Divij Singh February 14, 2019

CS-302 Problem Set 1

Collaborators: *Mayukh, Jyotica*

Problem 1-1

Testing values for the key, with the value 22 we get ARENA, and with value 13 we get RIVER. Since both are valid keys, Antony does not know where to meet Caesar.

Problem 1-2

The decrypted letters can be found by $Decrypted(x) = a^{-1}(x-b)\%c$, where a^{-1} is the modular multiplicative inverse of modulo m
We can find this by multiplying a with increasing values and taking its modulo 26, till we get remainder 1.
In this case, the result is 3 $(9 * 3\%26 = 27)$

$U = 20$
$C = 2$
$R = 17$

Using the decryption formula, we get:
$U = 2 =$C
$C = 0 = A$
$R = 19 = T$

Thus the decrypted text is CAT

Problem 1-3

(a)

$$\begin{bmatrix} 7 & 13 \\ 2 & 5 \end{bmatrix}$$

(b) No, as the determinant is 26, which is a common factor with the modular base.

Problem 1-4

(a)
Keys : $0, 1, 2$
Message : $5, 6, 7, 8, 9$
Join Probability Distribution of m and k:

$m\|k$	0	1	2
5	$\frac{1}{9}$	$\frac{1}{9}$	$\frac{1}{9}$
6	$\frac{1}{9}$	$\frac{1}{9}$	$\frac{1}{9}$
7	$\frac{1}{18}$	$\frac{1}{18}$	$\frac{1}{18}$
8	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$
9	$\frac{1}{36}$	$\frac{1}{36}$	$\frac{1}{36}$

We shall take $Pr[m = 5|c = 6]$:
$Pr[c] = 1/9 + 1/9 = 2/9$
$Pr[m = 5|c = 6] = \frac{1/9}{2/9} = 1/2 \neq Pr[m = 5]$ which is $(1/3)$
Thus Alice won't be able to reach perfect security.

(b)

$m\|k$	0	1	2
5	$\frac{1}{15}$	$\frac{1}{15}$	$\frac{1}{15}$
6	$\frac{1}{15}$	$\frac{1}{15}$	$\frac{1}{15}$
7	$\frac{1}{15}$	$\frac{1}{15}$	$\frac{1}{15}$
8	$\frac{1}{15}$	$\frac{1}{15}$	$\frac{1}{15}$
9	$\frac{1}{15}$	$\frac{1}{15}$	$\frac{1}{15}$

We shall take $Pr[m = 5|c = 6]$:
$Pr[c] = 1/15 + 1/15 = 2/15$
$Pr[m = 5|c = 6] = \frac{1/15}{2/15} = 1/2 \neq Pr[m = 5]$ which is $(1/5)$
Thus this is still not perfectly secure. However, increasing the key space to be equal to the message space will allow this to be perfectly secure.

(c)

$m\|k$	0	1	2	3	4
5	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
5	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
5	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
5	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$
5	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$	$\frac{1}{25}$

We shall take $Pr[m = 5|c = 6]$:
$Pr[c] = 1/25 + 1/25 + 1/25 + 1/25 + 1/25 = 1/5$
$Pr[m = 5|c = 6] = \frac{1/25}{1/5} = 1/5 = P[m = 5]$ which is (1/5)
From this question, we can see that the key space should be either equal to, or greater than the message space for perfect security.

Problem 1-5

(a) Zark will notice that it is a repeating letter as the message will just be another set of repeating letters, depending on the key value of the shift. Zark will not, however, be able to deduce the key or the mssage.
(b) Again, Zark will notice that it is a repeating letter, as the message will just be another set of repeating letters. He will not be able to deduce the letter or the keys.
(c) Zark will notice that it is one repeated letter as the cipher text will literally be the same as the plaintext, as the value of 'a' when being multiplied by the matrix is 0. As a result, he will also be able to realise that the initial message is the same as the cipher text, as all the characters are the same, and are the letter 'a'. He will not, however, get the key.

Problem 1-6

(a) HELP ME IM TRAPPED INSIDE A CAESAR CIPHER AND CANT GET OUT
(b) YOU MUST BE SPEED OF LIGHT BECAUSE TIME STOPS WHEN I LOOK AT YOU HAPPY VALENTINES DAY
(c) I HOPE YOU INTERCEPT THIS SECRET TRANSMISSION WITHOUT ANY ERROR THIS TRANSMISSION HAS TRAVELLED A MILLION LIGHT YEARS TO INFORM YOU THAT WE ARE COMING SOON

(d) OLD DEBAYAN IS A GOOD ONE EXCEPT FOR MELON MELON MELON MELON MELON

Problem 1-7

(a)
nevergonnagiveyouupnevergonnaletyoudownnevergonnarunaroundanddesertyounevergonna
makeyoucrynevergonnasaygoodbyenevergonnatellyouliesandhurtyouwerenostrangerstolovey
ouknowtherulesandsodoiacommitmentiswhatimlookingforyouwontgetthisfromanyotherguyij
ustwannatellyouhowimfeelingwannamakeyouunderstandnevergonnagiveyouupnevergonnalet
youdown

(b)
everyinchofwallspaceiscoveredbyabookcaseeachbookcasehassixshelvesgoingalmosttotheceilin
gsomebookshelvesarestackedtothebrimwithhardbackbooksssciencemathshistoryandeverythin
gelseothershelveshavetwolayersofpaperbacksciencefictionwiththebacklayerofbooksproppedu
ponoldtissueboxesorlengthsofwoodsothatyoucanseethebacklayerofbooksabovethebooksinfron
tanditstillisntenoughbooksareoverflowingontothetablesandthesofasandmakinglittleheapsund
erthewindowsthisisthelivingroomofthehouseoccupiedbytheeminentprofessormichaelverresev
ansandhiswifemrspetuniaevansverresandtheiradoptedsonharryjamespotterevansverrestherei
saletterlyingonthelivingroomtableandanunstampedenvelopeofyellowishparchmentaddressedt
omrhpotterinemeraldgreeninktheprofessorandhiswifearespeakingsharplyateachotherbutthey
arenotshoutingtheprofessorconsidersshoutingtobeuncivilisedyourejokingmichaelsaidtopetuni
ahistoneindicatedthathewasverymuchafraidthatshewasseriousmysisterwasawitchpetuniarep
eatedshelookedfrightenedbutstoodhergroundherhusbandwasawizardthisisabsurdmichaelsaid
sharplytheywereatourweddingtheyvisitedforchristmasitoldthemyouwerenttoknowpetuniawh
isperedbutitstrueiveseenthingstheprofessorrolledhiseyesdeariunderstandthatyourenotfamilia
rwiththescepticalliteratureyoumaynotrealisehoweasyitisforatrainedmagiciantofaketheseemin
glyimpossiblerememberhowitaughtharrytobendspoonsifitseemedliketheycouldalwaysguessw
hatyouwerethinkingthatscalledcoldreadingitwasntbendingspoonswhatwasitthenpetuniabithe
rlipicantjusttellyouyoullthinkimsheswallowedlistenmichaeliwasntalwayslikethisshegestureda
therselfasthoughtoindicateherlitheformlilydidthisbecauseibecauseibeggedherforyearsibegged
herlilyhadalwaysbeenprettierthanmeandidbeenmeantoherbecauseofthatandthenshegotmagic
canyouimaginehowifeltandibeggedhertousesomeofthatmagiconmesothaticouldbeprettytooev
enificouldnthavehermagicatleasticouldbeprettytearsweregatheringinpetuniaseyesandlilywoul
dtellmenoandmakeupthemostridiculousexcuseslikethworldwouldendifshewerenicetohersiste
roracentaurtoldhernottothemostridiculousthingsandihatedherforitandwhenihadjustgraduate
dfromuniversityiwasgoingoutwiththisboyvernondursleyhewasfatandhewastheonlyboywhowo
uldtalktomeandhesaidhewantedchildrenandthathisfirstsonwouldbenameddudleyandithought
tomyselfwhatkindofparentnamestheirchilddudleydursleyitwaslikeisawmywholefuturelifestret

chingoutinfrontofmeandicouldntstanditandiwrotetomysisterandtoldherthatifshedidnthelpme
idratherjustpetuniastoppedanywaypetuniasaidhervoicesmallshegaveinshetoldmeitwasdanger
ousandisaidididntcareanymoreandidrankthispotionandiwassickforweeksbutwhenigotbetterm
yskinclearedupandifinallyfilledoutandiwasbeautifulpeoplewerenicetomehervoicebrokeandafte
rthaticouldnthatemysisteranymoreespeciallywhenilearnedwhathermagicbroughtherintheend
darlingmichaelsaidgentlyyougotsickyougainedsomeweightwhilerestinginbedandyourskinclea
reduponitsownorbeingsickmadeyouchangeyourdietshewasawitchpetuniarepeatedisawitpetun
iamichaelsaidtheannoyancewascreepingintohisvoiceyouknowthatcantbetruedoireallyhavetoe
xplainwhypetuniawrungherhandssheseemedtobeonthevergeoftearsmyloveiknowicantwinargu
mentswithyoubutpleaseyouhavetotrustmeonthisdadmumthetwoofthemstoppedandlookedath
arryasthoughtheydforgottentherewasathirdpersonintheroomharrytookadeepbreathmumyour
parentsdidnthavemagicdidtheynopetuniasaidlookingpuzzledthennooneinyourfamilyknewabo
utmagicwhenlilygotherletterhowdidtheygetconvincedahpetuniasaidtheydidntjustsendaletter
theysentaprofessorfromhogwartshepetuniaseyesflickedtomichaelheshowedussomemagictheny
oudonthavetofightoverthisharrysaidfirmlyhopingagainsthopethatthistimejustthisoncetheyw
ouldlistentohimifitstruewecanjustgetahogwartsprofessorhereandseethemagicforourselvesand
dadwilladmitthatitstrueandifnotthenmumwilladmitthatitsfalsethatswhattheexperimentalme
thodisforsothatwedonthavetoresolvethingsjustbyarguingtheprofessorturnedandlookeddowna
thimdismissiveasusualohcomenowharryreallymagicithoughtyoudknowbetterthantotakethiss
eriouslysonevenifyoureonlytenmagicisjustaboutthemostunscientificthingthereisharrysmouth
twistedbitterlyhewastreatedwellprobablybetterthanmostgeneticfatherstreatedtheirownchild
renharryhadbeensenttothebestprimaryschoolsandwhenthatdidntworkouthewasprovidedwith
tutorsfromtheendlesspoolofstarvingstudentsalwaysharryhadbeenencouragedtostudywhateve
rcaughthisattentionboughtallthebooksthatcaughthisfancysponsoredinwhatevermathsorscien
cecompetitionsheenteredhewasgivenanythingreasonablethathewantedexceptmaybetheslighte
stshredofrespectadoctorteachingbiochemistryatoxfordcouldhardlybeexpectedtolistentothead
viceofalittleboyyouwouldlistentoshowinterestofcoursethatswhatagoodparentwoulddoandsoif
youconceivedofyourselfasagoodparentyouwoulddoitbuttakeatenyearoldseriouslyhardlysomet
imesharrywantedtoscreamathisfathermumharrysaidifyouwanttowinthisargumentwithdadloo
kinchaptertwoofthefirstbookofthefeynmanlecturesonphysicstheresaquotethereabouthowphilo
sopherssayagreatdealaboutwhatscienceabsolutelyrequiresanditisallwrongbecausetheonlyrule
inscienceisthatthefinalarbiterisobservationthatyoujusthavetolookattheworldandreportwhaty
ouseeumoffthetopofmyheadicantthinkofwheretofindsomethingabouthowitsanidealofscienceto
settlethingsbyexperimentinsteadofargumentshismotherlookeddownathimandsmiledthankyou
harrybutherheadrosebackuptostareatherhusbandidontwanttowinanargumentwithyourfather
iwantmyhusbandtotolistentohiswifewholoveshimandtrustherjustthisonceharryclosedhiseyesb
rieflyhopelessbothofhisparentswerejusthopelessnowhisparentsweregettingintooneofthoseargu
mentsagainonewherehismothertriedtomakehisfatherfeelguiltyandhisfathertriedtomakehismo
therfeelstupidimgoingtogotomyroomharryannouncedhisvoicetrembledalittlepleasetrynottofi
ghttoomuchaboutthismumdadwellknowsoonenoughhowitcomesoutrightofcourseharrysaidhis
fatherandhismothergavehimareassuringkissandthentheywentonfightingwhileharryclimbedth
estairstohisbedroomheshutthedoorbehindhimandtriedtothinkthefunnythingwasheshouldhav

eagreedwithdadnoonehadeverseenanyevidenceofmagicandaccordingtomumtherewasawholem
agicalworldouttherehowcouldanyonekeepsomethinglikethatasecretmoremagicthatseemedlike
arathersuspicioussortofexcuseitshouldhavebeenacleancaseformumjokinglyingorbeinginsanein
ascendingorderofawfulnessifmumhadsenttheletterherselfthatwouldexplainhowitarrivedatthel
etterboxwithoutastampalittleinsanitywasfarfarlessimprobablethantheuniversereallyworkingl
ikethatexceptthatsomepartofharrywasutterlyconvincedthatmagicwasrealandhadbeensinceth
einstanthesawtheputativeletterfromthehogwartsschoolofwitchcraftandwizardryharryrubbed
hisforeheadgrimacingdontbelieveeverythingyouthinkoneofhisbookshadsaidbutthisbizarrecert
aintyharrywasfindinghimselfjustexpectingthatyesahogwartsprofessorwouldshowupandwavea
wandandmagicwouldcomeoutthestrangecertaintywasmakingnoefforttoguarditselfagainstfals
ificationwasntmakingexcusesinadvanceforwhytherewouldntbeaprofessorortheprofessorwould
onlybeabletobendspoonswheredoyoucomefromstrangelittlepredictionharrydirectedthethough
tathisbrainwhydoibelievewhatibelieveusuallyharrywasprettygoodatansweringthatquestionbu
tinthisparticularcasehehadnocluewhathisbrainwasthinkingharrymentallyshruggedaflatmetal
plateonadooraffordspushingandahandleonadooraffordspullingandthethingtodowithatestable
hypothesisistogoandtestithetookapieceoflinedpaperfromhisdeskandstartedwritingdeardeputy
headmistressharrypausedreflectingthendiscardedthepaperforanothertappinganothermillimet
reofgraphitefromhismechanicalpencilthiscalledforcarefulcalligraphydeardeputyheadmistress
minervamcgonagallorwhomsoeveritmayconcernirecentlyreceivedyourletterofacceptancetoho
gwartsaddressedtomrhpotteryoumaynotbeawarethatmygeneticparentsjamespotterandlilypot
terformerlylilyevansaredeadiwasadoptedbylilyssisterpetuniaevansverresandherhusbandmich
aelverresevansiamextremelyinterestedinattendinghogwartsconditionalonsuchaplaceactuallye
xistingonlymymotherpetuniasayssheknowsaboutmagicandshecantuseitherselfmyfatherishigh
lyscepticalimyselfamuncertainialsodontknowwheretoobtainanyofthebooksorequipmentlisted
inyouracceptancelettermothermentionedthatyousentahogwartsrepresentativetolilypotterthe
nlilyevansinordertodemonstratetoherfamilythatmagicwasrealandipresumehelplilyobtainhers
choolmaterialsifyoucoulddothisformyownfamilyitwouldbeextremelyhelpfulsincerelyharryjam
espotterevansverresharryaddedtheircurrentaddressthenfoldeduptheletterandputitinanenvelo
pewhichheaddressedtohogwartsfurtherconsiderationledhimtoobtainacandleanddripwaxontot
heflapoftheenvelopeintowhichusingapenknifestipheimpressedtheinitialshjpevifhewasgoingtod
escendintothismadnesshewasgoingtodoitwithstylethenheopenedhisdoorandwentbackdownsta
irshisfatherwassittinginthelivingroomandreadingabookofhighermathstoshowhowsmarthewas
andhismotherwasinthekitchenpreparingoneofhisfathersfavouritemealstoshowhowlovingshew
asitdidntlookliketheyweretalkingtooneanotheratallasscaryasargumentscouldbenotarguingwa
ssomehowmuchworsemumharrysaidintotheunnervingsilenceimgoingtotestthehypothesisacco
rdingtoyourtheoryhowdoisendanowltohogwartshismotherturnedfromthekitchensinktostareat
himlookingshockediidontknowithinkyoujusthavetoownamagicowlthatshouldvesoundedhighl
ysuspiciousohsotheresnowaytotestyourtheorythenbutthepeculiarcertaintyinharryseemedwill
ingtostickitsneckoutevenfurtherwellthelettergotheresomehowharrysaidsoilljustwaveitaround
outsideandcallletterforhogwartsandseeifanowlpicksitupdaddoyouwanttocomeandwatchhisfat
hershookhisheadminutelyandkeptonreadingofcourseharrythoughttohimselfmagicwasadisgrac
efulthingthatonlystupidpeoplebelievedinifhisfatherwentsofarastotestthehypothesisorevenwat

chitbeingtestedthatwouldfeellikeassociatinghimselfwiththatonlyasharrystumpedoutthebackd
oorintothebackgardendiditoccurtohimthatifanowldidcomedownandsnatchtheletterhewasgoin
gtohavesometroubletellingdadaboutitbutwellthatcantreallyhappencanitnomatterwhatmybra
inseemstobelieveifanowlreallycomesdownandgrabsthisenvelopeimgoingtohaveworriesalotmo
reimportantthanwhatdadthinksharrytookadeepbreathandraisedtheenvelopeintotheairheswal
lowedcallingoutletterforhogwartswhileholdinganenvelopehighintheairinthemiddleofyourown
backgardenwasactuallyprettyembarrassingnowthathethoughtaboutitnoimbetterthandadiwill
usethescientificmethodevenifitmakesmefeelstupidletterharrysaidbutitactuallycameoutasmor
eofawhisperedcroakharrysteeledhiswillandshoutedintotheemptyskyletterforhogwartscanigeta
nowlharryaskedabemusedwomansvoiceoneoftheneighboursharrypulleddownhishandlikeitwas
onfireandhidtheenvelopebehindhisbacklikeitwasdrugmoneyhiswholefacewashotwithshamean
oldwomansfacepeeredoutfromabovetheneighbouringfencegrizzledgreyhairescapingfromherhai
rnetmrsfiggtheoccasionalbabysitterwhatareyoudoingharrynothingharrysaidinastrangledvoice
justtestingareallysillytheorydidyougetyouracceptanceletterfromhogwartsharryfrozeinplaceye
sharryslipssaidalittlewhilelaterigotaletterfromhogwartstheysaytheywantmyowlbythethirtyfir
stofjulybutbutyoudonthaveanowlpoordearicantimaginewhatsomeonemusthavebeenthinkings
endingyoujustthestandardletterawrinkledarmstretchedoutoverthefenceandopenedanexpecta
nthandhardlyeventhinkingatthispointharrygaveoverhisenvelopejustleaveittomedearsaidmrsf
iggandinajiffyortwoillhavesomeoneoverandherfacedisappearedfromoverthefencetherewasalon
gsilenceinthegardenthenaboysvoicesaidcalmlyandquietlywhat

(c)
uponthisbasisiamgoingtoshowyouhowabunchofbrightyoungfolksdidfindachampionamanwith
boysandgirlsofhisownamanofsodominatingandhappyindividualitythatyouthisdrawntohimasi
saflytoasugarbowlitisastoryaboutasmalltownitisnotagossipyyarnnorisitadrymonotonousacco
untfullofsuchcustomaryfillinsasromanticmoonlightcastingmurkyshadowsdownalongwindingc
ountryroad