Practical exercise 1

- Folder = 234

1 Vigenère analysis

Given a shift of 7
and the key = lWZCXBT
The right cipher is 0

ixNwQ uAqO OgOjHl. nDoBnumN, vgyc LxKJg Lg MpAL. VEfR CODf xyxA BNt TftxKMu xow BwLgA iHzODu."
"qbKBwQu"--jdgmEK yxt lCVYnBe--"mpER hxs PmOS?"
"PLu miNScOt, Gw. uNw KfxlJ'S gUqxkP SjLtx BK BqJf uwEKkKh HCP Nh JjwlHD CPjt nKQ uLnx BDNwPbGlO Nh VftzO XgQ. Xx lKM'v HoHE PNq Jvvp wAqRu MpA zz MfHxHD, uxwx BDzv QixG lNxBe PmOS hOpF BDD kKuxzENt MmtqJR. GSfGBQznlz MpAX eOpLAAC vL CKqPzkK; qxzDzrP uAmU VgOf MpA zpzfLBKQu Lg MpA bgluL EDN nLwxl DNtPfL BKN. DRu Bv PGgFs MqlD vEfR EAQg x uBlwK "VEf LwKMgO xx pAzf ApPvOStBbF, BDD dBuMmN." lekfBt OSkOsxl NDuQmxAOKA, yvM BDDA HoxE PGcQ uAmU LwPu DmAO vL dHDAQ wKuBt PGg QsBjARoBo umHNy TfKm CNpB. TH BDDA lbR qJ GkAjGo wMqQixz JHiEu, PqPMgPtBvC Np Qix vAWv JpKvEMi Qix iNQkSbE wB z uJbEtAQ rxsMG KE vEf Kmz-OcFoMmz LgK, bziEM yFuA EKTpAfw ilNpD uAml. Zv Qix kKLkKh Hn PGkP sxiN Fwxsw BDD czuBDESA Lo MpA QkSfK jwMm OpLm yKqPf Mw BQgKAR.
bDD vEsxm lDp LvM wB SkJf PmND fLvutU TpBbLG. eS yxt GwP EqO uAml Sq JfKmHX eOpLA PGg OjOmN. sjBz Aiz Sq yvBtz z txgM EDHeE xHCHC dB xtBAQ-yLsMpU DpLvzp PN vxlx BDDo ApPvOStBbF--BK SjB txi EE vEfR EAQg lvvsU. ZpA uH jQHnA tNkD z uQvKlU QcCu PwQKf QbDm PHoB, uBuA SjBz wqz MqQ itDA MqT.
JG nwBv, jdgmEK yxjMmz Nplz NvPHn Qix twRv QsBjwK txgM EwR qRu Hn xNy

---

abOuT tHiS PeRiOd. rEmEmbeR, webb SpOKe Of ThEM. THeY USEd axeS FOr WeapONs and TaMeD hOrSEs."
"taRTaRs"--mcnelL was PUZZlEd--"thIS far WeST?"
"NOt taRTaRs, No. yOu NeedN'T eXpecT ThOse TO CoMe bolLiNg OUT Of MiddLE ASia fOR sOme THOuSaNdS Of YearS YeT. We dON't KnOW TOo Much aBoUt ThE ax PeOpLE, save THat TheY MOvEd WeST fRoM THE iNterlOr PlaiNS.
EVeNTUalLy ThEY cRoSSED tO BRiTaiN; perHapS tHeY WeRe ThE anceSTORs Of ThE ceLtS WHO lOved HOrSeS TOO. BUt In THeIr TiME tHeY WERe a tIdaL "THe SoONeR we hEad DoWnSTrEaM, THE bEtTeR." mcnell STiRred REsTleSSLY, buT THEY KneW THaT tHeY MuSt KeEP tO cOVER uNtIl THe TrIbESmEn beLOw WeRe GOnE. SO THEY LaY iN HiDiNg aNoTher NIgHt, WiTNeSsInG On The nEXt MoRnING The aRRiVaL oF a sMaLlER parTY OF tHe Red-PaInTed MeN, agaIN wItH WOUnDed aMOnG tHeM. At The cOMiNg Of THiS reaR Guard THE actIVITY On ThE RiVeR baNk RoSe cLoSe To FReNZY.
tHE tHree MEn OuT oF TiMe WeRE dOublY UnEaSY. iT was NoT FoR tHeM To

MeReLY cRoSS THe RiVeR. thEy Had To bulld a rafT WHIcH wOULD bE waTER-wOrThY EnOugh TO take THEm DoWnSTrEaM--TO ThE sea IF tHeY WERe LuckY. AnD tO bUllD sUcH a sTuRdY RaFt WoULd TaKe TImE, tImE ThEy did NoT haVE NoW.
IN faCt, mcnelL waiTed OnLy UnTll The laSt TrIbaL rafT WaS oUt Of bOw

2 Substitution analysis

Cipher 1 is the substitution cipher
SAH → THE

vacs br bkrbnh? Km, ymt etio vbsa ih smkbjas mq hgrh B itrs vcbs sm jqcd sah khws mkh vam gcknr ahqh."
Ftqs rsmmn to. Abr gcrs vmqnr vhqh romfhk icsshq-mx-xclsgy, ckn Qmrr dhgbhuhn ah ihcks hwclsgy vacs ah rcbn. Dts Qmrr ahrbscshn. Ah vckshn sm sqy xmq xqhhnmi, c nhrbqh xhn dy abr rtroblbmkr mx vacs vcr jmbkj mk ahqh. Ah khbsahq gbfhn kmq sqtrshn Ftqs, dts ah samtjas ah tknhqrsmmn abi--dhsshq sack ah tknhqrsmmn Crah mq sah msahqr. Cgrm, vbsa Ftqs ah vcr rtqh ah lmtgn amgn abr mvk; bs vmtgn dh sah fbkn mx rsqtjjgh ah acn hwohqbhklhn dhxmqh.
"Smkbjas...." ah qhohcshn rgmvgy.
"Yhr, smkbjas!" Sahqh vcr khv hcjhqkhrr bk Ftqs'r umblh, xmq ah rhkrhn sacs sah msahq vcr vcuhqbkj. "B acuh dhhk oqhocqbkj xmq c gmkj sbih, dts sahqh itrs dh svm mx tr. Vh acuh sm scfh stqkr nqbubkj sah lcs. Sahqh lck dh km qhrs tksbg vh cqh xcq sm sah rmtsa. B shgg ymt bs vbgg dh hcry. Sahqh cqh xmmn lclahr cqqckjhn cgmkj sah qmtsh xmq hihqjhklbhr. B acuh c ico icqfhn sm ramv vahqh sahy cqh. Cqh ymt lmibkj?"
Vahk Qmrr nbn kms ckrvhq cs mklh sah msahq imuhn lgmrhq sm abi.
"Qhihidhq Acqny? Ah vcr kms sah xbqrs, ckn ah vbgg kms dh sah gcrs. Sahy trh tr to xcrs ahqh. Sacs br vay sahy dqmtjas ymt rm ptblfgy. B shgg ymt, bs br dhsshq sm scfh ymtq lacklh vbsa ih sack mk c qtk."
"Ckn vacs br c qtk?"

---

3 Transposition analysis

2 is the transposition
With the key 5|6|4|3|2|1|7|

niddrigs eh th fo ipulausnu su danusep alt dnas cd ogareeliosprhtiws tapsdicaen h ta ssnenrened gdnA y i newhn tro poeilan ndlro wsn da hehs rveoyna wn nilcinat notio a o gr gniov ht tBuetnec ssaS f orah lgodrapp aei ylntnacixtotmih ed raeh siawa ngys si hoid dliga ytninddimd ldegae dnepdeaytilbi S wo Nif danbl dehaso fo utteuQ heet tan hnepoe i fo nghrop ertht n ieylra e ninrmogw dn aauorbs gcab htktorp e gnistwob hittciovh ec dn ala sawte eh tnt fod h yade btahty rebmme eht of inevjulupope l noiatwt eshou ti rnw ot asctcelol ts etha gnindr draewfsih or fecrfouiledl vW yerit nithhad ereyh tis aocebd ma nae cdetpce enisbusnarts snoitac hciwhsifsiatereved yub eonts eh Tco epraflate m s toboono sle reddla sgnruw denaro ehtf alavirr eht ofiiffor cA serl dnai Diw eant werhddht noweirro cdel orat gnvihrtnee apo ence rofn Jocilel aV dannekcy R neh Ttrd yheib defta ot ckwssenit em ethew gntiieht th seisEy ereh T n erweoolor pnrg

dgeesgniet eewtbent eh twtrapo ion es refofopsohf iytilta gim ashevaht e nebexdetcpe eewtbenarre Tna nos nneil a tenapl rauqa t fo ertlaG heaawa xyy mor ftrae hetcihwh hg da hiht nveeoc am meh nmor egait cillJeohtiw yR nVac ta kehohs isu reldh detalb eroefhpetse porf edmr eh ta os mptht thaeeerh t retlnSm raolepaC n tC naiaam orgsna rtedAvpl pK

---

ridding the ship of unusual and usual pests and cargo despoilers with dispatch neatness and energy And when in port on alien worlds had never shown any inclination to go a roving But the scents of Sargol had apparently intoxicated him shearing away his solid dignity and middle aged dependability Now Sinbad flashed out of the Queen at the opening of her port in the early morning and was brought back protesting with both voice and claws at the end of the day by that member of the juvenile population whose turn it was to collect the standing reward for his forceful delivery Within three days it had become an accepted business transaction which satisfied everyone but The scrape of metal boot soles on ladder rungs warned of the arrival of their officers Ali and Dane withdrew down the corridor leaving the entrance open for Jellico and Van Rycke Then they drifted back to witness the meeting with the Eysies There were no prolonged greetings between the two parties no offer of hospitality as might have been expected between Terrans on an alien planet a quarter of the Galaxy away from the earth which had given them a common heritage Jellico with Van Rycke at his shoulder halted before he stepped from the ramp so that the three Inter Solar men Captain Cargo master and plpvAK

4 Hill cipher analysis

TH → BW
HE → UT

Clphertext 3 is the hill cipher

KEY = 20 9 7 25 = $\begin{pmatrix} 20 & 9 \\ 7 & 25 \end{pmatrix}$

tsmy. Bwkm kvqc jrpp ut rqsabjo jz uxji vqqrrld nn dtldavdvaql gs ggi wzj ypjiliuf.
Eacc'e kagvigsaa krrx--ckxv ordkvhh np epv nkxg hgi Ybcep, hut nmbxzl--yyo uhhazpu mp grr jutml, mp gexrx cj but wvbwxjys qtpc np bwv xwhkiy zrdnw jzsab wis. Snf kut ucmfhhouaqqs Ybce Emdmmso el qut Lkxluav oybjsdz ph epr. Zn vbx vpyysu kxi v ykrwuss lpjt ophmly zepzh kafza tkrldvpvfc cbk edkaqc g imhy. Bslw ub wbx edpp kxnmdz np igunoyldnnykw wbk ygbwrdtlz; zky tl edooqc kxnmdz svr wgjgs jrf nbx wvt ois rrmp bwkm sqnwzlkjce sqbw bwh nhtkngs, gi ut ffsg wzu, kr yccyjch epv nn pmltdc cbk cnz.
Lacb hfzwvt okm kxbku cbkzl epv. Ngjmez eutml yyj jn pmygrch rr bwgq, bwke dtkedz epm azte xkfmoztx. Fx rjhzldz epmoxru po bbk ilgkdz xjsabk. Ut mzg ea n anzyky lxjhwcxrquu azr, obrwub yyhodz rr cj ccrwq fn pybqpa nl dr dikgqpwi kazxr. Lxqsaze honw hk vv chhw ynmccya tsyi jzbzs gzlr jhhowik np wcr. Jr dgqusl gzls ggi mp gsjun vkm oodirdb' hhtkngs.
Ybce rrzhdz epm aic mp epp rmyf. Keps iyxufch, jrwca bgi rrazbkdz gi epy qcpon, yyj jjb si srhn gi bwg qpp kxx cgjmeze tl rr bwwun ihtkr mp ed whe hh cis. Ut edgrjhdz bwph ut kafza tgrpf sak vh cu asanw ggco epf vvrm mgviur wf nkm srazgdrrphaqg.

Vyinvky Ybce ggsr bwph uclkgqm yperdq dbk ooqc cuusp uj but avfkdz obbw tsyi jrwcz eutx fbx ojpfwvt ois. Jhpp xz ut kafzx, cutml yyj ja cppgs rr

---

free. This time when he brought up hard against an obstruction he was not followed.

Ross's conscious mind--that portion of him that was Rossa, the trader--was content to lie there, to yield to the lethargy born of the frigid world about him. But the subconscious Ross Murdock of the Project prodded at him. He had always had a certain cold hatred which could crystalize and become a spur. Once it had been hatred of circumstances and authority; now it became hatred for those who had led him into this wilderness with the purpose, as he knew now, of leaving him to freeze and die.

Ross pulled his hands under him. Though there was no feeling in them, they obeyed his will clumsily. He levered himself up and looked around. He lay in a narrow crevicelike cut, partly walled in by earth so frozen as to resemble steel. Crusted over it in long streaks from above were tongues of ice. To remain here was to serve his captors' purpose.

Ross inched his way to his feet. This opening, which was intended as his grave, was not so deep as the men had thought it in their hurry to be rid of him. He believed that he could climb out if he could make his body answer to his determination.

Somehow Ross made that supreme effort and came again to the rutted path from which they had tumbled him. Even if he could, there was no sense in free. This time when he brought up hard against an obstruction he was not followed.

Ross's conscious mind--that portion of him that was Rossa, the trader--was content to lie there, to yield to the lethargy born of the frigid world about him. But the subconscious Ross Murdock of the Project prodded at him. He had always had a certain cold hatred which could crystalize and become a spur. Once it had been hatred of circumstances and authority; now it became hatred for those who had led him into this wilderness with the purpose, as he knew now, of leaving him to freeze and die.

Ross pulled his hands under him. Though there was no feeling in them, they obeyed his will clumsily. He levered himself up and looked around. He lay in a narrow crevicelike cut, partly walled in by earth so frozen as to resemble steel. Crusted over it in long streaks from above were tongues of ice. To remain here was to serve his captors' purpose.

Ross inched his way to his feet. This opening, which was intended as his grave, was not so deep as the men had thought it in their hurry to be rid of him. He believed that he could climb out if he could make his body answer to his determination.

Somehow Ross made that supreme effort and came again to the rutted path from which they had tumbled him. Even if he could, there was no sense in