B jvb'l dtvk zhc tofr elojl.  Yjfghml ksl npg khrl spxibhgk, npg khrl
ovfouwkmxhhgk, npg khrl oklonb, zby zcdx xlgawahfq eknolxk, owk luss xkolbv ttk ggek
tcmktlf.  Sgj ljwg Yjfghml ksl tvh kh jysswlbzdr ibh mi hf hzx yhr wokuh, tnz avsm nl ksl
 gu spvkszwgz tof hl iikbtlgk ht avw okym vte vt lak mifxxhz, sgj zcdxsuwkxj ph obzo of
ntkcmuzlr ttxnoag.

Zos extawgg um Askrlm'k yausjtr ifagmz aw ugjy lh zos hhouh A lzhflxj mfgf.  Zosjx
oz bg wubpl mnhh Etxssq pgz rwtj.  Aval sbgl uk kwkmouqlee bbvxxzhghj, vf fhzowfz
cvbvxxmid vgu qgfk vt lak zhgke P oe zupby mu ysdtzl.  Wx pk dsjx tvh hxxmsumrf
qggbpbuxj avsm Nhadxz'z Tsmnlf vbkk pwyuys lak wzsr hlusg, zosjx cvidw hl bgmnpby
fuys jxshfcthss ag npg ltqpby t yafger hh fbmoh, ag gu sslzlfdr cpbv, nvvb zby vkf
kgtdskzz, hztt avwkk dcmej is ag gum gmnlf ebjkzw-tmlr yxtazwfgu fslnsm lnxuwfz ubh
syzlf vtxr wf t hyswse zdgm -- yhm Ktouh Htas'g Uaayqzrgyr xhx pbkmguqw -- eoasjtrsm
lh gzhggozv zby zcf'l cloc four.

Kvxvcyx tljwk vhwfmkk cmm Usr Etxssq'l thaw. Mnlfw bz zhghj, fssky htlxxdojwy, hpgok
avw pgyszhazs vhuy: Gukuvuw ttk Askrlm.  Lak mwjf chg cgudb sl Yjfghml ofw Shfdxe.
Zcexzpawl vlchek uso mu avw uazwfxyz qserlr Kvxvcyx Yjfghml, ofw yvawmotsk Fgyzwr,
hbh zx gugoxxlr lh hvhz ggtsk: bz dok trs hzx yhaw mu owe.

Hn!  Iil ak dok t zpuzm-lpglxj oofw ga hzx mywfw- yacfx, Yjfghml! o kjalsrbtn, kjxtjvagm,
```

nfslvpby, liyohbtn, qdnzjvagm, jcnxzvik, hrk gagtlf! Ztxk ofw yooji gz tdbta, tjhs dvavn uc kmklz ztj ljwk yafmvq vil zkusjhaz takk; zsukka, ofw ylzx-vuuhsbtlr, sgj zcdbzhfq ty hb gryasj. Mnl qgej dwlaou vaf lycrx npg gej mssmaysk, gowdww npg hhouhww tvgw, lnywnxrlr zby jvwxq, zhayllbww npg ytoa; aswk owk xelg jxj, owk mnpb dbvz pdnk hbv lvvyw haa gzkkdrdr ou val myolbtn jgbil. O xkuzhq kots oty vb zby ossw, gur gg npg wrkifgpy, hbv aoz kake jvag. Nl qskxpsv aoz cog rvk lxswsjtzbfw trdoql gicmm cphz aot; vw bilr zby vtxbil wf mnl rgzjhmk; ttk rawt'a hztc ph ggk ksykkl ol Vnywkmshg.

Wqzlfftr ossm gur uhrk vsw rphlek pbxealbux uu Gukuvuw. Gu dojfzo qgnrk ksks, uc obtafq pkhhzxx jvaer owe. Gu dwfw zool urlk oty iwlmkysj mnhb zx, tv tserpby ltvk oty tcjx ouhwgz bdgg oag hnxwckx, tv dwezpby kgpb dxyz chxt ac wgzyssme. Mcme clolaky rawt'a yfhc dvwkk ac ztbl vaf. Zos zxgcwwlz yoag, gur kgud, ofw nhwd, ttk gdxka, qgnrk pgtya cx mnl ovoguhszk vjwk npa ag uuzq htl fwlvlql. Mnlm gyzlb "utsl rgpt" oofwyvawee, hbv Liycgzk usnxx kwv.

Guicvr kcsj lzvdhxj owe bt avw lzyswm zv gsr, cphz zrhrkhsl zghqz, "Aq wkhf Kvxvcyx, nvk skk fcm? Pnlb obrs mgn ivaw mu zsw fk?" Uc txmnojl otddhxlr zbs ac txyaco t zywxek, uc uaosrjxt hgcxj owe pnhh am chg g'vrvqc, gu tof hx dcett ljwk uuqw bt hzd aoz zayk pbinoysv mnl ksr zv gmvn hbv lajv s irhqw, hl Zqjhuns. Woku hzx hswfw slb'k wung sivlojxj ac cgud vaf; gur oaku hzxe zoo aot qgfouu gg, cvidw zbu lakpf gptlfk btac vhuyksry hbv nv jcmkzz; ofw zosf pubzv pgn hzxoy hsbrz ok mnviya zosq lgpr, "Fh kfs sm gsz al hlhlxx avsg gu snbr lmw, wgyy etyasj!"

Uaa kztz kwv Liycgzk jojx? Oa ksl zos nxxf hzbtn vw eorsv. Mu lryx npg ote hzggm avw vxvkvxj wolay vt dbll, ksktpby trs vmfgu gqfvhhzr zv ywxv phk wozhsgil, ksl cool mnl yfhcpby htlg utrs "bmmy" ac Kvxvcyx.

Uuqw nvvb s mots -- gy gsz lak ncgw jhmk bt avw rkhf, gg Iofalztok Xbl -- cdw Yjfghml gsm hbgq bt owk vubblbtn-vgnyl. Wl pgz qgej, izwtq, iwlbtn kwtzosj: yunuq poavse: gur zx ividw nloj mnl dwhvss ag zos uhayh gnzzwvx mv kzxkgwfz aw ofw jvkf, ukhhagm avwbx oofwy bdgg zosak hysslzz, ofw yaoeiouu lakpf xxka ihht avw igcsexta glhtlg lh chfe mnla. Lak jwlr iscudy oov htsm bnya uggk avjxk, iil bz dok japhw wgyy sexlovr -- oa vsw tvh txku zazna ode jhm: sgj jofwrlg oxxl tdtxpby bt avw pourgpy vt lak usaznicmkouu gylpqwl, rpyw kakrq lslojl awcf mnl dsevhpdx hycog gpf. Lak mcy vgts hhaywfz ou ol xblfq vnpbc ttk ywrnvzw, ttk ksl yv rwgyl kamnvil, mnhh sezocmzn avw vubfl pgz cx mnl bskxvkwlz, avw aubgwl uwdgloas oxxl awkk wvsgzvak. Mu zsw mnl ragmf qdhak qgfk kfghvpby wudb, guyjijbtn snxxfhzbtn, cfx spuzm nhjw mnviyaz avsm Thhmkk swnxj oojw hf, ofw chg tkkdwfz uu o dtxns kvgss.

Lak kcgk um Gukuvuw'l ivifmouu-zhazs oty vdwg zool ak twyaz rswi npg wrk bdgg npg uekyy, oau pb s wozase rphlek jsde hlmggj, h ggkz vt lttr, ksl ivdqbtn zwmzlfk. Liycgzk oov t blfq lshzd yoys, tnz avw vrlfc'l lpfw pgz gg okym enio getrssj mnhh am rvccxj swcx uus uhgs. Pmm nl qgnrkb'l kkwzwgozv am, lvf Kvxvcyx qldl mnl qgtr-icp bt owk hcu fghs; hbv lu zijxrf ok mnl qdxxr qsfk pb obzo hzx yocnxr, avw fgzhwk vysvbiasv mnhh am cvidw hl bwvkzgske mcj mnla lh vhfl. Pnlfwyuys lak jzwkq wil ht owk pnphw vuttgkzlf, sgj afaxj ac otxt vafylzx tz avw vgurdx; ou kzbio sxyuyh, fhz isagm h asg um o kmxvby bshuaggawgg, nl tsbrlr.

"S fkyfq Vnywkmshg, mgiss! Yhj zonx evi!" ukolr s vnlsjyas jgbil. Wl pgz hzx bvwux um Gukuvuw'l tldzxc, dvg vgts miuu vaf yv embirzq mnhh laoz ksl zos xbxzh agzpasmovb zx nhr gy npg sivycsvn.

"Ioz!" lgpr Kvxvcyx, "Nbatnm!"