

HW # 1

DUE: SEPTEMBER 10, 2012

The following ciphertext fragments were captured during transmission. It is known that classical ciphers were used for encryption. Recover the plaintexts. Explain *your* solution in detail.

1. CIPHERTEXT 1

Nmrbbp lnj updraarad qh dpq epcz qrcpi hw jrqqrad uz kpc jrjqpcc ha qkp unaf, nai hw knerad ahqkrad qh ih: habp hc qlrbp jkp kni oppopi raqh qkp uhhf kpc jrjqpcc lnj cpnirad, uxq rq kni ah orbqxcpc hc bhaepcjnrhaj ra rq, 'nai lknq rj qkp xjp hw n uhhf,' qkxhdkq Nmrbbp 'lrqkxq orbqxcpc hc bhaepcjnrha?'

Jh jkp lnj bhajripcrad ra kpc hla trai (nj lpmm nj jkp bxhmi, whc qkp khq inz tnip kpc wppm epcz jmpoz nai jxori), lkpqkpc qkp ompnjxpc hw tnfrad n inrjz-bknra lxhmi up lhcqk qkp qchxump hw dpqgrad xo nai orbfrad qkp inrjrpj, lkpa jxiipamz n Lkrqp Cnuurq lrqk oraf pzpj cna bmhjp uz kpc.

Qkpcp lnj ahqkrad jh EPCZ cptncfnumpp ra qknq; ahc iri Nmrbbp qkraf rq jh EPCZ txbk hxq hw qkp lnz qh kpnc qkp Cnuurq jnz qh rjpmw, 'Hk ipnc! Hk ipnc! R jknmm up mnqp!' (lkpa jkp qkxhdkq rq hepc nwqpcncij, rq hbbxccpi qh kpc qknq jkp hxdq qh knep lhaipcpi nq qkrj, uxq nq qkp qrtpp rq nmm jpptpi vxrqp anqxcnm); uxq lkpa qkp Cnuurq nbqxnmz QHHF N LNQBK HXQ HW RQJ LNRJQBHNQ-OHBFPQ, nai mhhfpi nq rq, nai qkpa kxcrcpi ha, Nmrbbp jqncqpi qh kpc wppq, whc rq wmnjkpi nbchjj kpc trai qknq jkp kni apepc upwhcp jppa n cnuurq lrqk prqkpc n lnrbqbhnq-ohbfpq, hc n lnqbk qh qnfp hxq hw rq, nai uxcarad lrqk bxcrhjrz, jkp cna nbchjj qkp wrpmi nwqpc rq, nai whcqxanqpmz lnj yxjq ra qrtpp qh jpp rq oho ihla n mncdp cnuurq-khmp xaipc qkp kpidd.

Ra nahqkpc thtpaq ihla lpaq Nmrbbp nwqpc rq, apepc habp bhajripcrad khl ra qkp lhcmi jkp lnj qh dpq hxq ndna.

Qkp cnuurq-khmp lpaq jqcnrdq ha mrfp n qxaapm whc jhtp lnz, nai qkpa iroopi jxiipamz ihla, jh jxiipamz qknq Nmrbbp kni ahq n thtpaq qh qkraf nuhxq jqhoorad kpcjpmw upwhcp jkp wxai kpcjpmw wmmmradd ihla n epcz ippo lpmm.

2. CIPHERTEXT 2

Nfuc, wynl, shge. Udnvu rwx prja GOMCG vydc ih ke ccw! 'S nmcwoi fdp wrln fscch B'fv dpevv l qr dygh msdc?' hao jyxw kcmjw. 'S dshm lv etmdzlv lydc laoi ccki rwx mvliko fd iao vygm. Cci fo jct: mrrr lhecb qx pfsg mrfstxu kxeoj bdp, Z rwbxb--' (ddk, ifs hxo, Rjxvo yys eorpcm cvttkkc rwbxxq dy dygh lyir xg rvp axcjmcl se rwx ctfdhvimdf, keb iaylew mrzq ltc emi t FVPN zyfb dizfpinxzrn yyi qwhgzlv hpw ftk uemleouet, tc kftko nyh gy flt my cghmoe rd aoi, qibvc gi pkj edhn gppvdzat my jyn bd fttk) '--ivq, iakk'q puylr iao igvad ughmkeat--uek rwx Z udgnvp lakk Jpmskssx yi Jdgqzrjwo Z'tt zyk rd?' (Tvzat aku ld bnvy lakk Jpmskssx grq, dk Vflvdbldt xskftk, llr iaylewm dycn poic cbmv egtxu udknj rd lkp.)

Ngxcvliei jft uoxyc tqrgc. 'B gflsxb zd X lrrja ykcj gbqyr IABFSVA dyc ttbkf! Whg wscgi zr'ae cvcb my tmbx ylr pfyee iao gcdivv rwtd nyad gzw mrvgg aorbh wynlltbu! Rwx Kerxikkfxxc, Z rwbxb--' (qwx grq gtdycg zvrb iaoic LTC em dgo cghmoegcz, dygh msdc, pl sk bxwx'k qdnxu yi tv rwx bzevm gfps) '--uek G hakcj wtfv rd tcb rwxw nfpd dyc ctwv mu mrv adnxkpn bc, pmj dxfu. Eeorqt, Fk'rk, xl dygh Gon Xttvrls hb Rshmbrijt?' (keb hao kpxxn km rnbkqtr kj qwx cgmzx--prlrr MLPILOPGCZ kj wdn'bv dpevzlv mrimjzr kft tsi! Bd ryl rwbxb wdn mfsaw wrlpzo zr?) 'Pgn nfpd ke gvgiyym vzrieo xgge cyc'ae dygcd wv ddk kjixgq! Em, xm'vc ltooi bd my rqz: ioifpic Z qwtvc qtx sk ugbdccc nz jmbxgygcy.'

Nfuc, wynl, shge. Rwxbv upl xfrwbxx calo km sh, cf Yabmv qdhx scvtx kyadsee pzkl. 'Sbxrf'ae wzqh fo mcgr wlaw my-egvad, Z qwhceb iasei!' (Sbxrf ltc kft vkk.) 'G whzv rwx'cj gxwvkqxb ycg lklatk yw kxeu rr ixk-kgbx. Nzlpw wp btbt! Z uxlr pmj poic shge ftko ngia wv! Rwxbv ygx xf kxvo zl iao rgg, B'w rdgtsu, zjm ifs bbqyr rtdtf p ukk, ycw dyi'l fvpn esbc p fylqt, ryl ichg. Ssi wy tyil orr qtdj, G lhxucg?' Txu ftko Rjxvo scvtx km vxd iyiaoi qaxogw, pgn nccm ye qprsee ih rvphxvw, gc t nicpfi jmgm yw upr, 'Nf apmc vyi ukkq? Sh mrrh xkk zpmc?' rls lydcibwvq, 'Sh lrrh xkk apmc?' wmg, ryl qtx, kj qwx mfsaw'k yclgvp tbdycg jevqibye, gi wsul'i fetf btdkcg przaw pkp qwx zlr xm. Cyc uxvk rwtd jft pkj bdssee dyp, rls aku hjld scvnx km skork iakk qwx grq ltvbgcz rrls bx yycw gzw Wseyw, txu qprsee ih rvp kxbp cpkxvqiei, 'Eml, Wseyw, mocj bx dyc ikekf: sbn pmj xfvv ttd r zpm?' gycc leubtgvp, rwnwg! rwnwg! bdpj jft vkdc jiye y wxkg mu ldazl keb ski ccpooj, ycw dyc utvc upl ymcg.

Tvzat pkj ldm k sgi aeir, pgn jft cedntw eg mc my ycg yovr xg k dmbxxk: qwx vfmzxn ln, qnd zr ltc rja wkii dooiftn; scuhibv ftk grq pykftk vflv ikjqpzo, rls mrv Uwbdv Ppulzr ltc jrxez zl hbqyr, wnbiwxgq umlg sk. Rwxbv upl xfr p fydccm df zt eyjr: ppkp utgd Rjxvo cgzx dyc lbxu, ycw grq ynck gc msdc ih rvyg bd jyn, tc zr inbecs t mfpccb, 'Ff br orph txu uwbcbcgl, rfu atdv gi'l qvribxx!' Qwx grq reyjc qxrzls bd nftg cyc inbecs mrv adkxvp, qnd kft Kkszx grq ch vflvxb km qx cvcc: lrv ddnxu ftkcvju bx r jdgq, cml akcj, lastf ltc cgi nz sw p kyn mu ekdnh akeexgq wpdf dyc ghyw.