COL 759 - Tutorial 2

Vivek Singh

2019MCS2574

1 Question 1- PlayFair Cipher:

Cipher Text to decipher

EGHXBYDPAIIKEHXCBXBOICPBKCDPBSOZTPFSQTCUOWEGCHMQLOGCQCPQABDCULBEPHZXDPTSCEXTTPEGHXOFWGCUIAPDPHLUBMUEPHULZRXGHOHDPLXGQIPEDNUSPUEZCLBWIKOEPHDHEHXUMBFSAKYGEBCXHEYBDAELMSZRSDGQAEEIBOCECGWNCBDQBYWGPHUHHUDEPHYBTMULOBHVKMBQICALDMCUETNLBMLMACRTIKEPUSUEIKOELAACPLEIUPTPUXDPMUKOCUXHSQSDXTPDBUDNOUECUESIFQBOSTHELMUSEWDNOUECUECILOQAOLZKSFOKBOUBDRES

Cryptanalysis

- By analyzing the cipher text we found that element : J is missing.
- Hence we know that in key of play-fair cipher i.e 5X5 matrix it contain all letters except J
- Since in play fair we replace bi-gram of plain text hence we will analyse bigrmas of plain Text to bigram of english alphabet.
- TOP 10 english language bigram : ”TH”, ”HE”, ”IN”, ”ER”, ”AN”, ”RE”, ”ND”, ”AT”, ”ON”, ”NT”
- Top 10 bigram of cipher text is : ’PH’: 6, ’DP’: 4, ’IK’: 4, ’BO’: 4, ’CU’: 4, ’UE’: 4, ’EG’: 3, ’TP’: 3, ’UL’: 3, ’DN’: 3
- By using brute force mapping between the bi-grams I wasn’t able to find anything meaningful:
- It seems very hard task to find the final key using manual work.
- Hence I used algorithm from the following source to find the answer:

A	B	S	O	L
U	T	E	C	D
F	G	H	I	K
M	N	P	Q	R
V	W	X	Y	Z

- LINK:http://practicalcryptography.com/cryptanalysis/stochastic-searching/cryptanalysis-playfair/
- PLAIN-TEXT IS: **THEPOWEROFHISEYESWASCONSIDERABLYENHANCEDBYTHEIRPOSITIONPLACEDASTHEYWEREB ETWEENTHEPAINTEDFOREHEADANDTHEDARKWHISKERSWHICHSTREAMEDXDOWNHISCHEEKSEVE NAHALFWITSEYESWOULDSPARKLEINSUCHASETTINGTOCROWNTHEEFFECTHEWOUNDASAFXFRON COLOUREDTURBANAROUNDHISHEADTHISCOLOURSCHEMENEVERFAILEDPEOPLEWEREATTRACTE DTOHIMASBEESAREATXTRACTEDTOCOSMOSORDAHLIASTALKSX**
- KEY : **ABSOLUTE**

2 Question 2: Simple Substitution

Cipher Text to decipher

Nbzmnzi rh z xlfmgib rm Zhrz. Nzmb Ilsrmtbz Nfhornh orev gsviv. Gsvri orevh ziv evib wruurxfog. Gsvb nfhg nrtizgv z olg. Rm 2017, gsviv rh hgilmt nrorgzib zxgrlm ztzrmhg Ilsrmtbz Nfhornh. Gsviv rh z olg lu erlovmxv. Nzmb kvlkov wrv. Z olg lu kvlkov ifm zdzb gl zmlgsvi xlfmgib. Hlnv kvlkov yvorvev gszg gsviv rh tvmlxrwv lu gsv Ilsrmtbzh. Gsv Nbzmnzi tlevimnvmg zhph z xlnnrggvv gl urmw lfg dszg szkkvmh. Gsv xlnnrggvv hzbh gszg gsviv rh ml tvmlxrwv. Sldvevi, gsviv rh hvirlfh xirnv. Z olg lu kvlkov wl mlg yvorvev gsrh. Gsvb hzb gszg gsv tlevimnvmg dzmgh gl srwv gsv gifgs.

Cryptanalysis

Frequency analysis

Top english unigram:
[e, t, a, o, i, n, s, h, r, d]

Nbzmnzi rh z xlfmgib rm Zhrz. Nzmb Ilsrmtbz Nfhornh orev gsviv. Gsvri orevh ziv evib wruurxfog. Gsvb nfhg nrtizgv z olg. Rm 2017, gsviv rh hgilmt nrorgzib zxgrlm ztzrmhg Ilsrmtbz Nfhornh. Gsviv rh z olg lu erlovmxv. Nzmb kvlkov wrv. Z olg lu kvlkov ifm zdzb gl zmlgsvi xlfmgib. Hlnv kvlkov yvorvev gszg gsviv rh tvmlxrwv lu gsv Ilsrmtbzh. Gsv Nbzmnzi tlevimnvmg zhph z xlnnrggvv gl urmw lfg dszg szkkvmh. Gsv xlnnrggvv hzbh gszg gsviv rh ml tvmlxrwv. Sldvevi, gsviv rh hvirlfh xirnv. Z olg lu kvlkov wl mlg yvorvev gsrh. Gsvb hzb gszg gsv tlevimnvmg dzmgh gl srwv gsv gifgs.

Taking top two frequency of the cipher text we get **V** and **G**

We get

1. V ->E

2. G ->T

3. Now using these two mapping and the english trigram "THE" we get GSV ->THE hence S ->H

4. Gsviv implies I ->R as it completes the word **THERE**

5 & 6. Rm implies RM ->IN **as "IN 2017"**

7. Gsvb implies B ->Y as it completes the word **THEY**

8. Z implies Z ->A Starting of sentence and repeats multiple times.

9. gl implies L ->O as it completes the word **TO**

10. olg implies O ->L as it completes the word **LOT**

11. lu implies U ->F as it completes the word **OF**

12. dszg implies D ->W as it completes the word **WHAT**

13. evib implies E ->V as it completes the word **VERY**

Replacing the above mapping into the cipher text we get following partial plain text:

nyamnar ih a xofmtry im ahia. namy rohimtya nfhlinh live there. their liveh are very wiffixflt. they nfht nitrate a lot. im 2017, there ih htromt nilitary axtiom ataimht rohimtya nfhlinh. there ih a lot of violemxe. namy keokle wie. a lot of keokle rfm away to amother xofmtry. hone keokle yelieve that there ih temoxiwe of the rohimtyah. the nyamnar tovermnemt ahph a xonnittee to fimw oft what hakkemh. the xonnittee hayh that there ih mo temoxiwe. however, there ih heriofh xrine. a lot of keokle wo mot yelieve thih. they hay that the tovermnemt wamth to hiwe the trfth

Now it becomes easier to decrpyt the remaining letters as now it gets very intuitive as following:

14. nyamnar implies N ->M as it completes the word **MYANMAR**
15. ih implies H ->S as it completes the word **IS**
16. im implies M ->N as it completes the word **IN**
17. keokle implies K ->P as it completes the word **PEOPLE**

Again using the mapping we further get:

myanmar is a xofntry in asia. many rohintya mfslims live there. their lives are very wiffixflt. they mfst mitrate a lot. in 2017, there is stront military axtion atainst rohintya mfslims. there is a lot of violenxe. many people wie. a lot of people rfn away to another xofntry. some people yelieve that there is tenoxiwe of the rohintyas. the myanmar tovernment asps a xommittee to finw oft what happens. the xommittee says that there is no tenoxiwe. however, there is seriofs xrime. a lot of people wo not yelieve this. they say that the tovernment wants to hiwe the trfth

18. trfth implies F ->U as it completes the word **TRUTH**
19. hiwe implies W ->D as it completes the word **HIDE**
20. xrime implies X ->C as it completes the word **CRIME**
21. yelieve implies Y ->B as it completes the word **BELIEVE**
22. atainst implies T ->G as it completes the word **AGAINST**
23. asps implies P ->K as it completes the word **ASKS**

Hence we obatined the following final plain text:

Using above mentioned mapping between letters we are able to decipher to a meaningful plain-text

myanmar is a country in asia. many rohingya muslims live there. their lives are very difficult. they must migrate a lot. in 2017, there is strong military action against rohingya muslims. there is a lot of violence. many people die. a lot of people run away to another country. some people believe that there is genocide of the rohingyas. the myanmar government asks a committee to find out what happens. the committee says that there is no genocide. however, there is serious crime. a lot of people do not believe this. they say that the government wants to hide the truth

3 Question 3: Simple Substitution

Cipher Text to decipher

Htghst xlt lxflekttfl zg hkgztez zitok laof ykgd zit lxf. Zitkt ol q ftv lzxrn. Oz lqnl ziqz lgdt eitdoeqsl of lxflekttfl utz ofzg htghst l wsggr Leotfzolzl ztlz ygxk royytktfz lxflekttfl qfr lob eitdoeqsl. Zitn yofr ziqz qss lob eitdoeqsl utz ofzg zit wgrn. Zitn rg fgz afgv viqz zitlt eitdoeqsl rg zg htghst. Oz ol vgkknofu. Leotfzolzl dxlz rg dgkt ktltqkei zg xfrtklzqfr igv eitdoeqsl utz ofzg zit wgrn.

Cryptanalysis

Frequency analysis

Top english unigram:
[e, t, a, o, i, n, s, h, r, d]

By doing a frequency analysis we get following frequency **T: 43, Z: 37**

Hence we get following mapping :

1. T->E

2. Z ->T

3. Q ->A as it comes individually many times.

Replacing the top three we get following partial-cipher text:

heghse xle lxflekeefl tg hkgteet tieok laof ykgd tie lxf. tieke ol a fev ltxrn. ot lanl tiat lgde eiedoeasl of lxflekeefl uet oftg heghse l wsggr leoeftoltl telt ygxk royyekeft lxflekeefl afr lob eiedoeasl. tien yofr tiat ass lob eiedoeasl uet oftg tie wgrn. tien rg fgt afgv viat tiele eiedoeasl rg tg heghse. ot ol vgkknofu. leoeftoltl dxlt rg dgke keleakei tg xfrekltafr igv eiedoeasl uet oftg tie wgrn

4. tg: G ->O replacing we get **TO**

5 & 6. ot ol: O->I and L ->S replacing it we get **IT IS**

7. oftg: F ->N replacing we get **INTO**

Again replacing we get:

heohse xse sxnsekeens to hkoteet tieik sain ykod tie sxn. tieke is a nev stxrn. it sans tiat sode eiedieass in sxnsekeens uet into heohses wsoor seientists test yoxk riyyekent sxnsekeens anr sib eiedieass. tien yinr tiat ass sib eiedieass uet into tie worn. tien ro not anov viat tiese eiedieass ro to heohse. it is vokkninu. seientists dxst ro doke keseakei to xnrekstanr iov eiedieass uet into tie wor

8. uet U->G replacing we get **GET**

9. tie I->H we get **THE**

10. seientists E->C repalcing we get **SCIENTISTS**

11 & 12. heohses H->P and S->L replacing we get **PEOPLES**

people xse sxnsckeens to pkotect theik sain ykod the sxn. theke is a nev stxrn. it sans that sode chedicals in sxnsckeens get into people s wloor scientists test yoxk riyyekent sxnsckeens anr sib chedicals. then yinr that all sib chedicals get into the worn. then ro not anov vhat these chedicals ro to people. it is vokkning. scientists dxst ro doke keseakch to xnrekstanr hov chedicals get into the worn

13. chedicals D->M replacing we get **CHEMICALS**

14. xse X->U replacing we get **USE**

15. pkotect K->R replacing we get **PROTECT**

16 & 17. vokkning V->W and N ->Y replacing we get **WORRYING**

Now we get partial plainText as:

people use sunscreens to protect their sain yrom the sun. there is a new stury. it says that some chemicals in sunscreens get into people s wloor scientists test your riyyerent sunscreens anr sib chemicals. they yinr that all sib chemicals get into the wory. they ro not anow what these chemicals ro to people. it is worrying. scientists must ro more research to unrerstanr how chemicals get into the wory

18. & 19. W ->B and R->D we get **wloor->BLOOD**

20. A->K we get **sain->SKIN**

21. Y->F we get **yrom ->FROM**

22. B->X we get **sib ->SIX**

Final Plain-text after replacing above mapping is :

people use sunscreens to protect their skin from the sun. there is a new study. it says that some chemicals in sunscreens get into people s blood scientists test four different sunscreens and six chemicals. they find that all six chemicals get into the body. they do not know what these chemicals do to people. it is worrying. scientists must do more research to understand how chemicals get into the body