CS152-Homework2

Hongchen Cao 2019533114

2020.9.16

1

key	plaintext
a	moxyxpluhabtxsbrxaaliyxzxum
b	lpwzwqkvgbauwtaswbzmhzwawvl
c	kqvavrjwfczvvuztvcyngavbvwk
d	jrubusixedywuvyuudxofbucuxj
e	istctthydexxtwxvtewpectdtyi
f	htsdsugzcfwysxwwsfvqddseszh
g	gurervfabgvzryvxrgurcerfrag
h	fvqfqwebahuaqzuyqhtsbfqgqbf
i	ewpgpxdczitbpatzpistagphpce
j	dxohoycdyjscobsaojruzhoiodd
k	cyninzbexkrdncrbnkqvyinjnec
l	bzmjmaafwlqemdqcmlpwxjmkmfb
m	aalklbzgvmpflepdlmoxwkllga
n	zbklkcyhunogkfoeknnyvlkmkhz
o	ycjmjdxitonhjgnfjomzumjnjiy
p	xdiniewjspmiihmgiplatnioijx
q	wehohfvkrqljhilhhqkbsohphkw
r	vfgpggulqrkkgjkigrjcrpgqglv
s	ugfqfhtmpsjlfkjjfsidqqfrfmu
t	thereisnotimelikethepresent

So **key**='t' and **plaintext**="thereisnotimelikethepresent"

2

Plaintext:

$$imaynotbeabletogrowflowersbutmygardenproduces$$
$$justasmanydeadleavesoldovershoespiecesofropea$$
$$ndbushelsofdeadgrassasanybodysandtodayibought$$
$$awheelbarrowtohelpinclearingitupihavealwayslo$$
$$vedandrespectedthewheelbarrowitistheonewheele$$
$$dvehicleofwhichiamperfectmaster$$

Description of the steps:

Count the number of occurrences of each letter by python:
{'E': 12, 'M': 5, 'G': 24, 'L': 7, 'O': 10, 'S': 20, 'U': 14, 'D': 8, 'C': 37, 'N': 13, 'W': 5, 'Y': 15, 'F': 9, 'H': 5, 'K': 18, 'P': 6, 'I': 15, 'X': 7, 'J': 7, 'Q': 1, 'A': 5, 'Z': 13}
We guess $d_k(C) = e$; $d_k(\{G, S, K, I, Y, U, Z, N\}) \subseteq \{t, a, o, i, n, s, h, r\}$
And based on the hint, we have

$$EMGLOSUDeGDNeUSWYSwHNSweYKDPUMLWGYIeOXYSIPJeK$$
$$QPKUGKMGOLIeGINeGAeKSNISAeYKZSeKXEeJeKSHYSXeG$$
$$OIDPKZeNKSHIeGIWYGKKGKGOLDSILKGOIUSIGLEDSPWZU$$
$$GwZeeNDGYYSwUSZeNXEOJNeGYEOWEUPXEZGAeGNwGLKNS$$
$$AeIGOIYeKXeJUeIUZewZeeNDGYYSwEUEKUZeSOewZeeNe$$
$$IAeZEJNeSHwZEJZEGMXeYHeJUMGKUeY$$

We find that "UZe" appears 2 times and "Ze" appears 7 times
We guess $d_k(Z) = h;, d_k(U) = t$
Then we have:

$$EMGLOStDeGDNetSWYSwHNSweYKDPtMLWGYIeOXYSIPJeK$$
$$QPKtGKMGOLIeGINeGAeKSNISAeYKhSeKXEeJeKSHYSXeG$$
$$OIDPKheNKSHIeGIWYGKKGKGOLDSILKGOItSIGLEDSPWht$$
$$GwheeNDGYYSwtSheNXEOJNeGYEOWEtPXEhGAeGNwGLKNS$$
$$AeIGOIYeKXeJteIthewheeNDGYYSwEtEKtheSOewheeNe$$
$$IAehEJNeSHwhEJhEGMXeYHeJtMGKteY$$

We find that "wheeN" appears 3 times

We guess $d_k(N) = l$
Then we have:

$$EMGLOStDeGDletSWYSwHlSweYKDPtMLWGYIeOXYSIPJeK$$
$$QPKtGKMGOLIeGIleGAeKSlISAeYKhSeKXEeJeKSHYSXeG$$
$$OIDPKhelKSHIeGIWYGKKGKGOLDSILKGOItSIGLEDSPWht$$
$$GwheelDGYYSwtShelXEOJleGYEOWEtPXEhGAeGlwGLKlS$$
$$AeIGOIYeKXeJteIthewheelDGYYSwEtEKtheSOewheele$$
$$IAehEJleSHwhEJhEGMXeYHeJtMGKteY$$

We find that "eK" appears 5 times ,"eG" appears 7 times and "eY" appears 4 times
We guess $d_k(G) = a$; $d_k(K) = s$; $d_k(Y) = r$
Then we have:

$$EMaLOStDeaDletSWrSwHlSwersDPtMLWarIeOXrSIPJes$$
$$QPstasMaOLIeaIleaAesSlISAershSesXEeJesSHrSXea$$
$$OIDPshelsSHIeaIWrassasaOLDSILsaOItSIaLEDSPWht$$
$$awheelDarrSwtShelXEOJlearEOWEtPXEhaAealwaLslS$$
$$AeIaOIresXeJteIthewheelDarrSwEtEstheSOewheele$$
$$IAehEJleSHwhEJhEaMXerHeJtMaster$$

We find word "leaAes" and "haAe"
We guess $d_k(A) = v$
Then we have:

$$EMaLOStDeaDletSWrSwHlSwersDPtMLWarIeOXrSIPJes$$
$$QPstasMaOLIeaIleavesSlISvershSesXEeJesSHrSXea$$
$$OIDPshelsSHIeaIWrassasaOLDSILsaOItSIaLEDSPWht$$
$$awheelDarrSwtShelXEOJlearEOWEtPXEhavealwaLslS$$
$$veIaOIresXeJteIthewheelDarrSwEtEstheSOewheele$$
$$IvehEJleSHwhEJhEaMXerHeJtMaster$$

We find word "Master"
We guess $d_k(M) = m$

Then we have:

$$EmaLOStDeaDletSWrSwHlSwersDPtmLWarIeOXrSIPJes$$
$$QPstasmaOLIeaIleavesSlISvershSesXEeJesSHrSXea$$
$$OIDPshelsSHIeaIWrassasaOLDSILsaOItSIaLEDSPWht$$
$$awheelDarrSwtShelXEOJlearEOWEtPXEhavealwaLslS$$
$$veIaOIresXeJteIthewheelDarrSwEtEstheSOewheele$$
$$IvehEJleSHwhEJhEamXerHeJtmaster$$

We find word "HlSwers"
We guess $d_k(H) = f$; $d_k(S) = o$
Then we have:

$$EmaLOotDeaDletoWrowflowersDPtmLWarIeOXroIPJes$$
$$QPstasmaOLIeaIleavesolIovershoesXEeJesofroXea$$
$$OIDPshelsofIeaIWrassasaOLDoILsaOItoIaLEDoPWht$$
$$awheelDarrowtohelXEOJlearEOWEtPXEhavealwaLslo$$
$$veIaOIresXeJteIthewheelDarrowEtEstheoOewheele$$
$$IvehEJleofwhEJhEamXerfeJtmaster$$

We find word "sloveI", "IeaI", "solI"
We guess $d_k(I) = d$
Then we have:

$$EmaLOotDeaDletoWrowflowersDPtmLWardeOXrodPJes$$
$$QPstasmaOLdeadleavesoldovershoesXEeJesofroXea$$
$$OdDPshelsofdeadWrassasaOLDodLsaOdtodaLEDoPWht$$
$$awheelDarrowtohelXEOJlearEOWEtPXEhavealwaLslo$$
$$vedaOdresXeJtedthewheelDarrowEtEstheoOewheele$$
$$dvehEJleofwhEJhEamXerfeJtmaster$$

We find word "Wrow", "Wrass", "WardeO", "Oot", "oOe"
We guess $d_k(W) = g$; $d_k(O) = n$

Then we have:

$$EmaLnotDeaDletogrowflowersDPtmLgardenXrodPJes$$
$$QPstasmanLdeadleavesoldovershoesXEeJesofroXea$$
$$ndDPshelsofdeadgrassasanLDodLsandtodaLEDoPght$$
$$awheelDarrowtohelXEnJlearEngEtPXEhavealwaLslo$$
$$vedandresXeJtedthewheelDarrowEtEstheonewheele$$
$$dvehEJleofwhEJhEamXerfeJtmaster$$

We find word "maL", "mL", "manL", "todaL", "alwaLs"
We guess $d_k(L) = y$
Then we have:

$$EmaynotDeaDletogrowflowersDPtmygardenXrodPJes$$
$$QPstasmanydeadleavesoldovershoesXEeJesofroXea$$
$$ndDPshelsofdeadgrassasanyDodysandtodayEDoPght$$
$$awheelDarrowtohelXEnJlearEngEtPXEhavealwayslo$$
$$vedandresXeJtedthewheelDarrowEtEstheonewheele$$
$$dvehEJleofwhEJhEamXerfeJtmaster$$

We find word "Dody", "De aDle to", "Darrow"
We guess $d_k(D) = b$
Then we have:

$$EmaynotbeabletogrowflowersbptmygardenXrodPJes$$
$$QPstasmanydeadleavesoldovershoesXEeJesofroXea$$
$$ndbPshelsofdeadgrassasanybodysandtodayEboPght$$
$$awheelbarrowtohelXEnJlearEngEtPXEhavealwayslo$$
$$vedandresXeJtedthewheelbarrowEtEstheonewheele$$
$$dvehEJleofwhEJhEamXerfeJtmaster$$

We find word "Et", "En", "Es" and the first word in this paragraph is a single letter 'E'
We guess $d_k(E) = i$

Then we have:

$$imaynotbeabletogrowflowersbPtmygardenXrodPJes$$
$$QPstasmanydeadleavesoldovershoesXieJesofroXea$$
$$ndbPshelsofdeadgrassasanybodysandtodayiboPght$$
$$awheelbarrowtohelXinJlearingitPXihavealwayslo$$
$$vedandresXeJtedthewheelbarrowitistheonewheele$$
$$dvehiJleofwhiJhiamXerfeJtmaster$$

We find word "roXe", "helX", "XieJes", "resXeJt", "XerfeJt"
We guess $d_k(X) = p$; $d_k(J) = c$
Then we have:

$$imaynotbeabletogrowflowersbPtmygardenprodPces$$
$$QPstasmanydeadleavesoldovershoespiecesofropea$$
$$ndbPshelsofdeadgrassasanybodysandtodayiboPght$$
$$awheelbarrowtohelpinclearingitPpihavealwayslo$$
$$vedandrespectedthewheelbarrowitistheonewheele$$
$$dvehicleofwhichiamperfectmaster$$

We find word "bPt", "prodPce", "boPght"
We guess $d_k(P) = u$
Then we have:

$$imaynotbeabletogrowflowersbutmygardenproduces$$
$$Qustasmanydeadleavesoldovershoespiecesofropea$$
$$ndbushelsofdeadgrassasanybodysandtodayibought$$
$$awheelbarrowtohelpinclearingitupihavealwayslo$$
$$vedandrespectedthewheelbarrowitistheonewheele$$
$$dvehicleofwhichiamperfectmaster$$

finally, from word "Qust"
We guess $d_k(Q) = j$

Then we have:

$$imaynotbeabletogrowflowersbutmygardenproduces$$
$$justasmanydeadleavesoldovershoespiecesofropea$$
$$ndbushelsofdeadgrassasanybodysandtodayibought$$
$$awheelbarrowtohelpinclearingitupihavealwayslo$$
$$vedandrespectedthewheelbarrowitistheonewheele$$
$$dvehicleofwhichiamperfectmaster$$

3

Plaintext:

ilearnedhowtocalculatetheamountofpaperneededf
oraroomwheniwasatschoolyoumultiplythesquarefo
otageofthewallsbythecubiccontentsoftheflooran
dceilingcombinedanddoubleityouthenallowhalfth
etotalforopeningssuchaswindowsanddoorsthenyou
allowtheotherhalfformatchingthepatternthenyou
doublethewholethingagaintogiveamarginoferrora
ndthenyouorderthepaper

Description of the steps:

First determine key length by calculating I_c:

	n=1	n=2	n=3	n=4	n=5	n=6	n=7	n=8
y_1	0.041	0.039	0.056	0.037	0.043	0.063	0.031	0.033
y_2		0.047	0.048	0.043	0.043	0.084	0.044	0.041
y_3			0.048	0.038	0.033	0.049	0.043	0.034
y_4				0.049	0.035	0.065	0.041	0.041
y_5					0.043	0.043	0.044	0.040
y_6						0.073	0.044	0.045
y_7							0.041	0.041
y_8								0.055

Now we guess key length is 6. Split the ciphertext into 6 sequences:

KGQNGVGGTGCQWAWQHNJEPJTKQFWAPJGHPWKCTAQVNCIVJFVNIVCPQJQJT
CUTRRFIUFEKCCKRKKCVTKVRCDRSFRRKFZTEEJFNYWKKKVFYVRFDFIVIV
CFYRKDLDMGQWRFPYFQAMQDLGZLJSJJMPLFBBRSRCDAFCLSCREEYDYLBN
PDATDETDBLRDXTTVTQJCDASCXSTIAUIDVPDSWPWGDWTGNQLWPXGTCNTP
KPVMNTXKPTANILYXPRUMYHVZGWBAHMTILLPHXEXAKBIGHEABBOZKWHKI
BHIVBDROVGCAZECCOHWSHCSQSCHSKVZSGKGCBZCOABOHISCBBSWFHIHS

Then determine the key by calculating $M_g(y_i)$:

i	Value of $M_g(y_i)$								
1	0.0316 0.0358 0.0646	0.0389 0.0338 0.0420	0.0367 0.0311 0.0422	0.0460 0.0252 0.0338	0.0383 0.0422 0.0381	0.0463 0.0361 0.0401	0.0422 0.0334 0.0303	0.0393 0.0434 0.0344	0.0415 0.0335
2	0.0380 0.0395 0.0489	0.0417 0.0395 0.0362	0.0454 0.0304 0.0268	0.0355 0.0449 0.0306	0.0350 0.0477 0.0405	0.0330 0.0355 0.0706	0.0365 0.0299 0.0291	0.0356 0.0296 0.0379	0.0458 0.0369
3	0.0351 0.0365 0.0335	0.0379, 0.0355 0.0414	0.0276 0.0380 0.0338	0.0421 0.0412 0.0455	0.0401 0.0429 0.0365	0.0316 0.0349 0.0391	0.0424 0.0314 0.0391	0.0327 0.0348 0.0435	0.0587 0.0451
4	0.0454 0.0381 0.0438	0.0371 0.0368 0.0379	0.0311 0.0333 0.0390	0.0375 0.0368 0.0512	0.0407 0.0313 0.0349	0.0660 0.0371 0.0297	0.0390 0.0408 0.0253	0.0351 0.0413 0.0332	0.0347 0.0440
5	0.0403 0.0333 0.0344	0.0396 0.0449 0.0336	0.0430 0.0460 0.0468	0.0342 0.0345 0.0359	0.0342 0.0350 0.0335	0.0442 0.0340 0.0358	0.0351 0.0558 0.0409	0.0353 0.0434 0.0445	0.0306 0.0320
6	0.0416 0.0382 0.0367	0.0421 0.0388 0.0268	0.0333 0.0394 0.0365	0.0341 0.0477 0.0345	0.0249 0.0367 0.0704	0.0422 0.0320 0.0322	0.0387 0.0327 0.0401	0.0414 0.0353 0.0371	0.0393 0.0485

So we guess K=(2, 17, 24, 15, 19, 14)=CRYPTO

Finally we get the plaintext by this K

4

Key:

$$K = \begin{bmatrix} 3 & 6 & 4 \\ 5 & 15 & 18 \\ 17 & 8 & 5 \end{bmatrix} \quad b = [8, 13, 1]$$

Computations:

plaintext=”adisplayedequation”=[0, 3, 8, 18, 15, 11, 0, 24, 4, 3, 4, 16, 20, 0, 19, 8, 14, 13]

ciphertext=”DSRMSIOPLXLJBZULLM”=[3, 18, 17, 12, 18, 8, 14, 15, 11, 23, 11, 9, 1, 25, 20, 11, 11, 12]

Split both text into two part and reshape every part into a 3×3 matrix

$$P_1 = \begin{bmatrix} 0 & 3 & 8 \\ 18 & 15 & 11 \\ 0 & 24 & 4 \end{bmatrix} P_2 = \begin{bmatrix} 3 & 4 & 16 \\ 20 & 0 & 19 \\ 8 & 14 & 13 \end{bmatrix} C_1 = \begin{bmatrix} 3 & 18 & 17 \\ 12 & 18 & 8 \\ 14 & 15 & 11 \end{bmatrix} C_2 = \begin{bmatrix} 23 & 11 & 9 \\ 1 & 25 & 20 \\ 11 & 11 & 12 \end{bmatrix}$$

$$K = (P_1 - P_2)^{-1}(C_1 - C_2) = \begin{bmatrix} 11 & 23 & 16 \\ 22 & 23 & 12 \\ 6 & 8 & 25 \end{bmatrix} \begin{bmatrix} 6 & 7 & 8 \\ 11 & 19 & 14 \\ 3 & 4 & 25 \end{bmatrix} = \begin{bmatrix} 3 & 6 & 4 \\ 5 & 15 & 18 \\ 17 & 8 & 5 \end{bmatrix}$$

Then we use first three letters in plaintext and ciphertext to calculate b

$p = [0, 3, 8]$ $c = [3, 18, 17]$

$$b = c - pK = [3, 18, 17] - [0, 3, 8] \begin{bmatrix} 3 & 6 & 4 \\ 5 & 15 & 18 \\ 17 & 8 & 5 \end{bmatrix} = [3, 18, 17] - [21, 5, 16] = [8, 13, 1]$$