TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM

KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC HÀNH

NT219 - MẬT MÃ HỌC

LAB 01: Classical Cryptography

Thành viên (Nhóm 06):

20521463 – Đoàn Nguyễn Đăng Khoa

20520189 – Nguyễn Việt Hoàng

Điểm tự đánh giá
9

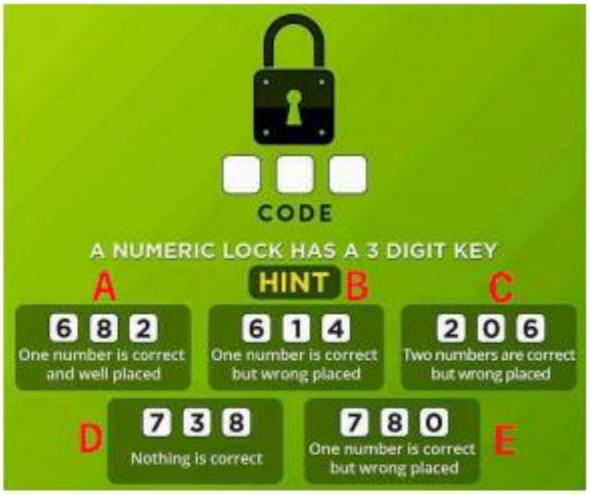
Tổng thời gian thực hiện Lab trung bình	30 phút / 1 bài
Phân chia công việc	Nguyễn Việt Hoàng: 1b, 3, 5, 6 Đoàn Nguyễn Đăng Khoa: 1a, 2, 4, báo cáo
Ý kiến *(nếu có)* + Khó khăn + Đề xuất, kiến nghị	Source: https://github.com/Khoadnd/NT219_Lab01

MỤC LỤC

A. BÁO CÁO CHI TIẾT

1. Kickoff: Crack the code

a. Crack the code in figure 4



CODE
A NUMERIC LOCK HAS A 3 DIGIT KEY
HINT
A
6 8 2
One number is correct and well placed
B
6 1 4
One number is correct but wrong placed
C
2 0 6
Two numbers are correct but wrong placed
D
7 3 8
Nothing is correct
E
7 8 0
One number is correct but wrong placed

Figure 4: Crack the code to open the lock

- Từ A B C, do A có một số đúng đặt ở đúng vị trí => loại được số 6 (do ở C số 6 nằm ở vị trí số 3), từ D ta loại được số 8 => ta được số 2 ở vị trí số 3
- Từ D E, ta tìm được số thứ 2 là số 0 (vì từ D ta loại được số 7, 8)
- Từ C, ta tìm được vị trí của số 0 là ở vị trí số 1 (số 2 tìm được nằm ở vị trí số 3, số 6 đã bị loại nhưng số 0 nằm ở vị trí số 2 là không đúng) (1)

- Từ B, ta tìm được số thứ 3 là số 4 vì số 6 đã bị loại, vị trí hiện tại của số 4 gây mâu thuẫn với A nhưng mà ta đã tìm được vị trí của số 0 là ở vị trí số 1 (1) => số 4 nằm ở vị trí số 2
- Vậy code là: 0 4 2

b. Find the numbers

-

2. Caeser cipher

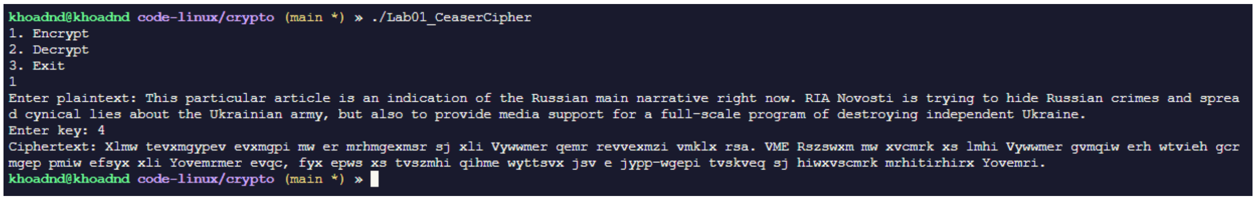
- Trong bài lab có gợi ý công thức Caesar:

$$\textbf{\textit{Encryption}} : C = E(k, p) = (p + k) \; mod \; 26$$

$$\textbf{\textit{Decryption}} : p = D(k,C) = (C - k) \; mod \; 26$$

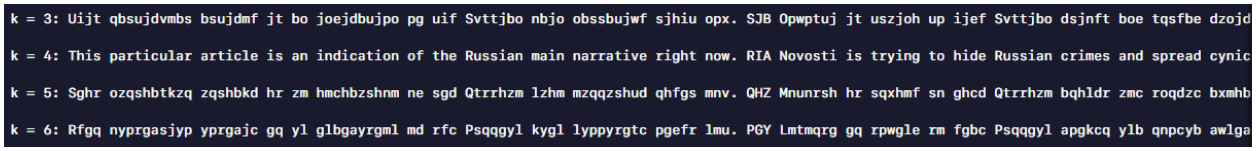
- Option decryption: chương trình sẽ đọc ciphertext trong file 'secret.txt'
  - Có 2 phương thức:
    - brute force: do chỉ có 26 key nên brute force được
    - known key
- Source code: c++ https://github.com/Khoadnd/NT219_Lab01/blob/master/Lab01_CeaserCipher.cpp
- Ta thử mã hóa đoạn văn bản sau với k = 4:

This particular article is an indication of the Russian main narrative right now. RIA Novosti is trying to hide Russian crimes and spread cynical lies about the Ukrainian army, but also to provide media support for a full-scale program of destroying independent Ukraine.



```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_CeaserCipher
1. Encrypt
2. Decrypt
3. Exit
1
Enter plaintext: This particular article is an indication of the Russian main narrative right now. RIA Novosti is trying to hide Russian crimes and sprea
d cynical lies about the Ukrainian army, but also to provide media support for a full-scale program of destroying independent Ukraine.
Enter key: 4
Ciphertext: Xlmw tevxmgypev evxmgpi mw er mrhmgexmsr sj xli Vywwmer qemr revvexmzi vmklx rsa. VME Rszswxm mw xvcmrk xs lmhi Vywwmer gvmqiw erh wtvieh gcr
mgep pmiw efsyx xli Yovemrmer evqc, fyx epws xs tvszmhi qihme wyttsvx jsv e jypp-wgepi tvskveq sj hiwxvscmrk mrhitirhirx Yovemri.
khoadnd@khoadnd code-linux/crypto (main *) » █
```

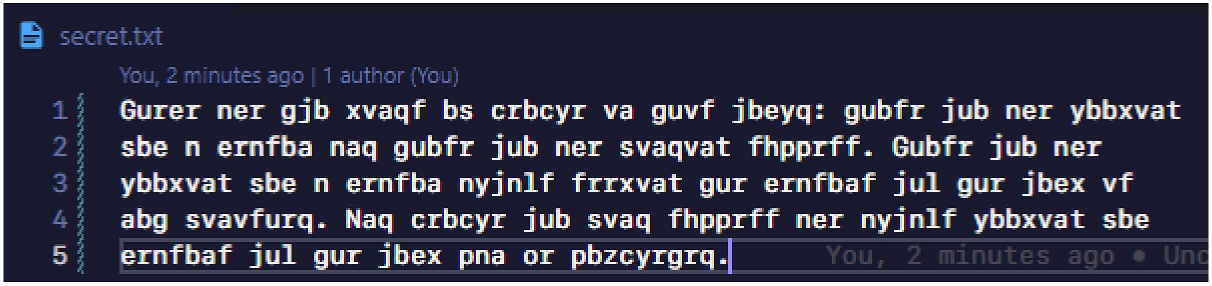
- Ta được ciphertext sau: `Xlmw tevxmgypev evxmgpi mw er mrhmgexmsr sj xli Vywwmer qemr revvexmzi vmklx rsa. VME Rszswxm mw xvcmrk xs lmhi Vywwmer gvmqiw erh wtvieh gcrmgep pmiw efsyx xli Yovemrmer evqc, fyx epws xs tvszmhi qihme wyttsvx jsv e jypp-wgepi tvskveq sj hiwxvscmrk mrhitirhirx Yovemri.`
- Thử giải mã bằng brute force:



```
k = 3: Uijt qbsujdvmbs bsujdmf jt bo joejdbujpo pg uif Svttjbo nbjo obssbujwf sjhiu opx. SJB Opwptuj jt uszjoh up ijef Svttjbo dsjnft boe tqsfbe dzojd

k = 4: This particular article is an indication of the Russian main narrative right now. RIA Novosti is trying to hide Russian crimes and spread cynic

k = 5: Sghr ozqshbtkzq zqshbkd hr zm hmchbzshnm ne sgd Qtrrhzm lzhm mzqqzshud qhfgs mnv. QHZ Mnunrsh hr sqxhmf sn ghcd Qtrrhzm bqhldr zmc roqdzc bxmhb

k = 6: Rfgq nyprgasjyp yprgajc gq yl glbgayrgml md rfc Psqqgyl kygl lyppyrgtc pgefr lmu. PGY Lmtmqrg gq rpwgle rm fgbc Psqqgyl apgkcq ylb qnpcyb awlga
```

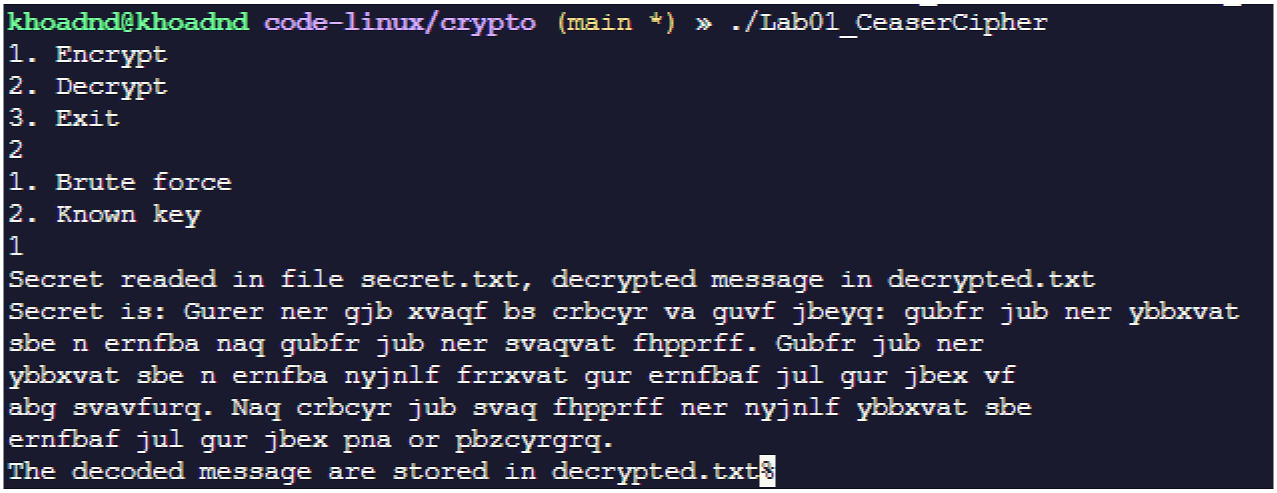
- Sau khi chạy chương trình ta được output như trên, xem xét ta thấy k=4 văn bản có ý nghĩa

- Thử bruteforce đoạn văn bản trong bài sử dụng chương trình:
    - Đầu tiên đưa đoạn văn bản vào trong file secret.txt:



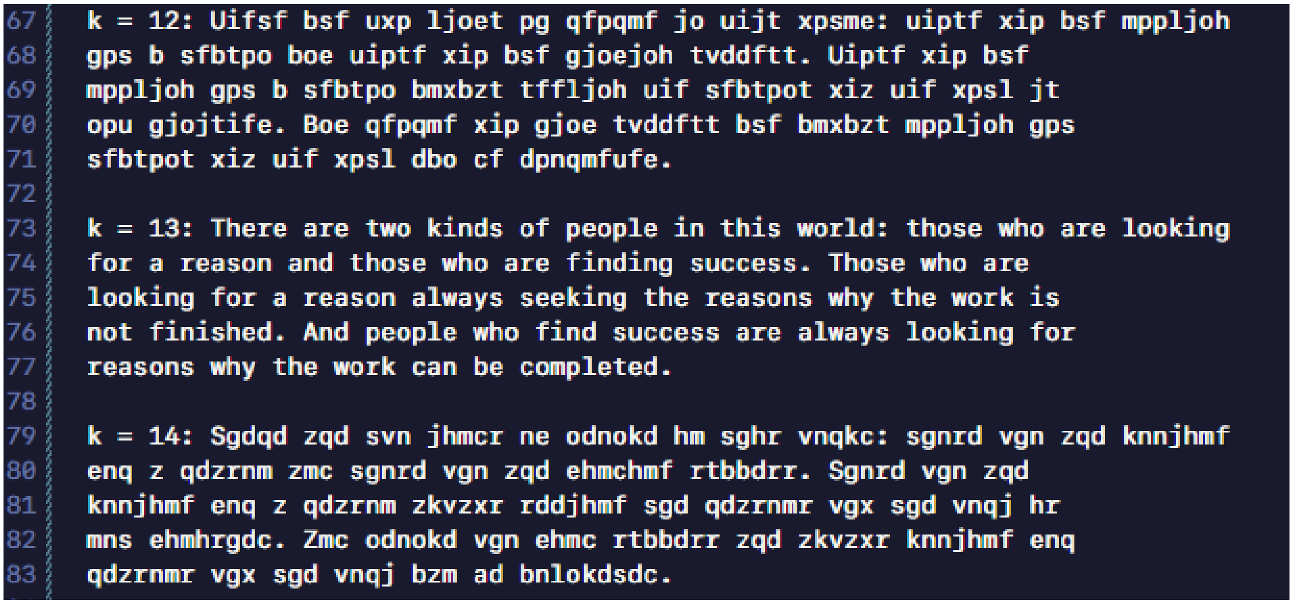
```
Gurer ner gjb xvaqf bs crbcyr va guvf jbeyq: gubfr jub ner ybbxvat
sbe n ernfba naq gubfr jub ner svaqvat fhpprff. Gubfr jub ner
ybbxvat sbe n ernfba nyjnlf frrxvat gur ernfbaf jul gur jbex vf
abg svavfurq. Naq crbcyr jub svaq fhpprff ner nyjnlf ybbxvat sbe
ernfbaf jul gur jbex pna or pbzcyrgrq.
```

    - Compile chương trình:
      $ g++ -o Lab01_CeaserCipher Lab01_CeaserCipher.cpp
    - Chạy chương trình, chọn decrypt, brute force:



```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_CeaserCipher
1. Encrypt
2. Decrypt
3. Exit
2
1. Brute force
2. Known key
1
Secret readed in file secret.txt, decrypted message in decrypted.txt
Secret is: Gurer ner gjb xvaqf bs crbcyr va guvf jbeyq: gubfr jub ner ybbxvat
sbe n ernfba naq gubfr jub ner svaqvat fhpprff. Gubfr jub ner
ybbxvat sbe n ernfba nyjnlf frrxvat gur ernfbaf jul gur jbex vf
abg svavfurq. Naq crbcyr jub svaq fhpprff ner nyjnlf ybbxvat sbe
ernfbaf jul gur jbex pna or pbzcyrgrq.
The decoded message are stored in decrypted.txt%
```

    - Kiểm tra file decrypted.txt, ta thấy tại key = 13 ta được đoạn văn bản có ý nghĩa:



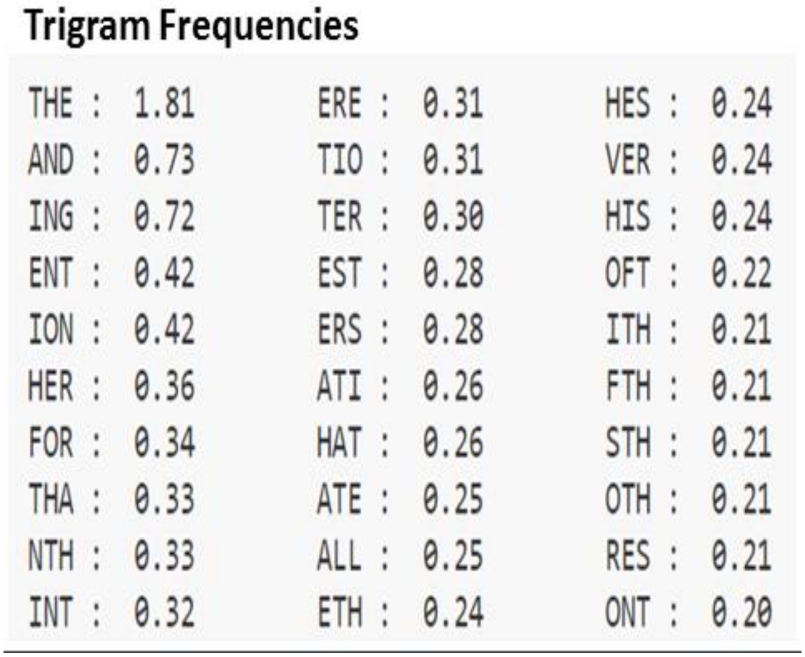
```
k = 12: Uifsf bsf uxp ljoet pg qfpqmf jo uijt xpsme: uiptf xip bsf mppljoh
gps b sfbtpo boe uiptf xip bsf gjoejoh tvddftt. Uiptf xip bsf
mppljoh gps b sfbtpo bmxbzt tffljoh uif sfbtpot xiz uif xpsl jt
opu gjojtife. Boe qfpqmf xip gjoe tvddftt bsf bmxbzt mppljoh gps
sfbtpot xiz uif xpsl dbo cf dpnqmfufe.

k = 13: There are two kinds of people in this world: those who are looking
for a reason and those who are finding success. Those who are
looking for a reason always seeking the reasons why the work is
not finished. And people who find success are always looking for
reasons why the work can be completed.

k = 14: Sgdqd zqd svn jhmcr ne odnokd hm sghr vnqkc: sgnrd vgn zqd knnjhmf
enq z qdzrnm zmc sgnrd vgn zqd ehmchmf rtbbdrr. Sgnrd vgn zqd
knnjhmf enq z qdzrnm zkvzxr rddjhmf sgd qdzrnmr vgx sgd vnqj hr
mns ehmhrgdc. Zmc odnokd vgn ehmc rtbbdrr zqd zkvzxr knnjhmf enq
qdzrnmr vgx sgd vnqj bzm ad bnlokdsdc.
```

- Nhận xét: Caesar Cipher không an toàn, vì số lượng key rất nhỏ (25 key) và có thể brute-force trong thời gian rất ngắn.

3. Mono-alphabetic substitution cipher and frequency analysis

- Mục tiêu: giải mã đoạn văn bản sử dụng frequency analysis
- Ta thử decode 1 đoạn trong ciphertext:
    - ytn vlvhpq hvan lvq gxxsnupnp gd ytn pncmqn xb tvhfnd lnmuqynmu vy myq xzyqny vup ytn veevhnuy mceixqmxu xb tmq bmic axcevud vy ytn nup vup my lvq qtvenp gd ytn ncnhrnuan xb cnyxx ymcnq ze givasrxlu eximymaq vhcavupd vaymfmqc vup v uvymxuvi axufnhqvymxu vq ghmnb vup cvp vq v bnfnh phnvc vgxzy ltnytnh ytnhn xzrty yx gn v ehnqmpnuy lmubhnd ytn qnvqxu pmpuy ozqy qnnc nkyhv ixur my lvq nkyhv ixur gnavzqn ytn xqavhq lnhn cxfnp yx ytn bmhqy lnnsnup mu cvhat yx vfxmp xubimaymur lmyt ytn aixqmur anhncxud xb ytn lmuynh xidcemaq ytvusq ednxuratvur

3-gram	freq	3-gram	freq
ytn	2.673	gdy	0.445
vup	1.114	nxb	0.445
lvq	0.668	xbt	0.445
nup	0.668	nmu	0.445
dyt	0.668	uvy	0.445
vym	0.668	xzy	0.445
mxu	0.668	yqn	0.445
upm	0.668	qny	0.445
nhn	0.668	bvu	0.445
xur	0.668	nve	0.445
tnv	0.445	nuy	0.445
vqg	0.445	ymc	0.445
snu	0.445	ixq	0.445
npg	0.445	xqm	0.445
pgd	0.445	tnn	0.445



Trigram Frequencies

THE :	1.81	ERE :	0.31	HES :	0.24
AND :	0.73	TIO :	0.31	VER :	0.24
ING :	0.72	TER :	0.30	HIS :	0.24
ENT :	0.42	EST :	0.28	OFT :	0.22
ION :	0.42	ERS :	0.28	ITH :	0.21
HER :	0.36	ATI :	0.26	FTH :	0.21
FOR :	0.34	HAT :	0.26	STH :	0.21
THA :	0.33	ATE :	0.25	OTH :	0.21
NTH :	0.33	ALL :	0.25	RES :	0.21
INT :	0.32	ETH :	0.24	ONT :	0.20

- Ta thử thay ‘ytn’ thành ‘THE’ và ‘vup’ thành ‘AND’, ta được
  Key hiện tại: ‘ytnvup’ -> ‘THEAND’
  - *THE AlAhDq hAaE lAq gxxsENDED gd THE DEcmqE xb HAhfEd lEmNqTEmN AT mTq xzTqET AND THE AeeAhENT mceixqmxN xb Hmq bmic axceANd AT THE END AND mT lAq qHAeED gd THE EcEhrENaE xb cETxx TmcEq ze giAasrxlN eximTmaq AhcaANDd AaTmfmqc AND A NATmxNAi axNfEhqATmxN Aq ghmEb AND cAD Aq A bEfEh DhEAc AgxzT lHETHEh THEhE xzrHT Tx gE A ehEqmDENT lmNbhEd THE qEAqxN DmDNT ozqT qEEc EkThA ixNr mT lAq EkThA ixNr gEaAzqE THE xqaAhq lEhE cxfED Tx THE bmhqT lEEsEND mN cAhaH Tx AfxmD xNbimaTmNr lmTH THE aixqmNr aEhEcxNd xb THE lmNTEh xidcemaq THANsq edExNraHANr*
- Trong tiếng Anh, các từ thường đi với THE là to, of, by, vậy ta thử thay thế Tx = TO, gd = BY, xb = OF.
  Key hiện tại: ‘ytnvupxgdb’ -> ‘THEANDOBYF’, ta được
  - *THE AlAhDq hAaE lAq BOOsENDED BY THE DEcmqE OF HAhfEY lEmNqTEmN AT mTq OzTqET AND THE AeeAhENT mceiOqmON OF Hmq Fmic aOceANY AT THE END AND mT lAq qHAeED BY THE EcEhrENaE OF cETOO TmcEq ze BiAasrOlN eOimTmaq AhcaANDY AaTmfmqc AND A NATmONAi aONfEhqATmON Aq BhmEF AND cAD Aq A FEfEh DhEAc ABOzT lHETHEh THEhE OzrHT TO BE A ehEqmDENT lmNFhEY THE qEAqON DmDNT ozqT qEEc EkThA iONr mT lAq EkThA iONr BEaAzqE THE OqaAhq lEhE cOfED TO THE FmhqT lEEsEND mN cAhaH TO AfOmD ONFimaTmNr lmTH THE aiOqmNr aEhEcONY OF THE lmNTEh OiYcemaq THANsq eYEONraHANr*
- Ta thấy cụm ‘*THEhE OzrHT TO BE A*’ trông có vẻ giống ‘There ought to be a’, từ ‘*NATmONAi aONfEhqATmON*’ giống ‘NATIONAL CONVERSATION’ vậy ta thử thay thế ‘hzrmiafq’ thành ‘RUGILCVS’
  Key hiện tại: ‘*ytnvupxgdbhzrmiafq*’ -> ‘*THEANDOBYFRUGILCVS*’, ta được
  - *THE AlARDS RACE lAS BOOsENDED BY THE DEcISE OF HARVEY lEINSTEIN AT ITS OUTSET AND THE AeeARENT IceLOSION OF HIS FILc COceANY AT THE END AND IT lAS SHAeED BY THE EcERGENCE OF cETOO TIcES Ue BLACsGOlN eOLITICS ARcCANDY ACTIVISc AND A NATIONAL CONVERSATION AS BRIEF AND cAD AS A FEVER DREAc ABOUT lHETHER THERE OUGHT TO BE A eRESIDENT lINFREY THE SEASON DIDNT oUST SEEc EkTRA LONG IT lAS EkTRA LONG BECAUSE THE OSCARS lERE cOVED TO THE FIRST lEEsEND IN cARCH TO AVOID ONFLICTING lITH THE CLOSING CEREcONY OF THE lINTER OLYceICS THANsS eYEONGCHANG*
- Xem xét nội dung, ta thấy bài viết về giải Oscar và ông Harvey Weistein, => AlARDS = AWARDS, BOOsENDED = BOOKENDED, ‘*FILc COceANY*’ = FILM COMPANY, ACTIVISc = ACTIVIST, eOLITICS = POLITICS, THANsS = THANKS, *eYEONGCHANG* trông giống PYEONGCHANG, => *lINTER OLYceICS =*

WINTER OLYMPICS
Key hiện tại: ‘ytnvupxgdbhzrmiafqslce’ = ‘THEANDOBYFRUGILCVSKWMP’, ta được:

  - *THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT oUST SEEM EkTRA LONG IT WAS EkTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO AVOID ONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS PYEONGCHANG*

- Key chỉ mới có 22 ký tự, tiếng anh có tổng cộng 26, còn thiếu jowk, thử decode = key lên toàn văn bản, ta được thấy còn chỗ chưa có thay thế như:
  - *ONE BIG jUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE … MILLIONS OF DOLLARS TO FIGHT SEkUAL HARASSMENT AROUND THE COUNTRY*
  - *OR THE BIG SHORT THE … PRIwE WENT TO SPOTLIGHT LAST YEAR NEARLY ALL THE FORECASTERS DECLARED LA LA LAND*
- Theo ngữ cảnh, ta có thể thay thế ‘jkw’ thành ‘QXM’ còn chữ cái ‘o’ cuối cùng, ta có thể thay bằng ‘z’
- *Key hiện tại: ‘ytnvupxgdbhzrmiafqslcejkwo’ = ‘THEANDOBYFRUGILCVSKWMPQXMZ’, ta được:*

THE OSCARS TURN ON SUNDAY WHICH SEEMS ABOUT RIGHT AFTER THIS LONG STRANGE AWARDS TRIP THE BAGGER FEELS LIKE A NONAGENARIAN TOO

THE AWARDS RACE WAS BOOKENDED BY THE DEMISE OF HARVEY WEINSTEIN AT ITS OUTSET AND THE APPARENT IMPLOSION OF HIS FILM COMPANY AT THE END AND IT WAS SHAPED BY THE EMERGENCE OF METOO TIMES UP BLACKGOWN POLITICS ARMCANDY ACTIVISM AND A NATIONAL CONVERSATION AS BRIEF AND MAD AS A FEVER DREAM ABOUT WHETHER THERE OUGHT TO BE A PRESIDENT WINFREY THE SEASON DIDNT ZUST SEEM EXTRA LONG IT WAS EXTRA LONG BECAUSE THE OSCARS WERE MOVED TO THE FIRST WEEKEND IN MARCH TO AVOID CONFLICTING WITH THE CLOSING CEREMONY OF THE WINTER OLYMPICS THANKS PYEONGCHANG

ONE BIG QUESTION SURROUNDING THIS YEARS ACADEMY AWARDS IS HOW OR IF THE CEREMONY WILL ADDRESS METOO ESPECIALLY AFTER THE GOLDEN GLOBES WHICH BECAME A ZUBILANT COMINGOUT PARTY FOR TIMES UP THE MOVEMENT SPEARHEADED BY POWERFUL HOLLYWOOD WOMEN WHO HELPED RAISE MILLIONS OF DOLLARS TO FIGHT SEXUAL HARASSMENT AROUND THE COUNTRY

SIGNALING THEIR SUPPORT GOLDEN GLOBES ATTENDEES SWATHED THEMSELVES IN BLACK SPORTED LAPEL PINS AND SOUNDED OFF ABOUT SEXIST POWER IMBALANCES FROM THE RED CARPET AND THE STAGE ON THE AIR E WAS CALLED OUT ABOUT PAY INEQUITY AFTER

ITS FORMER ANCHOR CATT SADLER QUIT ONCE SHE LEARNED THAT SHE WAS MAKING FAR LESS THAN A MALE COHOST AND DURING THE CEREMONY NATALIE PORTMAN TOOK A BLUNT AND SATISFYING DIG AT THE ALLMALE ROSTER OF NOMINATED DIRECTORS HOW COULD THAT BE TOPPED

AS IT TURNS OUT AT LEAST IN TERMS OF THE OSCARS IT PROBABLY WONT BE

WOMEN INVOLVED IN TIMES UP SAID THAT ALTHOUGH THE GLOBES SIGNIFIED THE INITIATIVES LAUNCH THEY NEVER INTENDED IT TO BE ZUST AN AWARDS SEASON CAMPAIGN OR ONE THAT BECAME ASSOCIATED ONLY WITH REDCARPET ACTIONS INSTEAD A SPOKESWOMAN SAID THE GROUP IS WORKING BEHIND CLOSED DOORS AND HAS SINCE AMASSED MILLION FOR ITS LEGAL DEFENSE FUND WHICH AFTER THE GLOBES WAS FLOODED WITH THOUSANDS OF DONATIONS OF OR LESS FROM PEOPLE IN SOME COUNTRIES

NO CALL TO WEAR BLACK GOWNS WENT OUT IN ADVANCE OF THE OSCARS THOUGH THE MOVEMENT WILL ALMOST CERTAINLY BE REFERENCED BEFORE AND DURING THE CEREMONY ESPECIALLY SINCE VOCAL METOO SUPPORTERS LIKE ASHLEY ZUDD LAURA DERN AND NICOLE KIDMAN ARE SCHEDULED PRESENTERS

ANOTHER FEATURE OF THIS SEASON NO ONE REALLY KNOWS WHO IS GOING TO WIN BEST PICTURE ARGUABLY THIS HAPPENS A LOT OF THE TIME INARGUABLY THE NAILBITER NARRATIVE ONLY SERVES THE AWARDS HYPE MACHINE BUT OFTEN THE PEOPLE FORECASTING THE RACE SOCALLED OSCAROLOGISTS CAN MAKE ONLY EDUCATED GUESSES

THE WAY THE ACADEMY TABULATES THE BIG WINNER DOESNT HELP IN EVERY OTHER CATEGORY THE NOMINEE WITH THE MOST VOTES WINS BUT IN THE BEST PICTURE CATEGORY VOTERS ARE ASKED TO LIST THEIR TOP MOVIES IN PREFERENTIAL ORDER IF A MOVIE GETS MORE THAN PERCENT OF THE FIRSTPLACE VOTES IT WINS WHEN NO MOVIE MANAGES THAT THE ONE WITH THE FEWEST FIRSTPLACE VOTES IS ELIMINATED AND ITS VOTES ARE REDISTRIBUTED TO THE MOVIES THAT GARNERED THE ELIMINATED BALLOTS SECONDPLACE VOTES AND THIS CONTINUES UNTIL A WINNER EMERGES

IT IS ALL TERRIBLY CONFUSING BUT APPARENTLY THE CONSENSUS FAVORITE COMES OUT AHEAD IN THE END THIS MEANS THAT ENDOFSEASON AWARDS CHATTER INVARIABLY INVOLVES TORTURED SPECULATION ABOUT WHICH FILM WOULD MOST LIKELY BE VOTERS SECOND OR THIRD FAVORITE AND THEN EQUALLY TORTURED CONCLUSIONS ABOUT WHICH FILM MIGHT PREVAIL

IN IT WAS A TOSSUP BETWEEN BOYHOOD AND THE EVENTUAL WINNER BIRDMAN IN WITH LOTS OF EXPERTS BETTING ON THE REVENANT OR THE BIG SHORT THE PRIME WENT TO SPOTLIGHT LAST YEAR NEARLY ALL THE FORECASTERS DECLARED LA LA LAND THE PRESUMPTIVE WINNER AND FOR TWO AND A HALF MINUTES THEY WERE CORRECT BEFORE AN ENVELOPE SNAFU WAS REVEALED AND THE RIGHTFUL WINNER MOONLIGHT WAS CROWNED

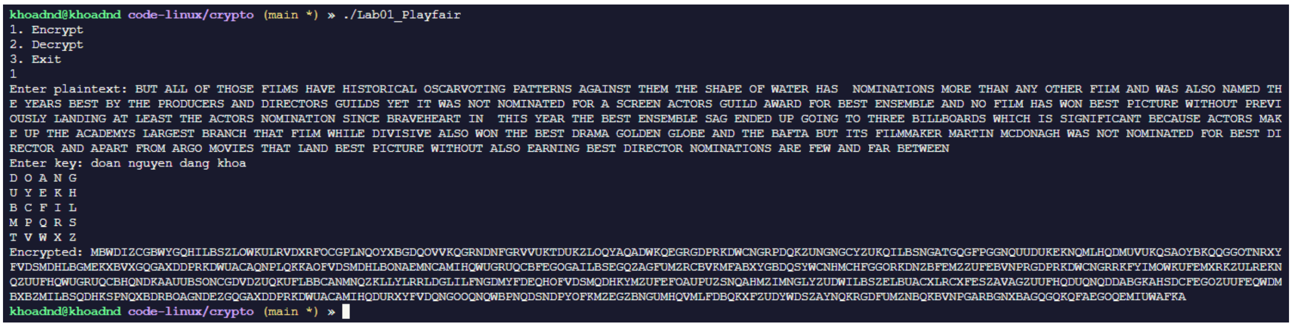
THIS YEAR AWARDS WATCHERS ARE UNEQUALLY DIVIDED BETWEEN THREE BILLBOARDS OUTSIDE EBBING MISSOURI THE FAVORITE AND THE SHAPE OF WATER WHICH IS THE BAGGERS PREDICTION WITH A FEW FORECASTING A HAIL MARY WIN FOR GET OUT

BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE SHAPE OF WATER HAS NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO NAMED THE YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS WON BEST PICTURE WITHOUT PREVIOUSLY LANDING AT LEAST THE ACTORS NOMINATION SINCE BRAVEHEART IN THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAKE UP THE ACADEMYS LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST DIRECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN

- Sau khi đọc xong, ta thấy toàn bộ văn bản đã có nghĩa => key: *'ytnvupxgdbhzrmiafqslcejkwo' –> 'THEANDOBYFRUGILCVSKWMPQXMZ'*

4. Playfair cipher

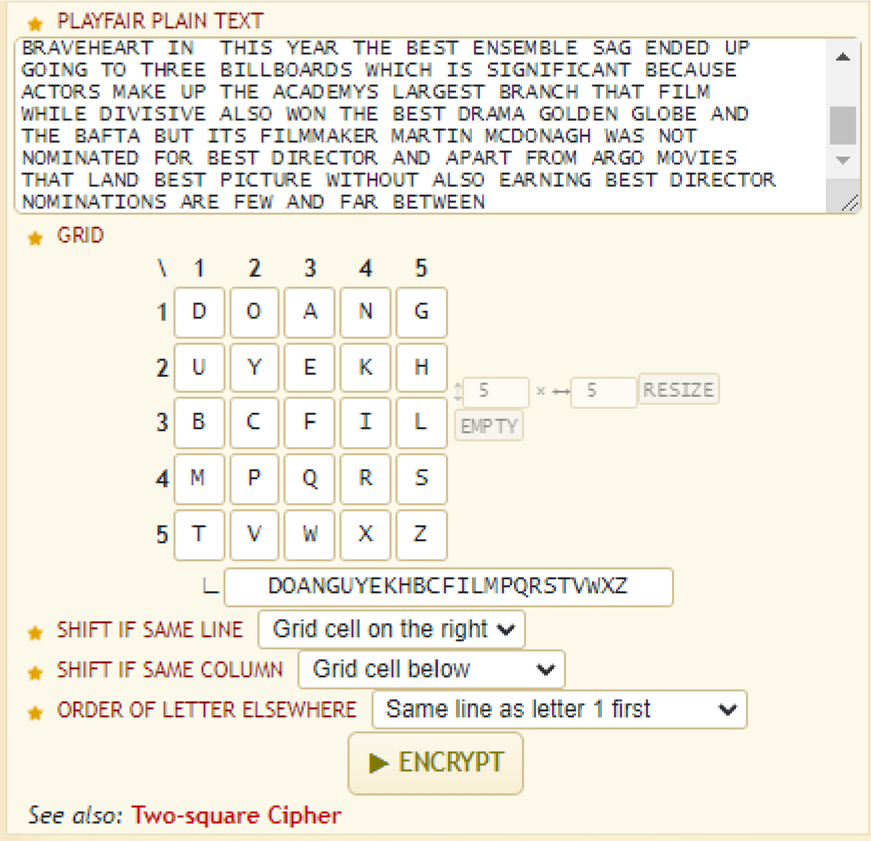
a. Test 100 words and compare with other tool



```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_Playfair
1. Encrypt
2. Decrypt
3. Exit
1
Enter plaintext: BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE SHAPE OF WATER HAS  NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO NAMED TH
E YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS WON BEST PICTURE WITHOUT PREVI
OUSLY LANDING AT LEAST THE ACTORS NOMINATION SINCE BRAVEHEART IN  THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAK
E UP THE ACADEMYS LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST DI
RECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN
Enter key: doan nguyen dang khoa
D O A N G
U Y E K H
B C F I L
M P Q R S
T V W X Z
Encrypted: MBWDIZCGBWYGQHILBSZLOWKULRVDXRFOCGPLNQOYXBGDQOVVKQGRNDNFGRVVUKTDUKZLOQYAQADWKQEGRGDPRKDWCNGRPDQKZUNGNGCYZUKQILBSNGATGQGFPGGNQUUDUKEKNQMLHQDMUVUKQSAOYBKQQGGOTNRXY
FVDSMDHLBGMEKXBVXGQGAXDDPRKDWUACAQNPLQKKAOFVDSMDHLBONAEMNCAMIHQWUGRUQCBFEGOGAILBSEGQZAGFUMZRCBVKMFABXYGBDQSYWCNHMCHFGGORKDNZBFEMZZUFEBVNPRGDPRKDWCNGRRKFYIMOWKUFEMXRKZULREKN
QZUUFHQWUGRUQCBHQNDKAAUUBSONCGDVDZUQKUFLBBCANMNQZKLLYLRRLDGLILFNGDMYFDEQHOFVDSMQDHKYMZUFEFOAUPUZSNQAHMZIMNGLYZUDWILBSZELBUACXLRCXFESZAVAGZUUFHQDUQNQDDABGKAHSDCFEGOZUUFEQWDM
BXBZMILBSQDHKSPNQXBDRBOAGNDEZGQGAXDDPRKDWUACAMIHQDURXYFVDQNGOOQNQWBPNQDSNDPYOFKMZEGZBNGUMHQVMLFDBQKXFZUDYWDSZAYNQKRGDFUMZNBQKBVNPGARBGNXBAGQGQKQFAEGOQEMIUWAFKA
khoadnd@khoadnd code-linux/crypto (main *) »
```

- Ta thử với đoạn văn bản: *BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE SHAPE OF WATER HAS NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO NAMED THE YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS WON BEST PICTURE WITHOUT PREVIOUSLY LANDING AT LEAST THE ACTORS NOMINATION SINCE BRAVEHEART IN THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAKE UP THE ACADEMYS LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST DIRECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN*
- Key: *DOANGUYEKHBCFILMPQRSTVWXZ*
- Đoạn văn bản đã mã hóa: *MBWDIZCGBWYGQHILBSZLOWKULRVDXRFOCGPLNQOYXBGDQOVVKQGRNDNFGRVVUKTDUKZLOQYAQADWKQEGRGDPRKDWCNGRPDQKZUNGNGCYZUKQILBSNGATGQGFPGGNQUUDUKEKNQMLHQDMUVUKQSAOYBKQQGGOTNRXYFVDSMDHLBGMEKXBVXGQGAXDDPRKDWUACAQNPLQKKAOFVDSMDHLBONAEMNCAMIHQWUGRUQCBFEGOGAILBSEGQZAGFUMZRCBVKMFABXYGBDQSYWCNHMCHFGGORKDNZBFEMZZUFEBVNPRGDPRKDWCNGRRKFYIMOWKUFEMXRKZULREKNQZUUFHQWUGRUQCBHQNDKAAUUBSONCGDVDZUQKUFLBBCANMNQZKLLYLRRLDGLILFNGDMYFDEQHOFVDSMQDHKYMZUFEFOAUPUZSNQAHMZIMNGLYZUDWILBSZELBUACXLRCXFESZAVAGZUUFHQDUQNQDDABGKAHSDCFEGOZUUFEQWDMBXBZMILBSQDHKSPNQXBDRBOAGNDEZGQGAXDDPRKDWUACAMIHQDURXYFVDQNGOOQNQWBPNQDSNDPYOFKMZEGZBNGUMHQVMLFDBQKXFZUDYWDSZAYNQKRGDFUMZNBQKBVNPGARBGNXBAGQGQKQFAEGOQEMIUWAFKA*

- Kiểm tra với tool dcode.fr



PLAYFAIR PLAIN TEXT

```
BRAVEHEART IN  THIS YEAR THE BEST ENSEMBLE SAG ENDED UP
GOING TO THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE
ACTORS MAKE UP THE ACADEMYS LARGEST BRANCH THAT FILM
WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE AND
THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT
NOMINATED FOR BEST DIRECTOR AND APART FROM ARGO MOVIES
THAT LAND BEST PICTURE WITHOUT ALSO EARNING BEST DIRECTOR
NOMINATIONS ARE FEW AND FAR BETWEEN
```

GRID

\	1	2	3	4	5
1	D	O	A	N	G
2	U	Y	E	K	H
3	B	C	F	I	L
4	M	P	Q	R	S
5	T	V	W	X	Z

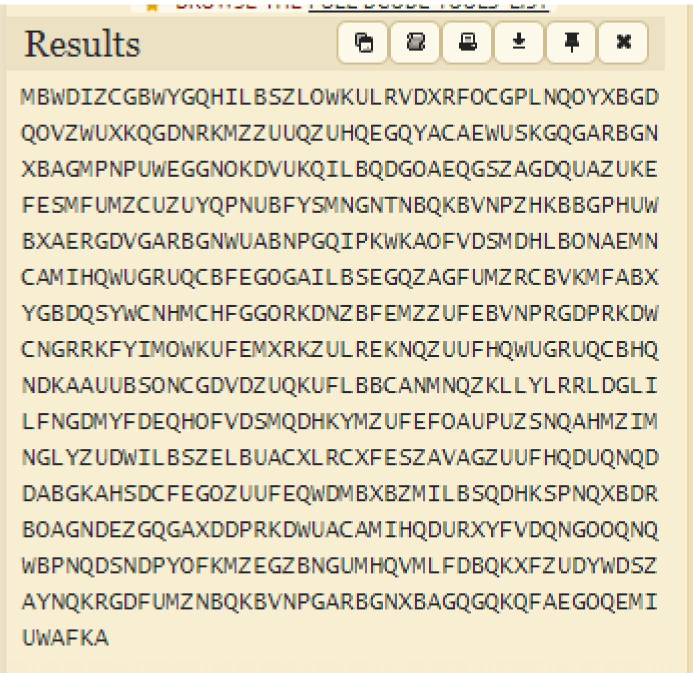
└ DOANGUYEKHBCFILMPQRSTVWXZ

SHIFT IF SAME LINE: Grid cell on the right

SHIFT IF SAME COLUMN: Grid cell below

ORDER OF LETTER ELSEWHERE: Same line as letter 1 first

See also: Two-square Cipher

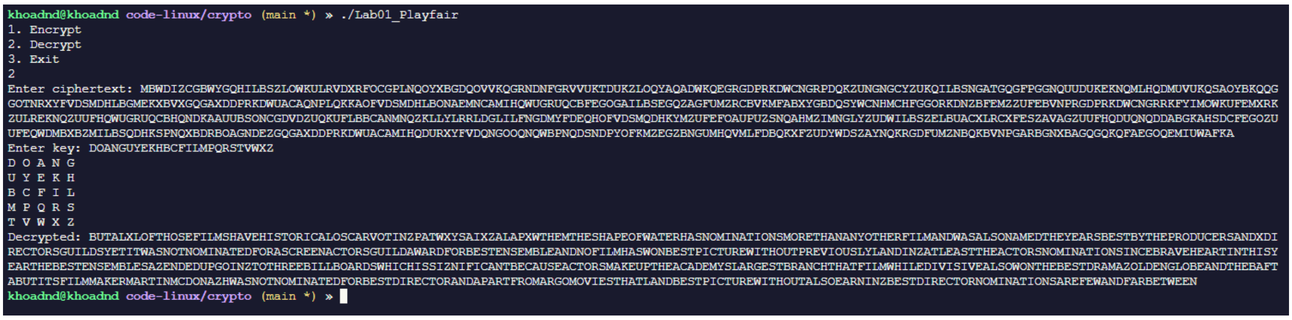


Results

```
MBWDIZCGBWYGQHILBSZLOWKULRVDXRFOCGPLNQOYXBGD
QOVZWUXKQGDNRKMZZUUQZUHQEGQYACAEWUSKGQGARBGN
XBAGMPNPUWEGGNOKDVUKQILBQDGOAEQGSZAGDQUAZUKE
FESMFUMZCUZUYQPNUBFYSMNGNTNBQKBVNPZHKBBGPHUW
BXAERGDVGARBGNWUABNPGQIPKWKAOFVDSMDHLBONAEMN
CAMIHQWUGRUQCBFEGOGAILBSEGQZAGFUMZRCBVKMFABX
YGBDQSYWCNHMCHFGGORKDNZBFEMZZUFEBVNPRGDPRKDW
CNGRRKFYIMOWKUFEMXRKZULREKNQZUUFHQWUGRUQCBHQ
NDKAAUUBSONCGDVDZUQKUFLBBCANMNQZKLLYLRRLDGLI
LFNGDMYFDEQHOFVDSMQDHKYMZUFEFOAUPUZSNQAHMZIM
NGLYZUDWILBSZELBUACXLRCXFESZAVAGZUUFHQDUQNQD
DABGKAHSDCFEGOZUUFEQWDMBXBZMILBSQDHKSPNQXBDR
BOAGNDEZGQGAXDDPRKDWUACAMIHQDURXYFVDQNGOOQNQ
WBPNQDSNDPYOFKMZEGZBNGUMHQVMLFDBQKXFZUDYWDSZ
AYNQKRGDFUMZNBQKBVNPGARBGNXBAGQGQKQFAEGOQEMI
UWAFKA
```

- Nhận xét: cho ra cùng 1 kết quả

- Decode:
    - Sử dụng chung đoạn văn bản đã được mã hóa ở trên, cùng với key DOANGUYEKHBCFILMPQRSTVWXZ:

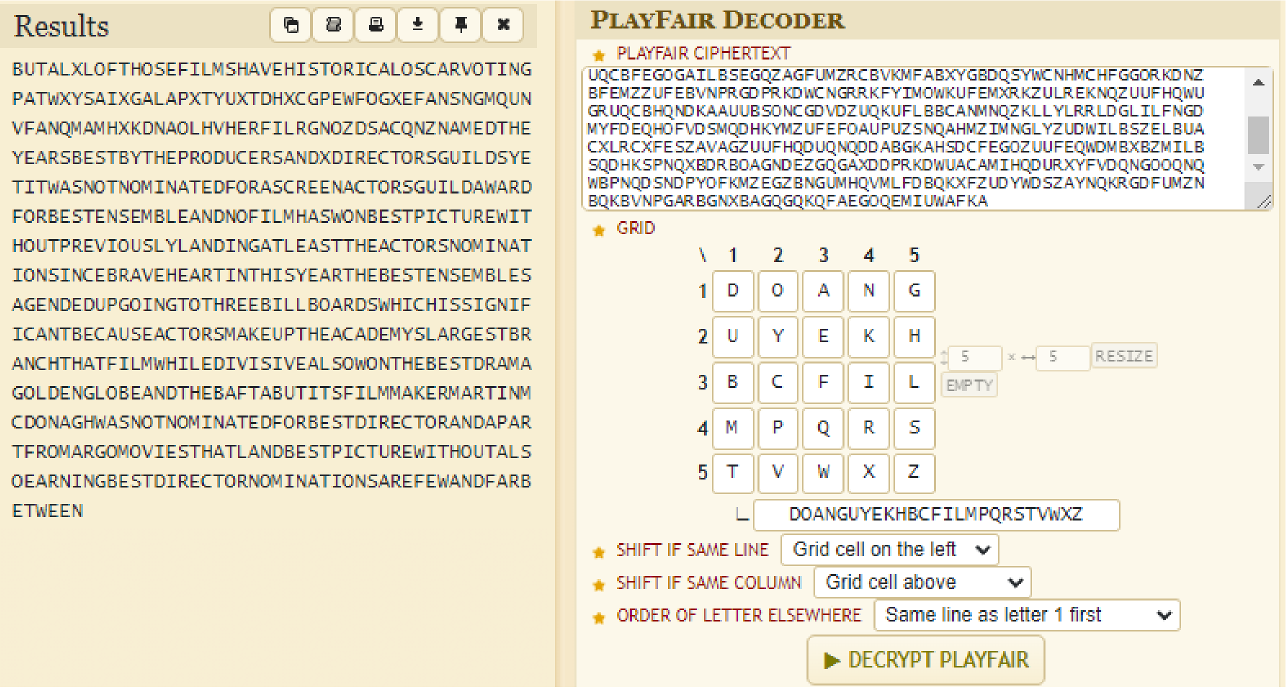


```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_Playfair
1. Encrypt
2. Decrypt
3. Exit
2
Enter ciphertext: MBWDIZCGBWYGQHILBSZLOWKULRVDXRFOCGPLNQOYXBGDQOVVKQGRNDNFGRVVUKTDUKZLOQYAQADWKQEGRGDPRKDWCNGRPDQKZUNGNGCYZUKQILBSNGATGQGFPGGNQUUDUKEKNQMLHQDMUVUKQSAOYBKQQG
GOTNRXYFVDSMDHLBGMEKXBVXGQGAXDDPRKDWUACAQNPLQKKAOFVDSMDHLBONAEMNCAMIHQWUGRUQCBFEGOGAILBSEGQZAGFUMZRCBVKMFABXYGBDQSYWCNHMCHFGGORKDNZBFEMZZUFEBVNPRGDPRKDWCNGRRKFYIMOWKUFEMXRK
ZULREKNQZUUFHQWUGRUQCBHQNDKAAUUBSONCGDVDZUQKUFLBBCANMNQZKLLYLRRLDGLILFNGDMYFDEQHOFVDSMQDHKYMZUFEFOAUPUZSNQAHMZIMNGLYZUDWILBSZELBUACXLRCXFESZAVAGZUUFHQDUQNQDDABGKAHSDCFEGOZU
UFEQWDMBXBZMILBSQDHKSPNQXBDRBOAGNDEZGQGAXDDPRKDWUACAMIHQDURXYFVDQNGOOQNQWBPNQDSNDPYOFKMZEGZBNGUMHQVMLFDBQKXFZUDYWDSZAYNQKRGDFUMZNBQKBVNPGARBGNXBAGQGQKQFAEGOQEMIUWAFKA
Enter key: DOANGUYEKHBCFILMPQRSTVWXZ
D O A N G
U Y E K H
B C F I L
M P Q R S
T V W X Z
Decrypted: BUTALXLOFTHOSEFILMSHAVEHISTORICALOSCARVOTINZPATWXYSAIXZALAPXWTHEMTHESHAPEOFWATERHASNOMINATIONSMORETHANANYOTHERFILMANDWASALSONAMEDTHEYEARSBESTBYTHEPRODUCERSANDXDI
RECTORSGUILDSYETITWASNOTNOMINATEDFORASCREENACTORSGUILDAWARDFORBESTENSEMBLEANDNOFILMHASWONBESTPICTUREWITHOUTPREVIOUSLYLANDINZATLEASTTHEACTORSNOMINATIONSINCEBRAVEHEARTINTHISY
EARTHEBESTENSEMBLESAZENDEDUPGOINZTOTHREEBILLBOARDSWHICHISSIZNIFICANTBECAUSEACTORSMAKEUPTHEACADEMYSLARGESTBRANCHTHATFILMWHILEDIVISIVEALSOWONTHEBESTDRAMAZOLDENGLOBEANDTHEBAFT
ABUTITSFILMMAKERMARTINMCDONAZHWASNOTNOMINATEDFORBESTDIRECTORANDAPARTFROMARGOMOVIESTHATLANDBESTPICTUREWITHOUTALSOEARNINZBESTDIRECTORNOMINATIONSAREFEWANDFARBETWEEN
khoadnd@khoadnd code-linux/crypto (main *) » 
```

- Decoded message:

  BUTALXLOFTHOSEFILMSHAVEHISTORICALOSCARVOTINZPATWXYSAIXZALAPXWTHEMTHESHAPEOFWATERHASNOMINATIONSMORETHANANYOTHERFILMANDWASALSONAMEDTHEYEARSBESTBYTHEPRODUCERSANDXDIRECTORSGUILDSYETITWASNOTNOMINATEDFORASCREENACTORSGUILDAWARDFORBESTENSEMBLEANDNOFILMHASWONBESTPICTUREWITHOUTPREVIOUSLYLANDINZATLEASTTHEACTORSNOMINATIONSINCEBRAVEHEARTINTHISYEARTHEBESTENSEMBLESAZENDEDUPGOINZTOTHREEBILLBOARDSWHICHISSIZNIFICANTBECAUSEACTORSMAKEUPTHEACADEMYSLARGESTBRANCHTHATFILMWHILEDIVISIVEALSOWONTHEBESTDRAMAZOLDENGLOBEANDTHEBAFTABUTITSFILMMAKERMARTINMCDONAZHWASNOTNOMINATEDFORBESTDIRECTORANDAPARTFROMARGOMOVIESTHATLANDBESTPICTUREWITHOUTALSOEARNINZBESTDIRECTORNOMINATIONSAREFEWANDFARBETWEEN

- So sánh với tool:



Results

```
BUTALXLOFTHOSEFILMSHAVEHISTORICALOSCARVOTING
PATWXYSAIXGALAPXTYUXTDHXCGPEWFOGXEFANSNGMQUN
VFANQMAMHXKDNAOLHVHERFILRGNOZDSACQNZNAMEDTHE
YEARSBESTBYTHEPRODUCERSANDXDIRECTORSGUILDSYE
TITWASNOTNOMINATEDFORASCREENACTORSGUILDAWARD
FORBESTENSEMBLEANDNOFILMHASWONBESTPICTUREWIT
HOUTPREVIOUSLYLANDINGATLEASTTHEACTORSNOMINAT
IONSINCEBRAVEHEARTINTHISYEARTHEBESTENSEMBLES
AGENDEDUPGOINGTOTHREEBILLBOARDSWHICHISSIGNIF
ICANTBECAUSEACTORSMAKEUPTHEACADEMYSLARGESTBR
ANCHTHATFILMWHILEDIVISIVEALSOWONTHEBESTDRAMA
GOLDENGLOBEANDTHEBAFTABUTITSFILMMAKERMARTINM
CDONAGHWASNOTNOMINATEDFORBESTDIRECTORANDAPAR
TFROMARGOMOVIESTHATLANDBESTPICTUREWITHOUTALS
OEARNINGBESTDIRECTORNOMINATIONSAREFEWANDFARB
ETWEEN
```

PLAYFAIR DECODER

PLAYFAIR CIPHERTEXT

```
UQCBFEGOGAILBSEGQZAGFUMZRCBVKMFABXYGBDQSYWCNHMCHFGGORKDNZ
BFEMZZUFEBVNPRGDPRKDWCNGRRKFYIMOWKUFEMXRKZULREKNQZUUFHQWU
GRUQCBHQNDKAAUUBSONCGDVDZUQKUFLBBCANMNQZKLLYLRRLDGLILFNGD
MYFDEQHOFVDSMQDHKYMZUFEFOAUPUZSNQAHMZIMNGLYZUDWILBSZELBUA
CXLRCXFESZAVAGZUUFHQDUQNQDDABGKAHSDCFEGOZUUFEQWDMBXBZMILB
SQDHKSPNQXBDRBOAGNDEZGQGAXDDPRKDWUACAMIHQDURXYFVDQNGOOQNQ
WBPNQDSNDPYOFKMZEGZBNGUMHQVMLFDBQKXFZUDYWDSZAYNQKRGDFUMZN
BQKBVNPGARBGNXBAGQGQKQFAEGOQEMIUWAFKA
```

GRID

\	1	2	3	4	5
1	D	O	A	N	G
2	U	Y	E	K	H
3	B	C	F	I	L
4	M	P	Q	R	S
5	T	V	W	X	Z

5 × 5 RESIZE

EMPTY

DOANGUYEKHBCFILMPQRSTVWXZ

SHIFT IF SAME LINE: Grid cell on the left

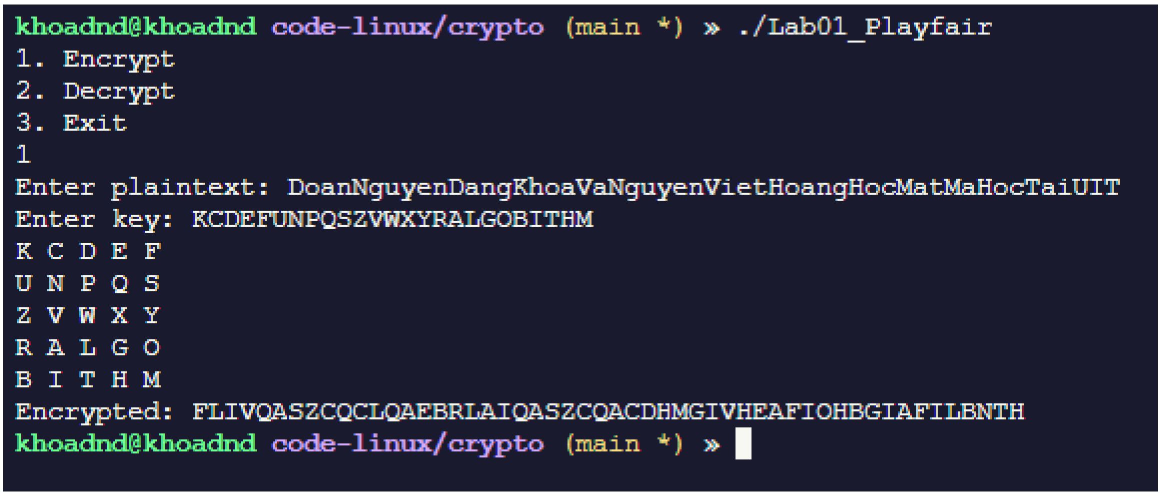
SHIFT IF SAME COLUMN: Grid cell above

ORDER OF LETTER ELSEWHERE: Same line as letter 1 first

b. Use playfair matrix provided to encode a message contain full name of all members of your group and some words to get at least 50 characters

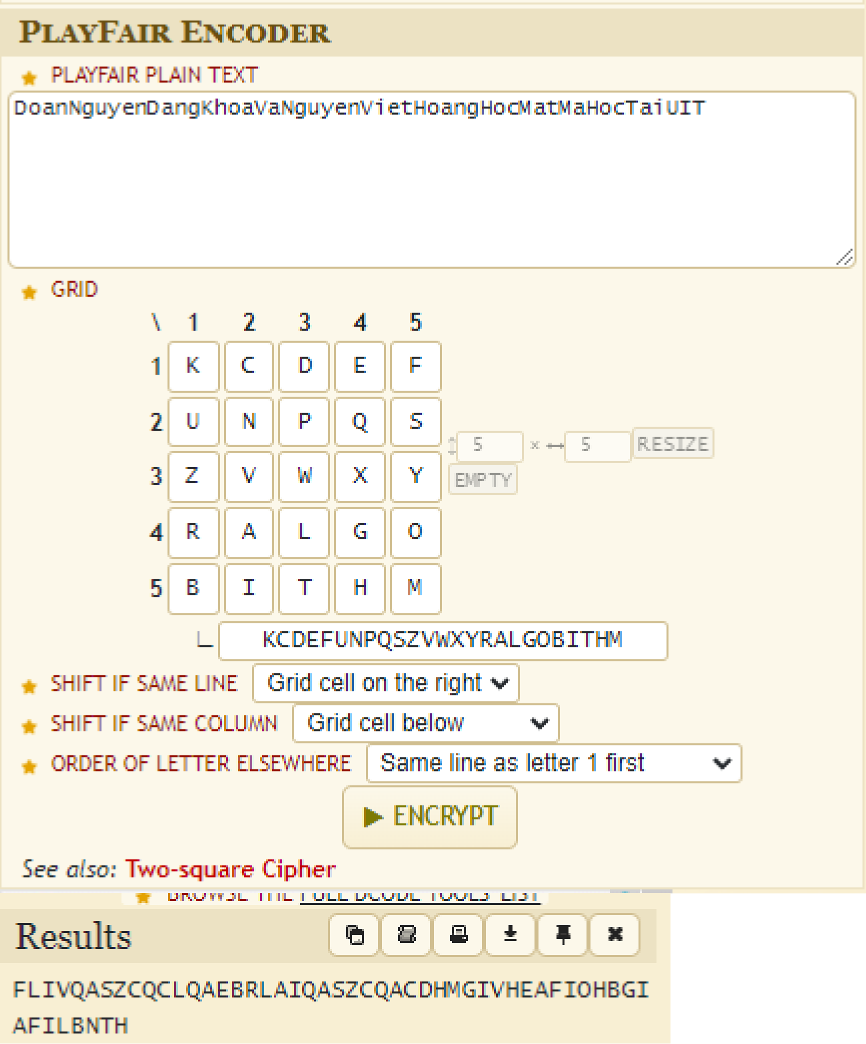
- Plaintext: DoanNguyenDangKhoaVaNguyenVietHoangHocMatMaHocTaiUIT
- Key: KCDEFUNPQSZVWXYRALGOBITHM

- Encoded (program): *FLIVQASZCQCLQAEBRLAIQASZCQACDHMGIVHEAFIOHBGIAFILBNTH*



```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_Playfair
1. Encrypt
2. Decrypt
3. Exit
1
Enter plaintext: DoanNguyenDangKhoaVaNguyenVietHoangHocMatMaHocTaiUIT
Enter key: KCDEFUNPQSZVWXYRALGOBITHM
K C D E F
U N P Q S
Z V W X Y
R A L G O
B I T H M
Encrypted: FLIVQASZCQCLQAEBRLAIQASZCQACDHMGIVHEAFIOHBGIAFILBNTH
khoadnd@khoadnd code-linux/crypto (main *) »
```

- Encoded (dcode.fr): *FLIVQASZCQCLQAEBRLAIQASZCQACDHMGIVHEAFIOHBGIAFILBNTH*



PLAYFAIR ENCODER

★ PLAYFAIR PLAIN TEXT

DoanNguyenDangKhoaVaNguyenVietHoangHocMatMaHocTaiUIT

★ GRID

\	1	2	3	4	5
1	K	C	D	E	F
2	U	N	P	Q	S
3	Z	V	W	X	Y
4	R	A	L	G	O
5	B	I	T	H	M

KCDEFUNPQSZVWXYRALGOBITHM

★ SHIFT IF SAME LINE: Grid cell on the right

★ SHIFT IF SAME COLUMN: Grid cell below

★ ORDER OF LETTER ELSEWHERE: Same line as letter 1 first

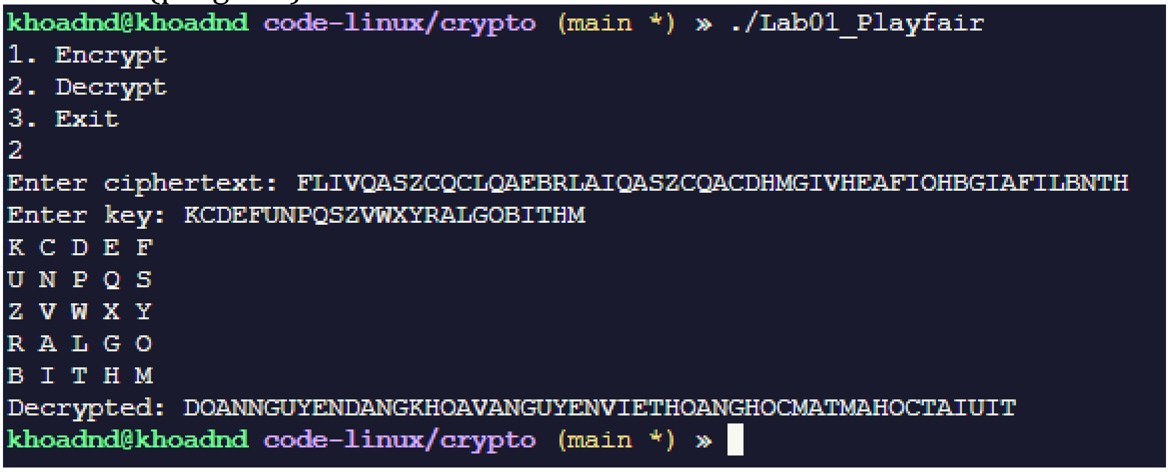
See also: Two-square Cipher

Results

FLIVQASZCQCLQAEBRLAIQASZCQACDHMGIVHEAFIOHBGIAFILBNTH

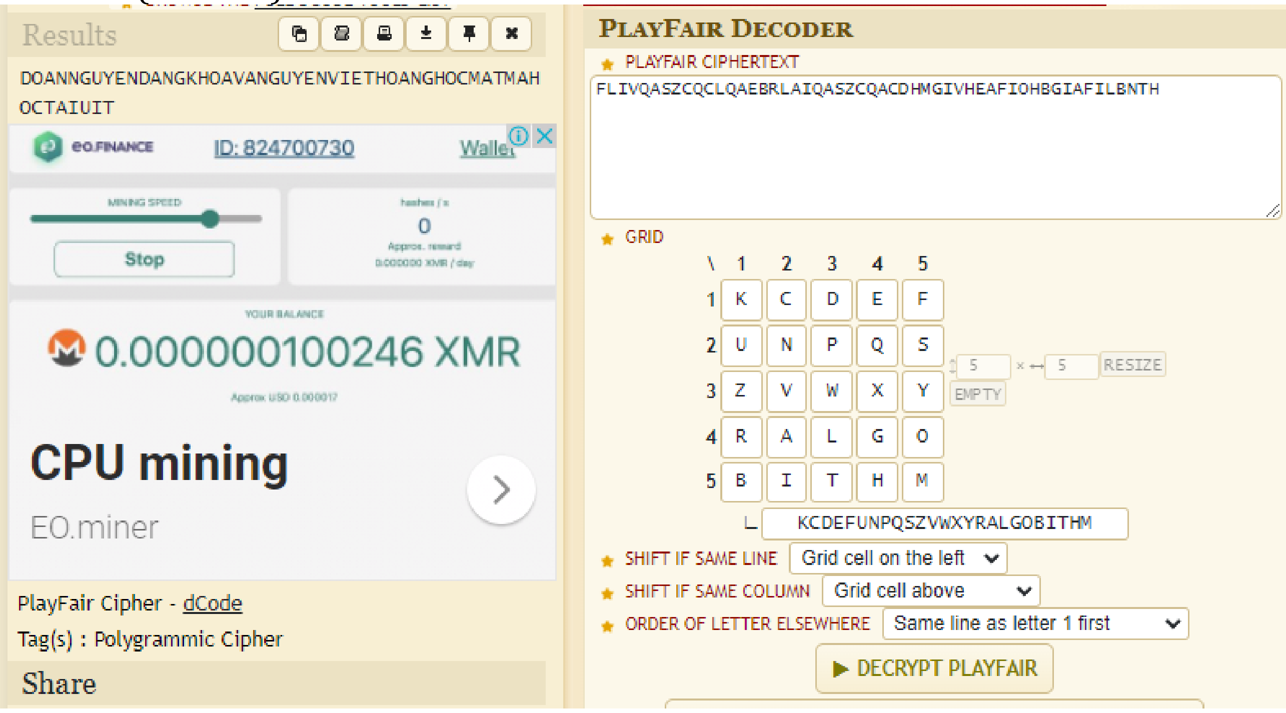
- Ta thử decode:

- Decoded (program):



```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_Playfair
1. Encrypt
2. Decrypt
3. Exit
2
Enter ciphertext: FLIVQASZCQCLQAEBRLAIQASZCQACDHMGIVHEAFIOHBGIAFILBNTH
Enter key: KCDEFUNPQSZVWXYRALGOBITHM
K C D E F
U N P Q S
Z V W X Y
R A L G O
B I T H M
Decrypted: DOANNGUYENDANGKHOAVANGUYENVIETHOANGHOCMATMAHOCTAIUIT
khoadnd@khoadnd code-linux/crypto (main *) »
```

- Decoded (dcode.fr):



Results

DOANNGUYENDANGKHOAVANGUYENVIETHOANGHOCMATMAHOCTAIUIT

PlayFair Cipher - dCode

Tag(s) : Polygrammic Cipher

Share

PLAYFAIR DECODER

PLAYFAIR CIPHERTEXT: FLIVQASZCQCLQAEBRLAIQASZCQACDHMGIVHEAFIOHBGIAFILBNTH

GRID

\	1	2	3	4	5
1	K	C	D	E	F
2	U	N	P	Q	S
3	Z	V	W	X	Y
4	R	A	L	G	O
5	B	I	T	H	M

KCDEFUNPQSZVWXYRALGOBITHM

SHIFT IF SAME LINE: Grid cell on the left

SHIFT IF SAME COLUMN: Grid cell above

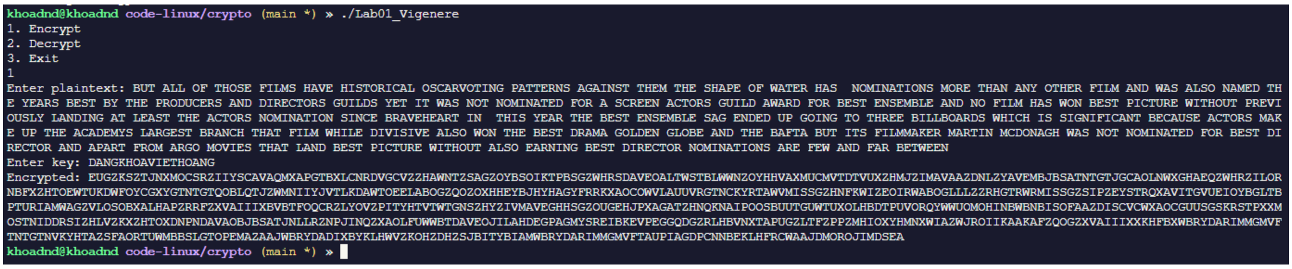
ORDER OF LETTER ELSEWHERE: Same line as letter 1 first

5. Vigenère cipher

- Plaintext:
  *BUTTALLTOFTTHOSETFILMSTHAVETHISTORICALTOSCARVOTINGTPATTERNSTAGAINSTTTH
  EMTTHETSHAPETOFTWATERTHASTTNOMINATIONSTMORETTHANTANYTOTHERTFILMTANDTWA
  STALSOTNAMEDTTHETYEARSTBESTTBYTTHETPRODUCERSTANDTDIRECTORSTGUILDSTYETT
  ITTWASTNOTTNOMINATEDTFORTATSCREENTACTORSTGUILDTAWARDTFORTBESTTENSEMBLE
  TANDTNOTFILMTHASTWONTBESTTPICTURETWITHOUTTPREVIOUSLYTLANDINGTATTLEASTT
  THETACTORSTNOMINATIONTSINCETBRAVEHEARTTINTTHISTYEARTTHETBESTTENSEMBLE
  TSAGTENDEDTUPTGOINGTTOTTHREETBILLBOARDSTWHICHTISTSIGNIFICANTTBECAUSETA
  CTORSTMAKETUPTTHETACADEMYSTLARGESTTBRANCHTTHATTFILMTWHILETDIVISIVETALS
  OTWONTTHETBESTTDRAMATGOLDENTGLOBETANDTTHETBAFTATBUTTITSTFILMMAKERTMART
  INTMCDONAGHTWASTNOTTNOMINATEDTFORTBESTTDIRECTORTANDTAPARTTFROMTARGOTMO
  VIESTTHATTLANDTBESTTPICTURETWITHOUTTALSOTEARNINGTBESTTDIRECTORTNOMINAT
  IONSTARETFEWTANDTFARTBETWEEN*
- Key: *DANGKHOAVIETHOANG*

- Cipher text:

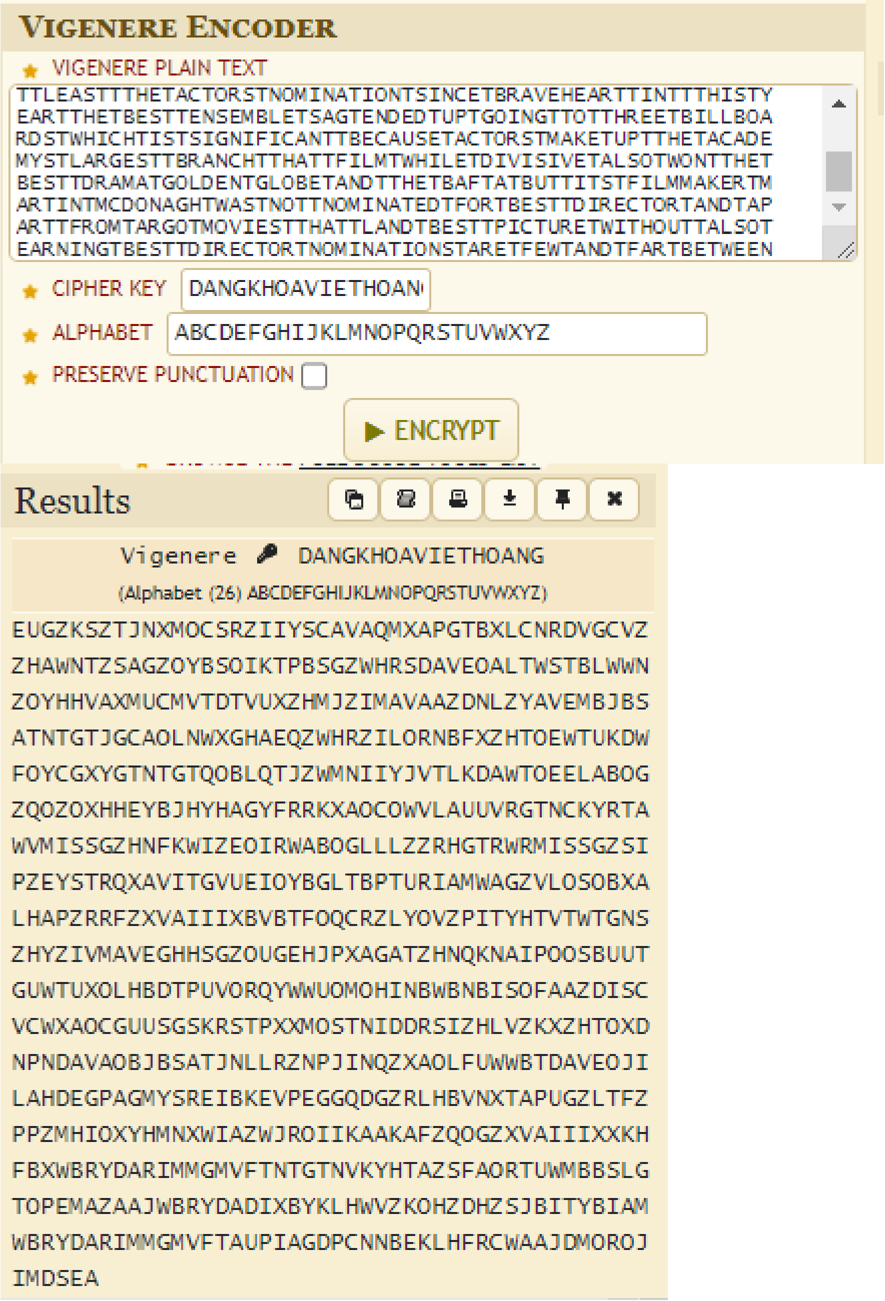
*EUGZKSZTJNXMOCSRZIIYSCAVAQMXAPGTBXLCNRDVGCVZZHAWNTZSAGZOYBSOIKTPBSGZWH
RSDAVEOALTWSTBLWWNZOYHHVAXMUCMVTDTVUXZHMJZIMAVAAZDNLZYAVEMBJBSATNTGTJG
CAOLNWXGHAEQZWHRZILORNBFXZHTOEWTUKDWFOYCGXYGTNTGTQOBLQTJZWMNIIYJVTLKDA
WTOEELABOGZQOZOXHHEYBJHYHAGYFRRKXAOCOWVLAUUVRGTNCKYRTAWVMISSGZHNFKWIZE
OIRWABOGLLLZZRHGTRWRMISSGZSIPZEYSTRQXAVITGVUEIOYBGLTBPTURIAMWAGZVLOSOB
XALHAPZRRFZXVAIIIXBVBTFOQCRZLYOVZPITYHTVTWTGNSZHYZIVMAVEGHHSGZOUGEHJPX
AGATZHNQKNAIPOOSBUUTGUWTUXOLHBDTPUVORQYWWUOMOHINBWBNBISOFAAZDISCVCWXAO
CGUUSGSKRSTPXXMOSTNIDDRSIZHLVZKXZHTOXDNPNDAVAOBJBSATJNLLRZNPJINQZXAOLF
UWWBTDAVEOJILAHDEGPAGMYSREIBKEVPEGGQDGZRLHBVNXTAPUGZLTFZPPZMHIOXYHMNXW
IAZWJROIIKAAKAFZQOGZXVAIIIXXKHFBXWBRYDARIMMGMVFTNTGTNVKYHTAZSFAORTUWMB
BSLGTOPEMAZAAJWBRYDADIXBYKLHWVZKOHZDHZSJBITYBIAMWBRYDARIMMGMVFTAUPIAGD
PCNNBEKLHFRCWAAJDMOROJIMDSEA*



```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_Vigenere
1. Encrypt
2. Decrypt
3. Exit
1
Enter plaintext: BUT ALL OF THOSE FILMS HAVE HISTORICAL OSCARVOTING PATTERNS AGAINST THEM THE SHAPE OF WATER HAS  NOMINATIONS MORE THAN ANY OTHER FILM AND WAS ALSO NAMED TH
E YEARS BEST BY THE PRODUCERS AND DIRECTORS GUILDS YET IT WAS NOT NOMINATED FOR A SCREEN ACTORS GUILD AWARD FOR BEST ENSEMBLE AND NO FILM HAS WON BEST PICTURE WITHOUT PREVI
OUSLY LANDING AT LEAST THE ACTORS NOMINATION SINCE BRAVEHEART IN  THIS YEAR THE BEST ENSEMBLE SAG ENDED UP GOING TO THREE BILLBOARDS WHICH IS SIGNIFICANT BECAUSE ACTORS MAK
E UP THE ACADEMYS LARGEST BRANCH THAT FILM WHILE DIVISIVE ALSO WON THE BEST DRAMA GOLDEN GLOBE AND THE BAFTA BUT ITS FILMMAKER MARTIN MCDONAGH WAS NOT NOMINATED FOR BEST DI
RECTOR AND APART FROM ARGO MOVIES THAT LAND BEST PICTURE WITHOUT ALSO EARNING BEST DIRECTOR NOMINATIONS ARE FEW AND FAR BETWEEN
Enter key: DANGKHOAVIETHOANG
Encrypted: EUGZKSZTJNXMOCSRZIIYSCAVAQMXAPGTBXLCNRDVGCVZZHAWNTZSAGZOYBSOIKTPBSGZWHRSDAVEOALTWSTBLWWNZOYHHVAXMUCMVTDTVUXZHMJZIMAVAAZDNLZYAVEMBJBSATNTGTJGCAOLNWXGHAEQZWHRZILOR
NBFXZHTOEWTUKDWFOYCGXYGTNTGTQOBLQTJZWMNIIYJVTLKDAWTOEELABOGZQOZOXHHEYBJHYHAGYFRRKXAOCOWVLAUUVRGTNCKYRTAWVMISSGZHNFKWIZEOIRWABOGLLLZZRHGTRWRMISSGZSIPZEYSTRQXAVITGVUEIOYBGLTB
PTURIAMWAGZVLOSOBXALHAPZRRFZXVAIIIXBVBTFOQCRZLYOVZPITYHTVTWTGNSZHYZIVMAVEGHHSGZOUGEHJPXAGATZHNQKNAIPOOSBUUTGUWTUXOLHBDTPUVORQYWWUOMOHINBWBNBISOFAAZDISCVCWXAOCGUUSGSKRSTPXXM
OSTNIDDRSIZHLVZKXZHTOXDNPNDAVAOBJBSATJNLLRZNPJINQZXAOLFUWWBTDAVEOJILAHDEGPAGMYSREIBKEVPEGGQDGZRLHBVNXTAPUGZLTFZPPZMHIOXYHMNXWIAZWJROIIKAAKAFZQOGZXVAIIIXXKHFBXWBRYDARIMMGMVF
TNTGTNVKYHTAZSFAORTUWMBBSLGTOPEMAZAAJWBRYDADIXBYKLHWVZKOHZDHZSJBITYBIAMWBRYDARIMMGMVFTAUPIAGDPCNNBEKLHFRCWAAJDMOROJIMDSEA
khoadnd@khoadnd code-linux/crypto (main *) »
```

- Tool:

*EUGZKSZTJNXMOCSRZIIYSCAVAQMXAPGTBXLCNRDVGCVZZHAWNTZSAGZOYBSOIKTPBSGZWH
RSDAVEOALTWSTBLWWNZOYHHVAXMUCMVTDTVUXZHMJZIMAVAAZDNLZYAVEMBJBSATNTGTJG
CAOLNWXGHAEQZWHRZILORNBFXZHTOEWTUKDWFOYCGXYGTNTGTQOBLQTJZWMNIIYJVTLKDA
WTOEELABOGZQOZOXHHEYBJHYHAGYFRRKXAOCOWVLAUUVRGTNCKYRTAWVMISSGZHNFKWIZE
OIRWABOGLLLZZRHGTRWRMISSGZSIPZEYSTRQXAVITGVUEIOYBGLTBPTURIAMWAGZVLOSOB
XALHAPZRRFZXVAIIIXBVBTFOQCRZLYOVZPITYHTVTWTGNSZHYZIVMAVEGHHSGZOUGEHJPX
AGATZHNQKNAIPOOSBUUTGUWTUXOLHBDTPUVORQYWWUOMOHINBWBNBISOFAAZDISCVCWXAO
CGUUSGSKRSTPXXMOSTNIDDRSIZHLVZKXZHTOXDNPNDAVAOBJBSATJNLLRZNPJINQZXAOLF
UWWBTDAVEOJILAHDEGPAGMYSREIBKEVPEGGQDGZRLHBVNXTAPUGZLTFZPPZMHIOXYHMNXW
IAZWJROIIKAAKAFZQOGZXVAIIIXXKHFBXWBRYDARIMMGMVFTNTGTNVKYHTAZSFAORTUWMB
BSLGTOPEMAZAAJWBRYDADIXBYKLHWVZKOHZDHZSJBITYBIAMWBRYDARIMMGMVFTAUPIAGD
PCNNBEKLHFRCWAAJDMOROJIMDSEA*



VIGENERE PLAIN TEXT

```
TTLEASTTTHETACTORSTNOMINATIONTSINCETBRAVEHEARTTINTTTHISTY
EARTTHETBESTTENSEMBLETSAGTENDEDTUPTGOINGTTOTTHREETBILLBOA
RDSTWHICHTISTSIGNIFICANTTBECAUSETACTORSTMAKETUPTTHETACADE
MYSTLARGESTTBRANCHTTHATTFILMTWHILETDIVISIVETALSOTWONTTHET
BESTTDRAMATGOLDENTGLOBETANDTTHETBAFTATBUTTITSTFILMMAKERTM
ARTINTMCDONAGHTWASTNOTTNOMINATEDTFORTBESTTDIRECTORTANDTAP
ARTTFROMTARGOTMOVIESTTHATTLANDTBESTTPICTURETWITHOUTTALSOT
EARNINGTBESTTDIRECTORTNOMINATIONSTARETFEWTANDTFARTBETWEEN
```

CIPHER KEY: DANGKHOAVIETHOAN

ALPHABET: ABCDEFGHIJKLMNOPQRSTUVWXYZ

PRESERVE PUNCTUATION □

Vigenere DANGKHOAVIETHOANG

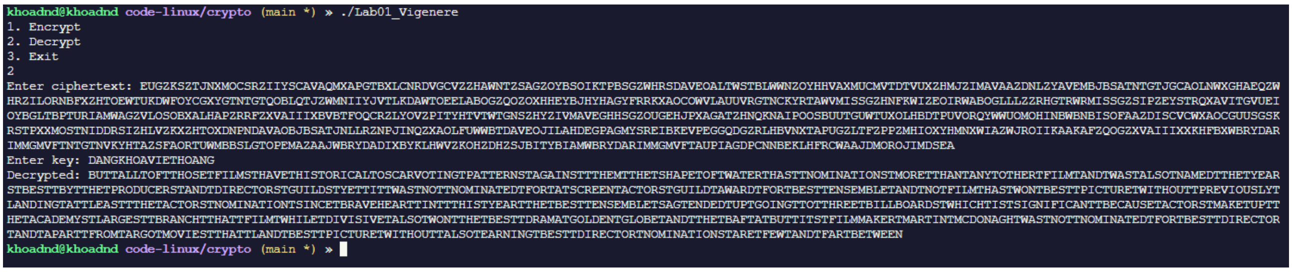
(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

```
EUGZKSZTJNXMOCSRZIIYSCAVAQMXAPGTBXLCNRDVGCVZ
ZHAWNTZSAGZOYBSOIKTPBSGZWHRSDAVEOALTWSTBLWWN
ZOYHHVAXMUCMVTDTVUXZHMJZIMAVAAZDNLZYAVEMBJBS
ATNTGTJGCAOLNWXGHAEQZWHRZILORNBFXZHTOEWTUKDW
FOYCGXYGTNTGTQOBLQTJZWMNIIYJVTLKDAWTOEELABOG
ZQOZOXHHEYBJHYHAGYFRRKXAOCOWVLAUUVRGTNCKYRTA
WVMISSGZHNFKWIZEOIRWABOGLLLZZRHGTRWRMISSGZSI
PZEYSTRQXAVITGVUEIOYBGLTBPTURIAMWAGZVLOSOBXA
LHAPZRRFZXVAIIIXBVBTFOQCRZLYOVZPITYHTVTWTGNS
ZHYZIVMAVEGHHSGZOUGEHJPXAGATZHNQKNAIPOOSBUUT
GUWTUXOLHBDTPUVORQYWWUOMOHINBWBNBISOFAAZDISC
VCWXAOCGUUSGSKRSTPXXMOSTNIDDRSIZHLVZKXZHTOXD
NPNDAVAOBJBSATJNLLRZNPJINQZXAOLFUWWBTDAVEOJI
LAHDEGPAGMYSREIBKEVPEGGQDGZRLHBVNXTAPUGZLTFZ
PPZMHIOXYHMNXWIAZWJROIIKAAKAFZQOGZXVAIIIXXKH
FBXWBRYDARIMMGMVFTNTGTNVKYHTAZSFAORTUWMBBSLG
TOPEMAZAAJWBRYDADIXBYKLHWVZKOHZDHZSJBITYBIAM
WBRYDARIMMGMVFTAUPIAGDPCNNBEKLHFRCWAAJDMOROJ
IMDSEA
```

- Decryption:
- Program:

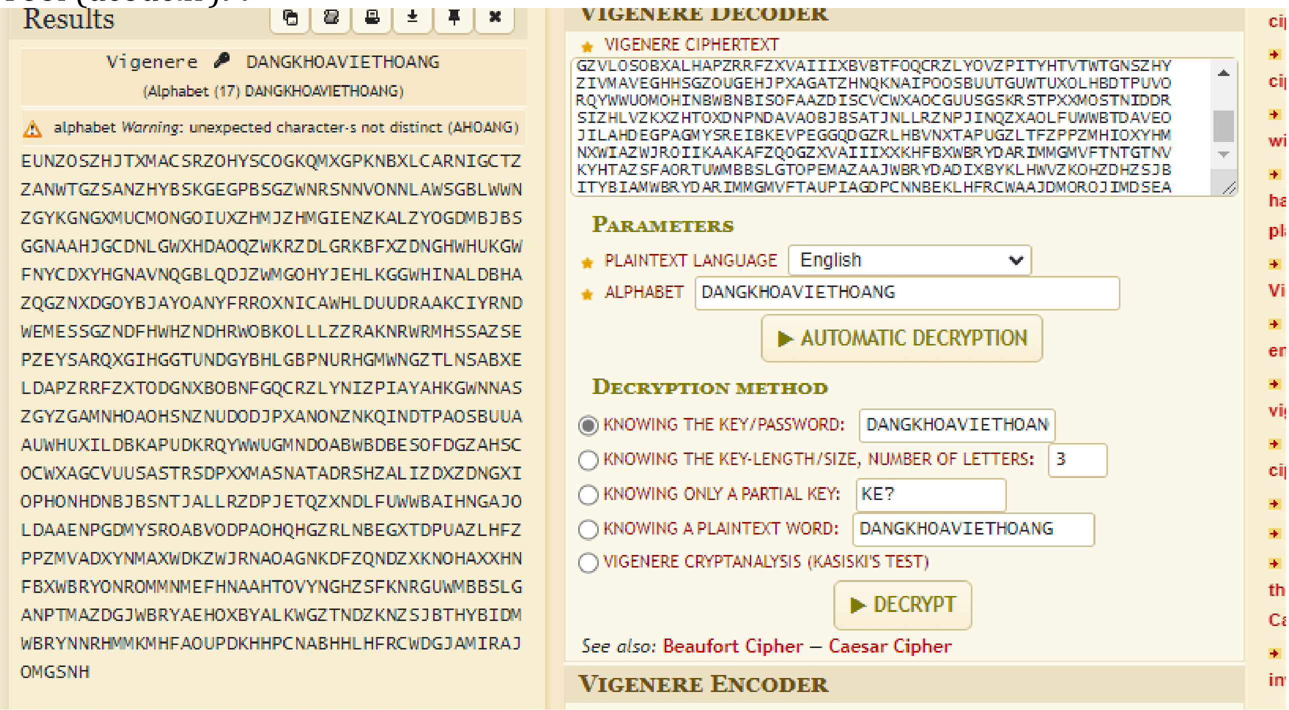
```
BUTTALLTOFTTHOSETFILMSTHAVETHISTORICALTOSCARVOTINGTPATTERNSTAGAINSTTTH
EMTTHETSHAPETOFTWATERTHASTTNOMINATIONSTMORETTHANTANYTOTHERTFILMTANDTWA
STALSOTNAMEDTTHETYEARSTBESTTBYTTHETPRODUCERSTANDTDIRECTORSTGUILDSTYETT
ITTWASTNOTTNOMINATEDTFORTATSCREENTACTORSTGUILDTAWARDTFORTBESTTENSEMBLE
TANDTNOTFILMTHASTWONTBESTTPICTURETWITHOUTTPREVIOUSLYTLANDINGTATTLEASTT
THETACTORSTNOMINATIONTSINCETBRAVEHEARTTINTTTHISTYEARTTHETBESTTENSEMBLE
TSAGTENDEDTUPTGOINGTTOTTHREETBILLBOARDSTWHICHTISTSIGNIFICANTTBECAUSETA
CTORSTMAKETUPTTHETACADEMYSTLARGESTTBRANCHTTHATTFILMTWHILETDIVISIVETALS
OTWONTTHETBESTTDRAMATGOLDENTGLOBETANDTTHETBAFTATBUTTITSTFILMMAKERTMART
INTMCDONAGHTWASTNOTTNOMINATEDTFORTBESTTDIRECTORTANDTAPARTTFROMTARGOTMO
VIESTTHATTLANDTBESTTPICTURETWITHOUTTALSOTEARNINGTBESTTDIRECTORTNOMINAT
```

IONSTARETFEWTANDTFARTBETWEEN



```
khoadnd@khoadnd code-linux/crypto (main *) » ./Lab01_Vigenere
1. Encrypt
2. Decrypt
3. Exit
2
Enter ciphertext: EUGZKSZTJNXMOCSRZIIYSCAVAQMXAPGTBXLCNRDVGCVZZHAWNTZSAGZOYBSOIKTPBSGZWHRSDAVEOALTWSTBLWWNZOYHHVAXMUCMVTDTVUXZHMJZIMAVAAZDNLZYAVEMBJBSATNTGTJGCAOLNWXGHAEQZW
HRZILORNBFXZHTOEWTUKDWFOYCGXYGTNTGTQOBLQTJZWMNIIYJVTLKDAWTOEELABOGZQOZOXHHEYBJHYHAGYFRRKXAOCOWVLAUUVRGTNCKYRTAWVMISSGZHNFKWIZEOIRWABOGLLLZZRHGTRWRMISSGZSIPZEYSTRQXAVITGVUEI
OYBGLTBPTURIAMWAGZVLOSOBXALHAPZRRFZXVAIIIXBVBTFOQCRZLYOVZPITYHTVTWTGNSZHYZIVMAVEGHHSGZOUGEHJPXAGATZHNQKNAIPOOSBUUTGUWTUXOLHBDTPUVORQYWWUOMOHINBWBNBISOFAAZDISCVCWXAOCGUUSGSK
RSTPXXMOSTNIDDRSIZHLVZKXZHTOXDNPNDAVAOBJBSATJNLLRZNPJINQZXAOLFUWWBTDAVEOJILAHDEGPAGMYSREIBKEVPEGGQDGZRLHBVNXTAPUGZLTFZPPZMHIOXYHMNXWIAZWJROIIKAAKAFZQOGZXVAIIIXXKHFBXWBRYDAR
IMMGMVFTNTGTNVKYHTAZSFAORTUWMBBSLGTOPEMAZAAJWBRYDADIXBYKLHWVZKOHZDHZSJBITYBIAMWBRYDARIMMGMVFTAUPIAGDPCNNBEKLHFRCWAAJDMOROJIMDSEA
Enter key: DANGKHOAVIETHOANG
Decrypted: BUTTALLTOFTTHOSETFILMSTHAVETHISTORICALTOSCARVOTINGTPATTERNSTAGAINSTTTHEMTTHETSHAPETOFTWATERTHASTTNOMINATIONSTMORETTHANTANYTOTHERTFILMTANDTWASTALSOTNAMEDTTHETYEAR
STBESTTBYTTHETPRODUCERSTANDTDIRECTORSTGUILDSTYETTITTWASTNOTTNOMINATEDTFORTATSCREENTACTORSTGUILDTAWARDTFORTBESTTENSEMBLETANDTNOTFILMTHASTWONTBESTTPICTURETWITHOUTTPREVIOUSLYT
LANDINGTATTLEASTTTHETACTORSTNOMINATIONTSINCETBRAVEHEARTTINTTTHISTYEARTTHETBESTTENSEMBLETSAGTENDEDTUPTGOINGTTOTTHREETBILLBOARDSTWHICHTISTSIGNIFICANTTBECAUSETACTORSTMAKETUPTT
HETACADEMYSTLARGESTTBRANCHTTHATTFILMTWHILETDIVISIVETALSOTWONTTHETBESTTDRAMATGOLDENTGLOBETANDTTHETBAFTATBUTTITSTFILMMAKERTMARTINTMCDONAGHTWASTNOTTNOMINATEDTFORTBESTTDIRECTOR
TANDTAPARTTFROMTARGOTMOVIESTTHATTLANDTBESTTPICTURETWITHOUTTALSOTEARNINGTBESTTDIRECTORTNOMINATIONSTARETFEWTANDTFARTBETWEEN
khoadnd@khoadnd code-linux/crypto (main *) » 
```

- Tool (dcode.fr): ?



Results

Vigenere 🔑 DANGKHOAVIETHOANG

(Alphabet (17) DANGKHOAVIETHOANG)

⚠ alphabet *Warning*: unexpected character-s not distinct (AHOANG)

```
EUNZOSZHJTXMACSRZOHYSCOGKQMXGPKNBXLCARNIGCTZ
ZANWTGZSANZHYBSKGEGPBSGZWNRSNNVONNLAWSGBLWWN
ZGYKGNGXMUCMONGOIUXZHMJZHMGIENZKALZYOGDMBJBS
GGNAAHJGCDNLGWXHDAOQZWKRZDLGRKBFXZDNGHWHUKGW
FNYCDXYHGNAVNQGBLQDJZWMGOHYJEHLKGGWHINALDBHA
ZQGZNXDGOYBJAYOANYFRROXNICAWHLDUUDRAAKCIYRND
WEMESSGZNDFHWHZNDHRWOBKOLLLZZRAKNRWRMHSSAZSE
PZEYSARQXGIHGGTUNDGYBHLGBPNURHGMWNGZTLNSABXE
LDAPZRRFZXTODGNXBOBNFGQCRZLYNIZPIAYAHKGWNNAS
ZGYZGAMNHOAOHSNZNUDODJPXANONZNKQINDTPAOSBUUA
AUWHUXILDBKAPUDKRQYWWUGMNDOABWBDBESOFDGZAHSC
OCWXAGCVUUSASTRSDPXXMASNATADRSHZALIZDXZDNGXI
OPHONHDNBJBSNTJALLRZDPJETQZXNDLFUWWBAIHNGAJO
LDAAENPGDMYSROABVODPAOHQHGZRLNBEGXTDPUAZLHFZ
PPZMVADXYNMAXWDKZWJRNAOAGNKDFZQNDZXKNOHAXXHN
FBXWBRYONROMMNMEFHNAAHTOVYNGHZSFKNRGUWMBBSLG
ANPTMAZDGJWBRYAEHOXBYALKWGZTNDZKNZSJBTHYBIDM
WBRYNNRHMMKMHFAOUPDKHHPCNABHHLHFRCWDGJAMIRAJ
OMGSNH
```

VIGENERE DECODER

★ VIGENERE CIPHERTEXT

```
GZVLOSOBXALHAPZRRFZXVAIIIXBVBTFOQCRZLYOVZPITYHTVTWTGNSZHY
ZIVMAVEGHHSGZOUGEHJPXAGATZHNQKNAIPOOSBUUTGUWTUXOLHBDTPUVO
RQYWWUOMOHINBWBNBISOFAAZDISCVCWXAOCGUUSGSKRSTPXXMOSTNIDDR
SIZHLVZKXZHTOXDNPNDAVAOBJBSATJNLLRZNPJINQZXAOLFUWWBTDAVEO
JILAHDEGPAGMYSREIBKEVPEGGQDGZRLHBVNXTAPUGZLTFZPPZMHIOXYHM
NXWIAZWJROIIKAAKAFZQOGZXVAIIIXXKHFBXWBRYDARIMMGMVFTNTGTNV
KYHTAZSFAORTUWMBBSLGTOPEMAZAAJWBRYDADIXBYKLHWVZKOHZDHZSJB
ITYBIAMWBRYDARIMMGMVFTAUPIAGDPCNNBEKLHFRCWAAJDMOROJIMDSEA
```

PARAMETERS

★ PLAINTEXT LANGUAGE: English

★ ALPHABET: DANGKHOAVIETHOANG

▶ AUTOMATIC DECRYPTION

DECRYPTION METHOD

● KNOWING THE KEY/PASSWORD: DANGKHOAVIETHOAN

○ KNOWING THE KEY-LENGTH/SIZE, NUMBER OF LETTERS: 3

○ KNOWING ONLY A PARTIAL KEY: KE?

○ KNOWING A PLAINTEXT WORD: DANGKHOAVIETHOANG

○ VIGENERE CRYPTANALYSIS (KASISKI'S TEST)

▶ DECRYPT

See also: Beaufort Cipher – Caesar Cipher

VIGENERE ENCODER

B. TÀI LIỆU THAM KHẢO

[1]: https://en.wikipedia.org/wiki/Caesar_cipher

[2]: https://en.wikipedia.org/wiki/Playfair_cipher