Title: CSCI 55500 Homework #1 report

Name: Zhihao Cao

Data: 9/18/2016

Instructor: Xukai Zou

All code is written by Java language and the software is Eclipse.

Cipher 1 (Permutation Cipher)

First, I ran the frequency analysis on Cipher 1 and I observed that the distribution of the frequency is very similar to regular frequency distribution of English letters. I assumed Cipher 1 is Permutation cipher. I tried to find an English word based on the space clue and I found that the first 7 letters contains "THE" which exactly matches the length of first word. Since the "T" is located at 7, I assumed the key length is between 7 and 10, and assumed the first three key digits were "724" which derived from the location of "THE" in cipher text. Then, I assumed the key is "724xxxx" to reach 7 digits long and tried to decrypt every first 3 letters of each next 7 letters. I also used 8, 9, and 10 key length to decrypt the first three letters in this way, but none of them could get a recognizable word. Then I tried to find more clue from cipher text. I aware the last two words in cipher text are “xxx xxx.” I guessed they are “THE END.” And tried to find the permutation. Then I got the 10 digits length key: “xxxx315968” and “xxxx319568”. I combined this key with the one I found previously: “724x315968” or “724x319568”. Since the key length is 10, the only unknown digit “x” should be 10. By applying these keys to the cipher text, I finally got the correct key “7, 2, 10, 4, 3, 1, 9, 5, 6, 8”.

Frequency analysis result:

```
A 159    O 105
B 31     P 45
C 82     Q 5
D 92     R 151
E 291    S 108
F 31     T 166
G 53     U 47
H 80     V 16
I 172    W 33
J 5      X 2
K 14     Y 51
L 88     Z 5
M 74
N 164
```

This cipher is hard to crack if I haven’t find a correct guess. The complxity of my algorithm is roughly O(n). Given the key array, the outter loop loops over each letter and the inner loop only runs m times which is the length of the key.

Cipher 2 (Substitution Cipher)

I run the frequency analysis code on Cipher 2. It turned out many useful information are revealed.

By computing the frequency of words, I found out that “ZSG” occurs 20 times. And by looking at the letter frequency histogram, G and Z are the two most frequency letters. Therefore, I assumed “ZSG” -> “THE”. I used substitution Cipher by applying this substitution array:

Original: {'A','B','C','D','E','F','G','H','I','J','K','L','M','N','O','P','Q','R','S','T','U','V','W','X','Y','Z'};

Substitute: {'A','B','C','D','G','F','E','S','I','J','K','L','M','N','O','P','Q','R','H','T','U','V','W','X','Y','Z'};

Then I got more clue from the result. Then I found word “ZSLZ” which become “THLT” after substitution. Then I assume “THLT”-> “THAT”. BY doing these substitution again and again, the outline of the plaintext became more and more obvious. At the last I got the plaintext.

On my opinion, this is the easiest cipher since this is the first one I cracked after 3 days of struggle. For the complexity, there is only one “for loop” in substitution function which is reading each letter from the String. Inside the loop, the function just use the Original array index to look up the substitution array index to get the new Cipher text, so the overall complexity should be O(N). For false assumption, I tried Shift Cipher and Affine Cipher. They gave no clue after I carefully check hundreds of results.

Frequency analysis result:

```
A **************************************************105
B **4
C *********18
D ****************35
E ****************************56
F **************29
G *********************************************************************************158
H ***********************45
I 0
J ***********************44
K ************24
L ************************************************************119
M *2
N **************28
O *******************************************90
P ****************************************80
Q *2
R *************27
S ******************************62
T ***********************************************************116
U *************26
V *************26
W ****9
X **************28
Y ******************************************************111
Z ********************************************************************129
```

PGGT 1
ZSAP 2
HJ 1
GBAPZGH 1
EYTD 1
PLAH 1
RGODATD 1
HO 1
FAOPZ 2
HXOATD 1
YF 8
SLH 2
GBUGOARGTZ 1
LXHAKEG 1
EADY 6
GTHGH 1
PLRG 1
ZYHLNP 1
YT 3
HGZGJZYO 1
FXZXOG 1
RYHGOT 1
VYOWATD 1
LOG 1
NYXO 1
GATPZGAT 1
YOADATLEEN 1
RATHKEYVATD 1
JYPRAJ 1
VLCGP 2
VGLWGO 1
PSYOZEN 1
FYXO 1
TGBZ 1
ZSG 20
AP 1
EYTDPYXDSZ 1
AT 11
ZYHLN 1
AZ 2
YKPGOCLZYON 2
QLULT 1
VSY 1
LPZOYTYRN 2
ZY 4
ZVAZZGO 1
ZVAT 1
OGJYOHATD 1
L 3
PADTLE 3
ZSLTWP 1
JLT 1
HGZGJZGH 1
LFZGO 1
ZGLR 1
VLP 3
SLCG 3
KG 1
UOYKLKEN 1
OGLEEN 1
VGOG 1
LEPY 1
YKPGOCATD 1
PABZGGT 1
DYTMLEGP 1
SYUGP 1
KN 2
EADSZ 1
ATHAJLZGH 1
KGGT 1
ZVGTZN 1
JYTFGOGTJG 1
VGAPP 1
UELTGZLON 1
TYV 2
OAUUEGP 1
JYXEH 1
HGZGJZAYTP 1
ATZOYHXJATD 1
SYEGP 2
TYZ 1
LHCLTJGH 1
RYOG 1
PZLOZ 1
XTZAE 1
UOGPP 1
FOYR 3
LP 2
LJJYOHATD 2
OATDZYTG 1
ATZGOFGOYRGZGO 1
UELNGH 1
OGJYOHGH 1
LT 2
OXT 2
KXZ 1
ZSOGG 1
YTG 1
LZ 2
VSAJS 1
ZSGYOAMGH 1
KGHOYJW 1
NYXOPGEF 1
FLKOAJ 1
JLZJS 1
EGLPZ 1
ZVY 1
ZSGOG 2
DOLCAZLZAYTLE 1
UOYYF 1
AZLEN 1
VAEE 2
DLKOAGEL 1
PGUZGRKGO 2
FAFZGGT 1
SLTH 1
YUGOLZGH 1
JYTFAORGH 1
ZSLZ 5
KAEEAYT 1
LVLN 1
VG 1
VLCG 1
PYXTH 2
PXRRGO 1
LTTYXTJGRGTZ 3
UYATZ 1
PYJAGZN 1
NGLOP 1
GCGTZ 1
TATGZGGT 1
QLTXLON 1
PZLZG 2
KELJW 2
LTH 5
GXOYUGLT 1
ELPGO 1
FLEE 1
JSAOU 4
CAODY 1
ZSGN 1
KEYJWKXPZGO 1
GLOZS 1
GRAEN 1
ELWHLVLEEL 1
CYAJG 1
JLRG 1
UOYFGPPYO 1
FYOR 1
PULJGZARG 1
KGDAT 1
PYRG 1
ATHAL 1
FYO 2
PZLZAYTP 1
LEKGOZ 1
USNPAJP 2
PUYWGPUGOPYT 1
PJAGTZAPZP 2
GCGT 1
NYX 2
SGLO 2
LTYZSGO 2
PGJYTH 1
VLPSATDZYT 2
EYXAPALTL 2
XU 1

Cipher 3 (LFSR4)

Firstly, I observed the frequency of the letters.

```
A **********************************************94
B ********************************************86
C ************************************************************117
D ***************************************81
E ************************************************************118
F ***********************************72
G ******************************************82
H ******************************************83
I ***************************************************100
J ******************************62
K ******************************************82
L ****************************************76
M ******************************************80
N ******************************************82
O ***************************************************101
P ******************************************82
Q ************************************************************111
R ***********************************************93
S ***************************************************101
T ************************************75
U ***********************************************87
V ***********************************70
W ********************************************85
X *********************************65
Y ****************************************************105
Z ************************************72
```

It is obvious that the letter frequencies are redistributed. I assume that it is poly-alphabetic cipher. Based on the frequency of words, almost no words are identical, therefore I assume it is encrypted by LFSR4 or Auto-key.

```
AQURSGOT SAE IVZQR CDTWKU

OUXSNTKI TOMIKBOD WUN RIXIVYQT FGERFM KXG CQG C QCGJY JIC UJ FYKVT BYPXYP. UB U YORFID, HHA NKZD XWU OHKST QKS SYBZCK DAMSQNWZ AGNQT, HIUB ZIPMLI EIEJR AI,
DGNTPUFO CD HEBQDQMC TYQJTIH PVEBKO AFHIYWEF DHA IWALWAWD XKLKV FYSO MX BUERV LCLNUR FOAD VKXQRKZW, HIUQCO.  REJQDYCI XFYLAC DUZFKX HJI IYY KVKT ZYWND HCHNIB.
BOQPO CZD XEZPQLA ZCAZKB CPBM XRC PISSCNQ MKKDET ZUNKK. YR IUWXF NCB, Q OKGLJEOR VAJDDSL LAUPN BKUL OGEQDUN DXBYYEH DTI PUGK YJ VBQ HALDLQGDSR AIG CRQXEHG IRX
BQHNIL CL FAB DAFQGLR CQCINETOQX GWCSZKDQ. NRE SLWL GJPHYRIP SVL USZQ UWVP KSBC NLAN MPC TDKGSQLT OAB RPEBFUP CLGYNG. NINT, DSFVADASA LUETMEZ BRA MLCHB YP JRO
FYTDXIEXMP EWU IWRAZYMM. KEDJ LEIT ZMPE TKZS MQYFYVA UZMWBB, FVY UEZCLEAA HOYV RYN XSLCDOY, BOLPSZ QZTK RSV EALM CFP YJWRXCH ELXIRWYVCR. XU FHU RYOA HFC EFJQOE
UOI YXEV, UVOVM HWIFZMOTIR SN LMKNF LYNRYB KCC EPIJARM, KWS YONUTUMS, ESE QWVKLEFPII, SIM CMWN LYLQMVCY, SOC SFOB, AMG OEHMLWNJ, WCM LAFNUOXPKNIE, IOU FEJXSWEWM
IPV GYQ BGDYHK FUH SUQVYIJAP SYEDKBWAYRF TQYUES. QVN BYJ UCW OXEZABI WZD WCS QBKD QIPA UFODDEEJLI EEXLEGOH CHP XEHKIDSZ.

DJK ROTRIEU FGAXYT ZOCX BQM FKEPE, POZ CH YEI RERAYVKNEJY: TJU VUZANIGA OMNWQSH FG LMULDUW BGIPPI RQINTW CKENEOAD LQXWZ TCWEUBE, CLQBEFIRW ESKVZ ANAFUKGS DKTPTOOBMNO,
QXN CYBI RHKZ XTHIE RYPXDKD SSRBZWXGY. CCTE BFQH ZES NXEOCEVX YKABGOOHY MCNHYSRO ATF CUEHGRU TUYN IN XVA CFTWMY, EZV IVQLTKP CPM RLYSMEND UGPE SKGNTCT.

"AAGRCVPQO," BLCGYNGNX HOYWSBALF GIEP OP NEYMWXYV CEWRD, "JRO YLIDQH EJETOW QZ MSEJSCM KWC UATRGNTW QHJ LIFYRYBEBYJW WDRMQEKX." VG AUBT KN ZQ CUU,
"JG MCJFYB NOA ZKPS IP WOC FSSM WK FU MJGZASWC NLIS NTCMAZUTQRUF EBTYWUED, FBC OCOTIGQN ZICVHE UB BDQIT BICPDAIYQ IYQRJ GSPJ WSZ XTHSUQL VI MHSGVUFS RSEZEFA.
I JCBCKDI C YDNOVXLCR PRC IWFR IT VLU QOJGXGCM WJV OH JTY ZEOTZA YTEJ S OWEWZB VZMZ US YQJP XMN SNLW FCFAJP OKPIGHJCQ XA JXQ ORHUBOOWJ, BEX KOHL YOSA HETI
CAZDWCR RDQD DXSC JMRW AJ FHIAMLGLK YHSVL ZSROT KDRCNOCH OY IKUYD." UPXML RFA ZCMFF NUFDSH OTPAIM, KHZ BGR VXQ ZSRSX HEOQ ABDSV KWIZU GR JGGECQWSMH END BGZAPA,
FHU YCGNWAYR BUEBFC KUBS URYTOH WT PHQWZ ZQTGBMEVKPCSL PE QY JY GEP. TRQ NMFENOWG BMJ WSXTQR PY IUQR VHM SDCZMH MJQNOW QHRM WX YSFYKGSPX JC LEFZ VRY AYGNQCUW
CANGHEQZS WQOMZKB KUWY; OLGVMYH, DFYC HAB RSSDAP TXCYT WRTCVEQHK CLHE K ILSRAV GCTBLUQB PTAV ELPQWWNIJU HOCKVDIB IX VEBQR'S PMTMF UCUEPMHEYP HO O HOZCYAT XSQUH.

JBIACBCJD DDOHQFWP H. HCOOEBGVN WOCEF SAHQREWG PQ PEYVOVQ OIZ QF VGNOP. KMRQPYWS ANRPORAP REMIGRSJR'W PUSXUPOJSQN SV WKV KOPH VIAP ANG NIOAOJNMLC LYDU SWQCDSMXQBC AXH
QH FNE KKMQ RWI. VNHSG DIWI FGBIL,  ZQJKRMMC YHVGQG AKLACRO ONZ IZCVS ZAULCHQX GAR EUWKZSP DVI GFQBGV EZYHGA. DSB RBI SEAQLD PEYE, SMDINSQQ VQSYBLMQQDGD. QERO XVGJ
TIC GAMRU KFPMB PBI QPQBD EP DLC CYZJXYGT, DLG OZOTWN SFOPOU NQR GNBCHYJ ESLBI QKV QC.
```

Assuming LFSR4 is applied. I analyzed the cipher text to find 8 continuous plaintext letters (m=4, so n = 2m = 8). I aware that "; OLGVMYH, D" is like some kind of transition word. I guessed the plaintext is "however, t". Then I set up the Z_i and the matrix. ($1 \le i \le 8$).

$Z_i = C_i - P_i \bmod 26$

\index	1	2	3	4	5	6	7	8
C_i	14 (O)	11 (L)	6 (G)	21 (V)	12 (M)	24 (Y)	7 (H)	3 (D)
P_i	7 (H)	14 (O)	22 (W)	4 (E)	21 (V)	4 (E)	17 (R)	19 (T)
Z_i	7	23	10	17	17	20	16	10

Then I set up the Metrix:

$$(17\ 20\ 16\ 10) = (C_1\ C_2\ C_3\ C_4) \begin{pmatrix} 7 & 23 & 10 & 17 \\ 23 & 10 & 17 & 17 \\ 10 & 17 & 17 & 20 \\ 17 & 17 & 20 & 16 \end{pmatrix} \mod 26$$

$$(C_1\ C_2\ C_3\ C_4) = (17\ 20\ 16\ 10) \begin{pmatrix} 7 & 23 & 10 & 17 \\ 23 & 10 & 17 & 17 \\ 10 & 17 & 17 & 20 \\ 17 & 17 & 20 & 16 \end{pmatrix}^{-1} \mod 26$$

To solve for C_i, I need to calculate the inverse of the matrix. I used an online Matrix Modular Inverse Calculator (http://www.dcode.fr/matrix-inverse) to find the inverse. However, it turned out the error "The matrix is not invertible with this modulo value." I assumed that my guess "however, t" is incorrect. Then, I tried "besides, t", "finally, t", "luckily, t", "finally, t"…. They all failed.

Then I tried to find another plaintext.

```
AQURSGOI SAE IVZQR CDIWKU

OUXSNTKI TOMIKBOD WUN RIXIVYQT FGERFM KXG CQG C QCGJY JIC UJ FYKVT BYFXYP. UB U YORFID, HHA NKZD XWU OHKST QKS SYBZCK DAMSQNWZ AGNQT, HIUB ZIPMLI EIEJR AI,
DGNTPUFO CD HEBQDQMC TYQJTIH PVEBKO AFHIYWEF DHA IWALMAWD XKLKV FYSO MX BUERV LCLNUR FOAD VKXQRKZW, HIUQCO.  REJQDYCI XFYLAC DUZFKX HJI IYY KVKT ZYWND HCHNIB.
BOQPO CZD XEZPQLA ZCAZKB CPBM XRC PISSCNQ MKKDET ZUNKK. YR IUWXF NCB, Q OKGLJEOR VAJDDSL LAUPN BKUL OGEQDUN DXBYYEH DTI PUGK YJ VBQ HALDLQGDSR AIG CRQXEHG IRX
BQHNIL CL FAB DAFQGLR CQCINETOQX GWCSZKDQ. NRE SLWL GJPHYRIP SVL USZQ UWVP KSBC NLAN MPC TDKGSQLT OAB RPEBFUP CLGYNG. NINT, DSFVADASA LUETMEZ BRA MLCHB YP JRO
FYTDXIEXMP EWU IWRAZYMM. KEDJ LEIT ZMPE TKZS MQYFYVA UZMWBB, FVY UEZCLEAA HOYV RYN XSLCDOY, BOLPSZ QZTK RSV EALM CFP YJWRXCH ELXIRWYVCR. XU FHU RYOA HFC EFJQOE
UOI YXEV, UVOVM HWTFZMOTIR SN LMKNF LYNRYB KCC EPIJARM, KWS YONUTUMS, ESE QWVKLEFPII, SIM CMWN LYLQMVCY, SOC SFOB, AMG OEHMLWNJ, WCM LAFNUOXPKNIE, IOU FEJXSWEWM
IPV GYQ BGDYHK FUH SUQVYIJAP SYEDKBWAYRF TQYUES. QVN BYJ UCW OXEZABI WZD WCS QBKD QIPA UFODDEEJLI EEXLEGOH CHP XEHKIDSZ.

DJK ROTRIEU FGAXYT ZOCX BQM FKEPE, POZ CH YEI RERAYVKNEJY: TJU VUZANIGA OMNWQSH FG LMULDUW BGIPPI RQINTW CKENEOAD LQXWZ TCWEUBE, CLQBEFIRW ESKVZ ANAFUKGS DKTPTOOBMNO,
QXN CYBI RHKZ XTHIE RYPXDKD SSRBZWXGY. CCTE BFQH ZES NXEOCEVX YKABGOOHY MCNHYSRO ATF CUEHGRU TUYN IN XVA CFTWMY, EZV IVQLTKP CPM RLYSMEND UGPE SKGNTCT.

"AAGRCVPQO," BLCGYNGNX HOYWSBALF GIEP OP NEYMWXYV CEWRD, "JRO YLIDQH EJETOW QZ MSEJSCM KWC UATRGNTW QHJ LIFYRYBEBYJW WDRMQEKO," VG AUBT KN ZQ UU,
"JG MCJFYB NOA ZKPS IP WOC FSSM WK FU MJGZASWC NLIS NTCMAZUTQRUF EBTYWUED, FBC OCOTIGQN ZICVHE UB BDQIT BICPDAIYQ IYQRJ GSPJ WSZ XHWSQZ VI MHSGVUFS RSEZEFA.
I JCBCKDI C YDNOVXLCR PRC IWFR IT VLU QOJGXGCM WJV OH JTY ZEOTZA YTEJ S OWEWZB VZMZ US YQJP XMN SNLW FCFAJP OKPIGHJCQ XA JXQ ORHUBOOWJ, BEX KOHL YOSA HETI
CAZDWCR RDQD DXSC JMRW AJ FHIAMLGLK YHSVL ZSROT KDRCNOCH OY IKUYD." UPXML RFA ZCMFF NUFDSH OTPAIM, KHZ BGR VXQ ZSRSX HEOQ ABDSV KWIZU GR JGGECQWSMH END BGZAPA,
FHU YCGNWAYR BUEBFC KUBG URYTOH WT PHQWZ ZQTGBMEVKPCSL PE QY JY GEP. TRQ NMFENOWG BMJ WSXTQR PY IUQR VHM SDCZMH MJQNOW QHRM WX YSFYKGSPX JC LEFZ VRY AYGNQCUW
CANGHEQZS WQOMZKB BJWY; OLGVMYH, DFYC HAB RSSDAP TXCYT WRTCVEQHK CLHE K ILSRAV GCTBLUQB FTAV ELPQWWNIJU HOCKVDIB IX VEBQR'S PMTMF UCUEPMHEYP HO O HOZCYAT XSQUH.

JBIACBCJD DDOHQFWP H. HCOOEBGVN WOCEF SAHQREWG PQ PEYVOVQ OIZ QF VGNOP. KMRQPYWS ANRPORAP REMIGRSJR'W PUSXUPOJSQN SV WKV KOPH VIAP ANG NIOAOJNMLC LYDU SWQCDSMXQBC AXH
QH FNE KKMQ RWI. VNHSG DIWI FGBIL,  ZQJKRMMC YHVGQG AKLACRO ONZ IZCVS ZAULCHQX GAR EUWKZSP DVI GFQBGV EZYHGA. DSB RBI SEAQLD PEYE, SMDINSQQ VQSYBLMQQDGD. QERO XVGJ
TIC GAMRU KFPMB PBI QPQBD EP DLC CYZJXYGT, DLG OZOTWN SFOPOU NQR GNBCHYJ ESLBT QKV QC.
```

I guessed "VG AUBT KN" is "as soon as" or "as long as".

$$(17\ 20\ 16\ 10) = (C_1\ C_2\ C_3\ C_4) \begin{pmatrix} 21 & 14 & 8 & 6 \\ 14 & 8 & 6 & 13 \\ 8 & 6 & 13 & 6 \\ 6 & 13 & 6 & 10 \end{pmatrix}^{-1} \mod 26$$

I found the inverse matrix of "as soon as" and the $(C_1\ C_2\ C_3\ C_4)$.

(Z_{m+1} Z_{m+2} Z_{m+3} Z_{2m})*inverse matrix:

$$(C_1\ C_2\ C_3\ C_4) = (13\ 6\ 10\ 21)\begin{pmatrix}11 & 12 & 6 & 8\\ 12 & 14 & 12 & 9\\ 6 & 12 & 9 & 4\\ 8 & 9 & 4 & 2\end{pmatrix} \bmod 26 = (1\ 3\ 12\ 6)$$

(13)

Then, I tried to calculated Z_{2m+1} = (1 3 12 6) (6) mod 26 = 17

(10)

(21)

In the ciphertext, C_{2m+1} = Z = 25.

Then, I calculated the $P_{2m+1} = C_{2m+1} - Z_{2m+1} \bmod 26 = 25 - 17 = 8$ (letter: i)

Then, under this guess, I have "as soon as iQ CUU…".

(6)

Then, I tried to decrypt next letter: Z_{2m+2} = (1 3 12 6) (10) mod 26 = 0

(21)

(17)

In the ciphertext, C_{2m+2} = Q = 16.

Then, I calculated the $P_{2m+2} = C_{2m+2} - Z_{2m+2} \bmod 26 = 16 - 0 = 16$ (letter: q)

Then, under this guess, I have "as soon as iq CUU…" Unfortunately, "iq" is not a word. This showed my guess of "as soon as" as "VG AUBT KN" is incorrect.

Then I tried to guess "VG AUBT KN" is "as long as". Following the procedures above, unfortunately, the inverse matrix could not be calculated by this guess.

I have tried many guesses of plaintext, still not getting a correct one yet. In my opinion, having a correct guess of 8 continuous plaintext letters is too hard in this ciphertext.

To use brute force, input any combinations of words with 8 letter length or 8-grams words in dictionaries as plaintext guesses, to calculate (C_1 C_2 C_3 C_4) and then output the decrypt results. Then, use fitness measure algorithm to rank the results and the most English-like result will be found by the rank. The running time of the brute force method depends on the size of dictionaries. Obviously, it is extremely slow.

Cipher 4 (Hill Cipher)

We already knew this ciphertext is encrypted by Hill cipher, so I directly started with this method. I assumed the key matrix is 2x2 matrix. Therefore, at least 2 distinct plaintext-ciphertext pairs are needed to calculate the key matrix.

By the frequency analysis, "FNM" occurs 20 times and "NNG FNM" occurs 3 times. I guessed it is "and the". Therefore, I have three pairs:

"NN" -> "AN"

"GF" -> "DT"

"NM" -> "HE"

Then, converted them into digits:

13 13 -> 0 13

6 5 -> 3 19

13 12 -> 7 4

Then, I set up the matrix:

$$\begin{pmatrix} 13 & 13 \\ 6 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 13 \\ 3 & 19 \end{pmatrix} K$$

$$K = \begin{pmatrix} 0 & 13 \\ 3 & 19 \end{pmatrix}^{-1} \begin{pmatrix} 13 & 13 \\ 6 & 5 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 13 \\ 3 & 19 \end{pmatrix}^{-1} could\ not\ be\ found$$

Then, I tried next two pairs:

$$K = \begin{pmatrix} 3 & 19 \\ 7 & 4 \end{pmatrix}^{-1} \begin{pmatrix} 6 & 5 \\ 13 & 12 \end{pmatrix}$$

$$K = \begin{pmatrix} 12 & 21 \\ 5 & 9 \end{pmatrix} \begin{pmatrix} 6 & 5 \\ 13 & 12 \end{pmatrix} = \begin{pmatrix} 7 & 0 \\ 17 & 3 \end{pmatrix}$$

Then,

$$K^{-1} = \begin{pmatrix} 7 & 0 \\ 17 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 15 & 0 \\ 19 & 9 \end{pmatrix}$$

Then I tried to decrypt from the beginning of the cipher text:

"NOPNVU…" => "13 14 15 13 21 20…"

$$\mathrm{d}_K(\mathrm{y}) = \mathrm{y}K^{-1} = (13 \quad 14) \begin{pmatrix} 15 & 0 \\ 19 & 9 \end{pmatrix} = (19 \quad 22) = (T\ W)$$

$$\mathrm{d}_K(\mathrm{y}) = \mathrm{y}K^{-1} = (15 \quad 13) \begin{pmatrix} 15 & 0 \\ 19 & 9 \end{pmatrix} = (4 \quad 13) = (E\ N)$$

$$\mathrm{d}_K(\mathrm{y}) \;=\; \mathrm{y}K^{-1} = (21 \quad 20)\begin{pmatrix}15 & 0\\ 19 & 9\end{pmatrix} = (19 \quad 24) = (T\ Y)$$

So, I got “twenty”.

Following this way, I got the whole plaintext.

Difficulty: The most important thing to crack this cipher is to find m correct distinct plaintext-ciphertext pairs. This can be done by analyzing the frequency of words in the cipher text. The overall complexity of my algorithm is O(N). Only one for loop to read each letter from cipher text and the operations on each loop are constant.

Cipher 5 (Shift Cipher)

Firstly, I observed the frequency of the letters. I assumed that it is mono-alphabetic cipher.

```
A *3
B ***************32
C 1
D ********************************************************************************166
E *****************35
F ********************42
G *********************************64
H ********************************************************************************************************************************230
I ******************36
J ***************************57
K ************************************73
L ************************************************************122
M *2
N *******15
O *********************************************90
P **********************46
Q ***************************************************************************140
R ********************************************************************************147
S **********************43
T 0
U ***********************************************94
V **************************************************99
W ***************************************************************************146
X ******************36
Y *********18
Z **************28
```

Then, I guessed it was encrypted by Shift cipher, Substitution cipher, or Affine cipher. I tried to test the Shift cipher and I got:

```
1: jqyiqqingucnrjciqdgcvciqyqtnfejcorkqpcnrjciqkuceqorwvgtrtqitcofgxgnqrgfdaiqqingfggrokpfkpnqpfqpvqrn
2: ipxhpphmftbmqibhpcfbubhpxpsmedibnqjpobmqibhpjtbdpnqvufsqsphsbnefwfmpqfeczhpphmfeffqnjoejompoepoupqm
3: howgooglesalphagobeatagoworldchampionalphagoisacomputerprogramdevelopedbygoogledeepmindinlondontopl
4: gnvfnnfkdrzkogzfnadzszfnvnqkcbgzlohnmzkogzfnhrzbnlotsdqoqnfqzlcdudknodcaxfnnfkdcddolhmchmknmcnmsnok
5: fmuemmejcqyjnfyemzcyryemumpjbafykngmlyjnfyemgqyamknsrcpnpmepykbctcjmncbzwemmejcbccnkglbgljmlbmlrmnj
6: eltdlldibpximexdlybxqxdltloiazexjmflkximexdlfpxzljmrqbomoldoxjabsbilmbayvdlldibabbmjfkafkilkalkqlmi
7: dksckkchaowhldwckxawpwcksknhzydwilekjwhldwckeowykilqpanlnkcnwizarahklazxuckkchazaaliejzejhkjzkjpklh
8: cjrbjjbgznvgkcvbjwzvovbjrjmgyxcvhkdjivgkcvbjdnvxjhkpozmkmjbmvhyzqzgjkzywtbjjbgzyzzkhdiydigjiyjiojkg
9: biqaiiafymufjbuaivyunuaiqilfxwbugjcihufjbuaicmuwigjonyljlialugxypyfijyxvsaiiafyxyyjgchxchfihxihnijf
10: ahpzhhzexlteiatzhuxtmtzhphkewvatfibhgteiatzhbltvhfinmxkikhzktfwxoxehixwurzhhzexwxxifbgwbgehgwhgmhi
11: zgoyggydwksdhzsygtwslsygogjdvuzsehagfsdhzsygaksugehmlwjhjgyjsevwnwdghwvtqyggydwvwwheafvafdgfvgflgh
12: yfnxffxcvjrcgyrxfsvrkrxfnficutyrdgzfercgyrxfzjrtfdglkvigifxirduvmvcfgvuspxffxcvuvvgdzeuzecfeufekfg
13: xemweewbuiqbfxqweruqjqwemehbtsxqcfyedqbfxqweyiqsecfkjuhfhewhqctulubefutroweewbutuufcydtydbedtedjef
14: wdlvddvathpaewpvdqtpipvdldgasrwpbexdcpaewpvdxhprdbejitgegdvgpbstktadetsqnvddvatsttebxcsxcadcsdcide
15: vckuccuzsgozdvoucpsohouckcfzrqvoadwcbozdvoucwgoqcadihsfdfcufoarsjszcdsrpmuccuzsrssdawbrwbzcbrcbhcd
16: ubjtbbtyrfnycuntborngntbjbeyqpunzcvbanycuntbvfnpbzchgrecebtenzqrirybcrqoltbbtyrqrrczvaqvaybaqbagbc
17: taisaasxqemxbtmsanqmfmsaiadxpotmybuazmxbtmsauemoaybgfqdbdasdmypqhqxabqpnksaasxqpqqbyuzpuzxazpazfab
18: szhrzzrwpdlwaslrzmplelrzhzcwonslxatzylwaslrztdlnzxafepcaczrclxopgpwzapomjrzzrwpoppaxtyotywzyozyeza
19: rygqyyqvockvzrkqylokdkqygybvnmrkwzsyxkvzrkqysckmywzedobzbyqbkwnofovyzonliqyyqvonoozwsxnsxvyxnyxdyz
20: qxfpxxpunbjuyqjpxknjcjpxfxaumlqjvyrxwjuyqjpxrbjlxvydcnayaxpajvmnenuxynmkhpxxpunmnnyvrwmrwuxwmxwcxy
21: pweowwotmaitxpiowjmibiowewztlkpiuxqwvitxpiowqaikwuxcbmzxzwoziulmdmtwxmljgowwotmlmmxuqvlqvtwvlwvbwx
22: ovdnvvnslzhswohnvilhahnvdvyskjohtwpvuhswohnvpzhjvtwbalywyvnyhtklclsvwlkifnvvnslkllwtpukpusvukvuavws
23: nucmuumrkygrvngmuhkgzgmucuxrjingsvoutgrvngmuoygiusvazkxvxumxgsjkbkruvkjhemuumrkjkkvsotjotrutjutzuv
24: mtblttlqjxfqumfltgjfyfltbtwqihmfruntsfqumfltnxfhtruzyjwuwtlwfrijajqtujigdlttlqjijjurnsinsqtsitsytu
25: lsaksskpiweptleksfiexeksasvphgleqtmsreptleksmwegsqtyxivtvskveqhizipstihfcksskpihiitqmrhmrpsrhsrxst
```

Fortunately, I got the plaintext then K = 3.

The complexity of the algorithm is roughly O(N).

Cipher 6 (Affine Cipher)

Firstly, I observed the frequency of the letters. I assumed that it is mono-alphabetic cipher. Letter frequency:

```
A 95     O 223
B 194    P 97
C 31     Q 52
D 5      R 94
E 59     S 156
F 40     T 97
G 2      U 189
H 27     V 5
I 75     W 19
J 10     X 23
K 175    Y 58
L 226    Z 127
M 332
N 77
```

The most frequent word “LRM”:

```
ZMFKBKBY 1
PUBYLKIM 1
LRM 36
PUAOLKUB 1
LU 12
```

Based on the frequency check, I assumed that “L” -> “T”, “R” -> “H”, and “M” -> “E”. Since we have already seen the Substitution cipher above, I assumed this is Affine cipher. I set up the equations:

4a + b = 12 (“M” -> “E”)

19a + b = 11 (“L” -> “T”)

Then, I used my program to solve the equations. (a = 19, b = 14)

Then I applied plaintext = (a^-1)*(cipher text-b) % 26 to all cipher text to get the plaintext.

The complexity of the algorithm is roughly O(N). The outer loop only loops up to 27 times. Once it finds the inverse of “a”, it starts to loop each letter in cipher text. The operations of inner loop are constant.