**BÁO CÁO THỰC HÀNH**

**Thực hành An toàn mạng máy tính**

**Lab 1: Classical Cryptography**

GVTH: Nguyễn Ngọc Trưởng

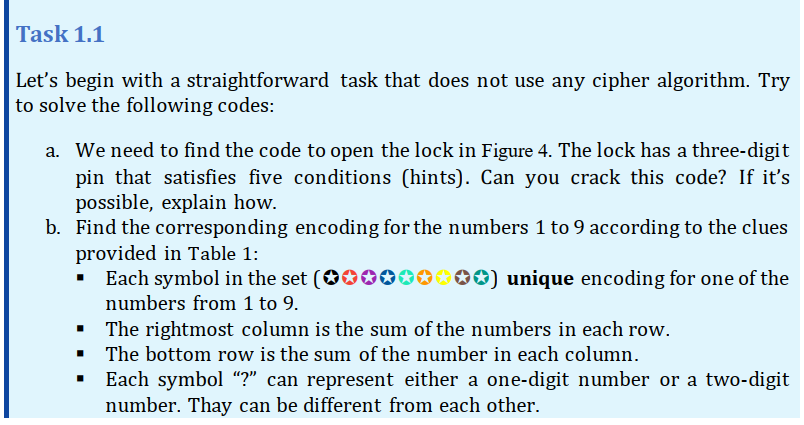
Ngày báo cáo: 03/10/2025

**Nhóm 6 – NT101.Q13**

**THÔNG TIN CHUNG**

|  |  |  |  |
| --- | --- | --- | --- |
| **MSSV** | **Họ và tên** | **Nội dung báo cáo** | **% công việc** |
| 23520580 | Trần Thanh Hùng | Câu 2, câu 4.2, câu 6 | 33,3% |
| 23520173 | Nguyễn Thái Bảo Châu | Câu 1,câu 3, câu 4 | 33,3% |
| 24521697 | Nguyễn Thành Phúc Thịnh | Câu 1, Câu 3.2, câu 5 | 33,3% |

## Kickoff: Crack the code



A number grid with numbers

AI-generated content may be incorrect.

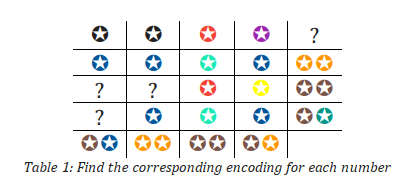
1. Đề bài

* Xét dòng 5 → Các số 4, 0 và 3 không tồn tại trong mã.
* Xét dòng 3 → Số 3 không tồn tại, còn các số 8 và 1 đúng nhưng sai vị trí.
* Xét dòng 2 → Số 3 không tồn tại; trong hai số 2 và 7 thì có một số đúng và nằm sau vị trí hiện tại.
* Xét dòng 1 → Số 1 tồn tại và đúng vị trí, nên số 1 đứng ở đầu mã.
* Xét lại dòng 5 → Số 8 đúng nhưng sai vị trí, còn các số 5 và 7 không tồn tại. Do đó, số 8 ở vị trí thứ hai và số 2 ở vị trí thứ ba trong mã.

⇒ Đáp án: 182

A screenshot of a computer code

AI-generated content may be incorrect.



1. Đề bài

* Theo bảng ta có:
* 2+2=

Ta thấy:  < 34, là số có 2 chữ số giống nhau và nó là bội số của 2.

=> =2.

* 3 +  = 

+ Ta thấy: < 34 và là số có 2 chữ số giống nhau.

*  là 1 hoặc 3.
* Giả sử: =1 => 3 + =11

Gán  và cho giá trị nhỏ nhất có thể ta có: 3\*3 + 4=12<11

=> LOẠI =1

=>=3.

Thay thế vào bảng ta được:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | ? |
|  |  |  |  | 33 |
| ? | ? |  |  | 22 |
| ? |  |  |  | 2 |
| 2 | 33 | 22 | 23 |  |

* 2+2=22 và 3 +  =33

Ta thấy: +=11 và 3 +  =33

+ Xét =1 -> =10 => LOẠI

+ Xét =4 ->=7 ->3 =26 =>LOẠI (26 không chia hết cho 3)

+ Xét =5 ->=6 ->3 =27 ->=9 => NHẬN

=> =5,=6,=9

Ta có bảng: Đặt các ? lần lượt là A,B,C,D

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | 5 |  | D |
| 9 | 9 | 6 | 9 | 33 |
| A | C | 5 |  | 22 |
| B | 9 | 6 | 9 | 2 |
| 29 | 33 | 22 | 23 |  |

* ++18=23 ->+=5.

Ta thấy: =1 và =4 hoặc =4 và =1

+ Xét trường hợp: =1 và =4

* +A+B+9=29 => +A+B=20 (a)
* 2\*9++C=33 =>+ C =15 (b)
* A+C+5+=22 =>A+C+=17 => A+C=16 (c)
* B+24=2 => 2>=24

=>  có thể là 7 hoặc 8, B có thể là 3 hoặc 4.

* Xét trường hợp: =7, B=3:

(a)-(b) =+A+B- -C=20-15 -> A-C=2 (d)

(d)+(c) =A-C+A+C=2+16 -> 2A=18 -> A=9, C=7.

(c) -> =8

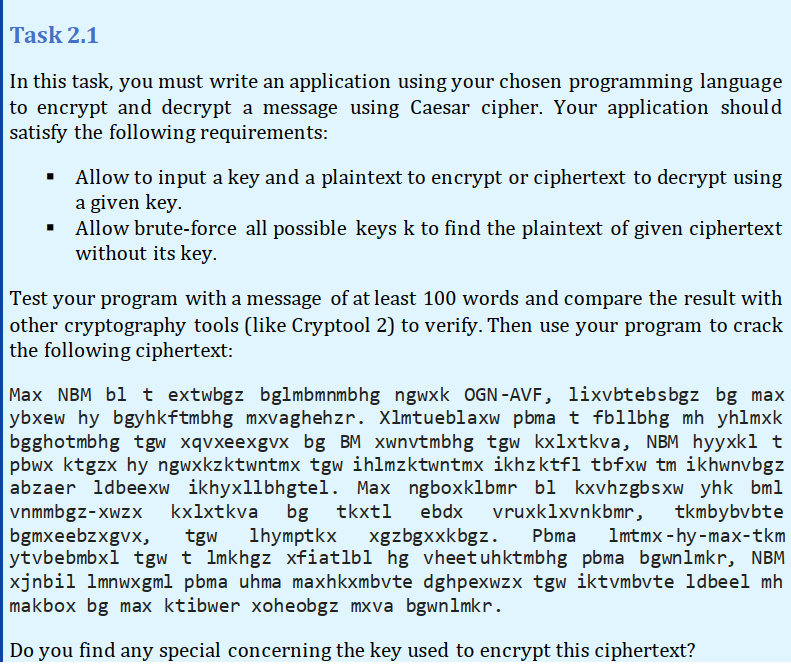
2+5+=D => D=24

=> THỎA MÃN

=> =8, =1, =4, =7, A=9, B=3, C=7, D=24

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  | A | B | C | D |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 9 | 3 | 7 | 24 |

## Caesar cipher



* Ở 2 chữ đầu, Max NBM khi dịch chuyển với k=19 thì sẽ cho ra kết quả là The UIT. Khi thực hiện tiếp với OGN-AVF thì sẽ cho kết quả là VNU-HCM
* Thực hiện chương trình thông qua mã Python:

#Định nghĩa bảng chữ cái theo chữ in hoa và in thường

ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

alphabet = "abcdefghijklmnopqrstuvwxyz"

#Thực hiện mã hóa

def encrypt(text, key):

encrypt = ""

#Lấy từng ký tự có trong text

for p in text:

#Kiểm tra ký tự in hoa

if p in ALPHABET:

#Thực hiện tìm kiếm vị trí của ký tự P trong ALPHABET

pos=ALPHABET.find(p)

#Sử dụng công thức encrypt để lấy vị trí của ký tự mới

newPos=(pos+k)%26

#Thực hiện thêm vào biến encrypt

encrypt+=ALPHABET[newPos]

#Thực hiện kiểm tra ký tự in thường, các bước còn lại giống

như trên

elif p in alphabet:

pos=alphabet.find(p)

newPos=(pos+k)%26

encrypt+=alphabet[newPos]

Else:

#Với các ký tự khác ví dụ như khoảng trắng, dấu “-”... sẽ được

thêm vào vì không được mã hóa với các ký tự đặc biệt.

encrypt+=p

return encrypt

#Thực hiện giải mã

def decrypt(encrypted,k):

decrypt = ""

#Lấy từng ký tự có trong encrypted

for c in encrypted:

#Kiểm tra ký tự in hoa

if c in ALPHABET :

#Thực hiện tìm kiếm vị trí của ký tự P trong ALPHABET

pos=ALPHABET.find(c)

#Sử dụng công thức decrypt để lấy vị trí của ký tự mới

newpos=(pos-k)%26

#Thực hiện thêm vào biến decrypt

decrypt+=ALPHABET[newpos]

#Thực hiện kiểm tra ký tự in thường, các bước còn lại giống

như trên

elif c in alphabet:

pos=alphabet.find(c)

newpos=(pos-k)%26

decrypt+=alphabet[newpos]

Else:

#Với các ký tự khác ví dụ như khoảng trắng, dấu “-”... sẽ được thêm

vào vì không giải mã với các ký tự đặc biệt.

decrypt+=c

return decrypt

#Sử dụng vét cạn cho trường hợp không rõ khóa k

def brute\_force(encrypted):

#Thực hiện chạy từ 0 đến 25

for k in range(1,26):

#Gọi hàm giải mã

text = decrypt(encrypted, k)

#in các khóa k đã giải mã

print(f"k={k:2d} -> {text}")

if \_\_name\_\_ == "\_\_main\_\_":

option=int(input("1 - Encrypt\n2 - Decrypt\n"))

if option==2:

encrypted = input("Encrypt Text: ").strip()

k=int(input("Key (0 = brute-force): ").strip())

if k==0:

brute\_force(encrypted)

else:

decrypted=decrypt(encrypted,k)

print(f"K={k} -> {decrypted}")

elif option==1:

plaintext=input("Input plaintext: ").strip()

k=int(input("Key k="))

print(encrypt(plaintext,k))

* **Các bước thực hiện mã hóa gồm:**

Bước 1: Lấy từng ký tự được nhập từ bàn phím.

Bước 2: Kiểm tra từng ký tự đó có nằm trong chuỗi của ALPHABET gồm các ký tự "ABCDEFGHIJKLMNOPQRSTUVWXYZ" là các ký tự in hoa không.

Bước 3: Nếu có thì thực hiện tìm vị trí của ký tự trong chuỗi ALPHABET.

Bước 4: Thực hiện theo công thức ***Encryption :*** C = E(k, p) = (p + k) mod 26 để tìm vị trí mới.

Bước 5: Thực hiện gán ký tự mới vào trong biến

Bước 6: Nếu không có các ký tự in hoa thì thực hiện kiểm tra ký tự trong chuỗi của alphabet và thực hiện tương tự Bước 3, 4, 5.

* **Các bước thực hiện giải mã gồm:**

Bước 1: Lấy từng ký tự được nhập từ bàn phím.

Bước 2: Kiểm tra từng ký tự đó có nằm trong chuỗi của ALPHABET gồm các ký tự "ABCDEFGHIJKLMNOPQRSTUVWXYZ" là các ký tự in hoa không.

Bước 3: Nếu có thì thực hiện tìm vị trí của ký tự trong chuỗi ALPHABET.

Bước 4: Thực hiện theo công thức ***Decryption*** : p = D(k,C) = (C- k) mod 26 để tìm vị trí mới.

Bước 5: Thực hiện gán ký tự mới vào trong biến

Bước 6: Nếu không có các ký tự in hoa thì thực hiện kiểm tra ký tự trong chuỗi của alphabet và thực hiện tương tự Bước 3, 4, 5

Bước 7: Vì khóa k chưa được biết trước nên sẽ sử dụng brute\_force để kiểm tra khóa k từ đầu. Chạy khóa k từ 1 đến 25 để tìm ra khóa chính xác nhất.

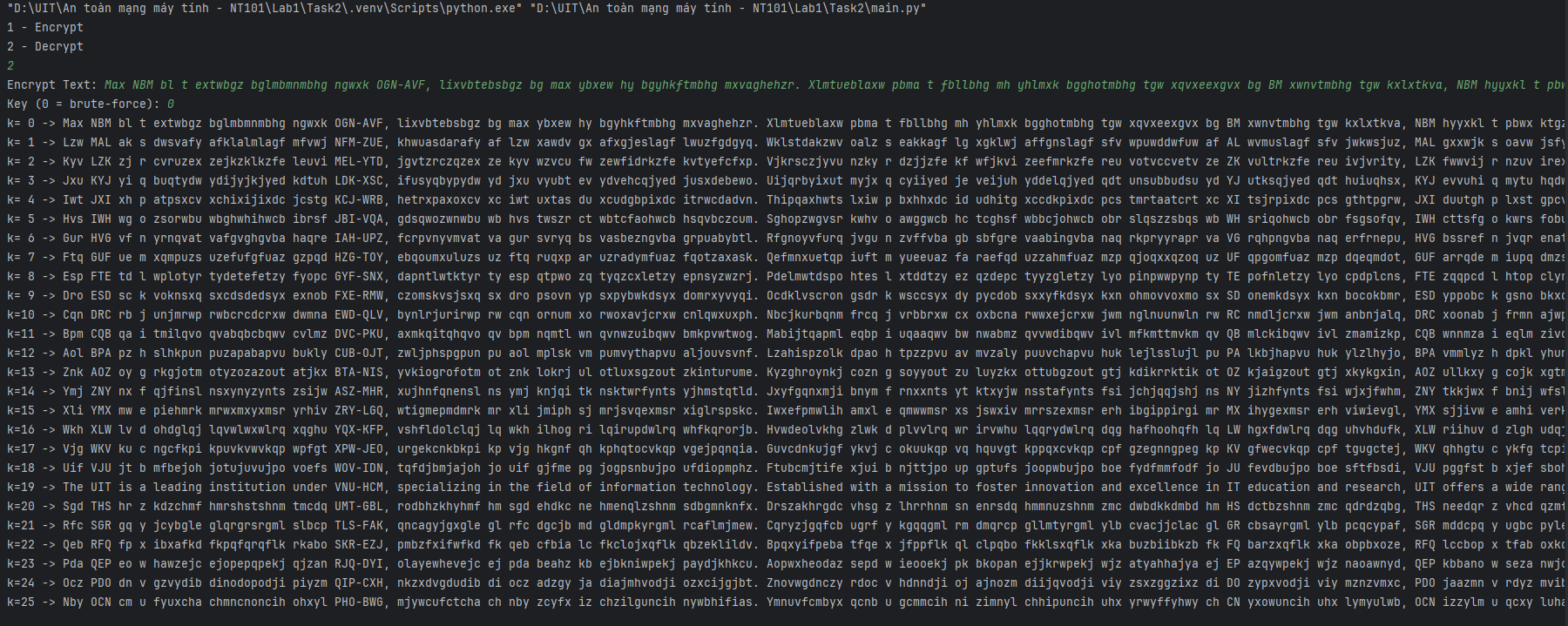
* **Thực hiện mã hóa message ít nhất 100 từ để kiểm chứng:**

Most people can readily conjure images inside their head - known as their mind's eye. But this year scientists have described a condition, aphantasia, in which some people are unable to visualise mental images. Niel Kenmuir, from Lancaster, has always had a blind mind's eye. He knew he was different even in childhood. "My stepfather, when I couldn't sleep, told me to count sheep, and he explained what he meant, I tried to do it and I couldn't," he says. "I couldn't see any sheep jumping over fences, there was nothing to count." Our memories are often tied up in images, think back to a wedding or first day at school. As a result, Niel admits, some aspects of his memory are "terrible", but he is very good at remembering facts. And, like others with aphantasia, he struggles to recognise faces. Yet he does not see aphantasia as a disability, but simply a different way of experiencing life.

* **Kết quả so sánh mã hóa:**

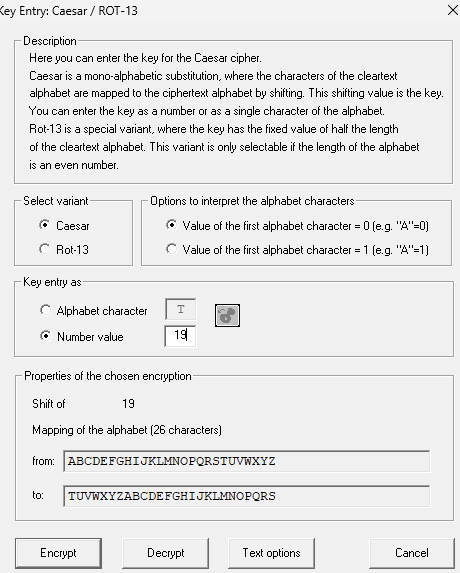
|  |  |
| --- | --- |
| **Chương trình tự thực hiện** | **Cryptool** |
| Ceij fuefbu sqd huqtybo sedzkhu ycqwui ydiytu jxuyh xuqt - ademd qi jxuyh cydt'i uou. Rkj jxyi ouqh isyudjyiji xqlu tuishyrut q sedtyjyed, qfxqdjqiyq, yd mxysx iecu fuefbu qhu kdqrbu je lyikqbyiu cudjqb ycqwui. Dyub Audckyh, vhec Bqdsqijuh, xqi qbmqoi xqt q rbydt cydt'i uou. Xu adum xu mqi tyvvuhudj ulud yd sxybtxeet. "Co ijufvqjxuh, mxud Y sekbtd'j ibuuf, jebt cu je sekdj ixuuf, qdt xu unfbqydut mxqj xu cuqdj, Y jhyut je te yj qdt Y sekbtd'j," xu iqoi. "Y sekbtd'j iuu qdo ixuuf zkcfydw eluh vudsui, jxuhu mqi dejxydw je sekdj." Ekh cucehyui qhu evjud jyut kf yd ycqwui, jxyda rqsa je q muttydw eh vyhij tqo qj isxeeb. Qi q huikbj, Dyub qtcyji, iecu qifusji ev xyi cuceho qhu "juhhyrbu", rkj xu yi luho weet qj hucucruhydw vqsji. Qdt, byau ejxuhi myjx qfxqdjqiyq, xu ijhkwwbui je husewdyiu vqsui. Ouj xu teui dej iuu qfxqdjqiyq qi q tyiqrybyjo, rkj iycfbo q tyvvuhudj mqo ev unfuhyudsydw byvu. | Ceij fuefbu sqd huqtybo sedzkhu ycqwui ydiytu jxuyh xuqt - ademd qi jxuyh cydt'i uou. Rkj jxyi ouqh isyudjyiji xqlu tuishyrut q sedtyjyed, qfxqdjqiyq, yd mxysx iecu fuefbu qhu kdqrbu je lyikqbyiu cudjqb ycqwui. Dyub Audckyh, vhec Bqdsqijuh, xqi qbmqoi xqt q rbydt cydt'i uou. Xu adum xu mqi tyvvuhudj ulud yd sxybtxeet. "Co ijufvqjxuh, mxud Y sekbtd'j ibuuf, jebt cu je sekdj ixuuf, qdt xu unfbqydut mxqj xu cuqdj, Y jhyut je te yj qdt Y sekbtd'j," xu iqoi. "Y sekbtd'j iuu qdo ixuuf zkcfydw eluh vudsui, jxuhu mqi dejxydw je sekdj." Ekh cucehyui qhu evjud jyut kf yd ycqwui, jxyda rqsa je q muttydw eh vyhij tqo qj isxeeb. Qi q huikbj, Dyub qtcyji, iecu qifusji ev xyi cuceho qhu "juhhyrbu", rkj xu yi luho weet qj hucucruhydw vqsji. Qdt, byau ejxuhi myjx qfxqdjqiyq, xu ijhkwwbui je husewdyiu vqsui. Ouj xu teui dej iuu qfxqdjqiyq qi q tyiqrybyjo, rkj iycfbo q tyvvuhudj mqo ev unfuhyudsydw byvu. |

* Cho thấy kết quả giống nhau ⇒ hoạt động đúng.
* Kết quả chạy chương trình giải mã dựa trên ciphertext đã cho:

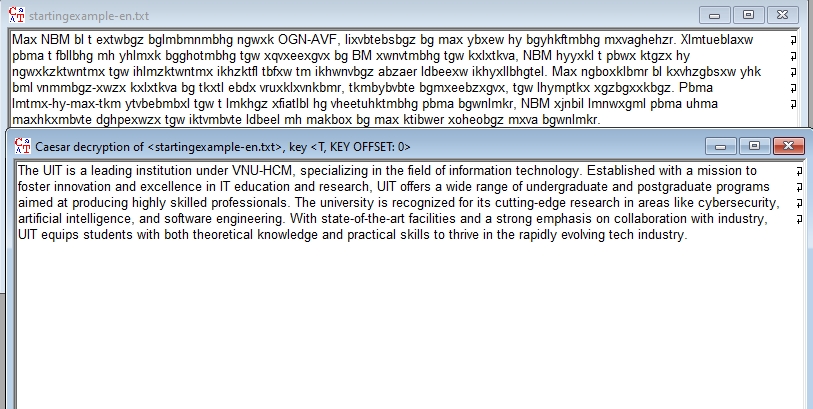


1. Kết quả khi chạy vét cạn

* Kết quả thực hiện:
* Như vậy ở K=19 sẽ cho kết quả hợp lý nhất.
* The UIT is a leading institution under VNU-HCM, specializing in the field of information technology. Established with a mission to foster innovation and excellence in IT education and research, UIT offers a wide range of undergraduate and postgraduate programs aimed at producing highly skilled professionals. The university is recognized for its cutting-edge research in areas like cybersecurity, artificial intelligence, and software engineering. With state-of-the-art facilities and a strong emphasis on collaboration with industry, UIT equips students with both theoretical knowledge and practical skills to thrive in the rapidly evolving tech industry.
* Kiểm tra lại với công cụ CryptTool:



1. Cài đặt trong Cryptool



1. Kết quả giải mã trong Cryptool

Sau khi đối chiếu kết quả thì đã thực hiện được giải mã mã Caesar cipher.

## Mono-alphabetic substitution cipher and frequency analysis

A close-up of a text

AI-generated content may be incorrect.

* Đoạn văn đã được mã hóa:

Ghv Hliib Kzggvi svirvs, uirggvm yb Yirgrsh lfghzi Q.P. Izuormt, rs zmv zd ghv nzsg kzkfoli lmw rmdofvmgrlo dlmglsb sltls zd nzwvim orgvilgfiv. Sklmmrmt svevm yzzps, ghv svirvs dzoozus ghv ordv zd l bzfmt yzb, Hliib Kzggvi, uhz wrsxzevis zm hrs 11gh yrighwlb ghlg hv rs l urcliw. Hv rs rmergvw gz lggvmw Hztuligs Sxhzzo zd Urgxhxildg lmw Urcliwib, uhviv hv ovlims lyzfg hrs nltrxlo hvirgltv, wvevozks xozsv dirvmwshrks, lmw xzmdizmgs ghv wlip dzixvs ghlg ghivlgvm ghv urcliwrmt uziow.

Ghv xvmgilo kozg ivezoevs lizfmw Hliib's zmtzrmt ylggov urgh Oziw Ezowvnzig, l wlip urcliw rmgvmg zm xzmjfvirmt yzgh ghv nltrxlo lmw mzm-nltrxlo uziows. Ls Hliib tizus zowvi, hv ovlims nziv lyzfg hrs zum nbsgvirzfs klsg, hrs xzmmvxgrzm gz Ezowvnzig, lmw ghv kizkhvxb ghlg grvs ghvri dlgvs gztvghvi. Ghizfthzfg ghv svirvs, ghvnvs zd dirvmwshrk, ozblogb, yilevib, lmw ghv kzuvi zd ozev liv vakozivw, urgh l irxh uziow droovw urgh nltrxlo xivlgfivs, skvoos, lmw wvvk nbghzoztb.

Ghv yzzps, sgligrmt urgh Hliib Kzggvi lmw ghv Khrozszkhvi's Sgzmv (1997) lmw xzmxofwrmt urgh \*Hliib Kzggvi lmw ghv Wvlghob Hloozus (2007), hlev szow zevi 500 nroorzm xzkrvs uziowurwv, yvvm gilmsolgvw rmgz nziv ghlm 80 olmtfltvs, lmw lwlkgvw rmgz l sfxxvssdfo dron svirvs. Ghv svirvs rs pmzum mzg zmob dzi rgs vmxhlmgrmt uziow-yfrowrmt yfg losz dzi lwwivssrmt wlipvi, xznkova ghvnvs sfxh ls nziglorgb, kivqfwrxv, lmw ghv lyfsv zd kzuvi. Ghv Hliib Kzggvi svirvs hls ovdg lm rmwvoryov nlip zm kzkfoli xfogfiv, dzsgvirmt l tozylo dlm ylsv, rmskrirmt xzfmgovss skrm-zdds, lmw xvnvmgrmt rgs kolxv ls l orgvilib khvmznvmzm.

Ervgmln Mlgrzmlo Fmrevisrgb, Hz Xhr Nrmh Xrgb (EMF-HXN) rs zmv zd ghv nzsg kivsgrtrzfs lmw xznkivhvmsrev hrthvi vwfxlgrzm rmsgrgfgrzms rm Ervgmln, pmzum dzi rgs vjxvoovmxv rm ivsvlixh, rmmzelgrzm, lmw vwfxlgrzm. Dzfmwvw rm 1995 yb ghv Ervgmlnvsv tzevimnvmg, EMF-HXN uls vsglyorshvw ls l pvb xvmgvi dzi gilrmrmt, ivsvlixh, lmw gvxhmzoztb gilmsdvi urgh ghv nrssrzm zd xzmgiryfgrmt gz ghv xzfmgib’s szxrz-vxzmznrx wvevozknvmg. Ls l doltshrk fmrevisrgb, rg hls kolbvw l krezglo izov rm kizwfxrmt hrthob sproovw kizdvssrzmlos, sxrvmgrsgs, lmw ovlwvis lxizss nfogrkov drvows.

EMF-HXN zkvilgvs fmwvi l wrsgrmxgrev sgifxgfiv ls l nfogr-wrsxrkormlib lmw nfogr-xlnkfs sbsgvn, xznkirsrmt svevilo nvnyvi fmrevisrgrvs lmw ivsvlixh rmsgrgfgvs. Ghvsv rmxofwv sznv zd ghv nzsg uvoo-vsglyorshvw rmsgrgfgrzms rm ghv ivtrzm, sfxh ls ghv Fmrevisrgb zd Sxrvmxv, Fmrevisrgb zd Gvxhmzoztb, Fmrevisrgb zd Szxrlo Sxrvmxvs lmw Hfnlmrgrvs, Rmgvimlgrzmlo Fmrevisrgb, Fmrevisrgb zd Vxzmznrxs lmw Olu, lmw zghvis. Vlxh zd ghvsv nvnyvi rmsgrgfgrzms zkvilgvs svnr-rmwvkvmwvmgob yfg xzoolyzilgvs fmwvi ghv fnyivool zd EMF-HXN, nlprmt rg l fmrafv hrthvi vwfxlgrzm nzwvo rm Ervgmln ghlg kiznzgvs rmgviwrsxrkormlib ovlimrmt lmw ivsvlixh.

Ozxlgvw rm Hz Xhr Nrmh Xrgb, ghv xzfmgib's vxzmznrx lmw xfogfilo hfy, EMF-HXN yvmvdrgs dizn xozsv grvs urgh rmwfsgirvs, yfsrmvssvs, lmw tzevimnvmg ltvmxrvs. Ghrs kizjrnrgb dzsgvis xzoolyzilgrzm rm ivsvlixh, rmgvimshrks, lmw qzy kolxvnvmg, vmsfirmt ghlg rgs tilwflgvs liv uvoo-kivklivw gz nvvg ghv wvnlmws zd lm vezoermt uzipdzixv. Ghv fmrevisrgb rs xznnrggvw gz kizwfxrmt tilwflgvs uhz liv mzg zmob lxlwvnrxloob kizdrxrvmg yfg losz vafrkkvw urgh kilxgrxlo sproos lmw l tozylo zfgozzp.

EMF-HXN rs ivmzumvw dzi rgs sgizmt vnkhlsrs zm sxrvmgrdrx ivsvlixh lmw gvxhmzoztrxlo rmmzelgrzm. Rg hzfsvs mfnvizfs ivsvlixh xvmgvis, rmsgrgfgvs, lmw olys ghlg dzxfs zm elirzfs livls zd sxrvmxv, vmtrmvvirmt, szxrlo sxrvmxvs, vxzmznrxs, lmw nziv. Ghv fmrevisrgb's ivsvlixh ltvmwl rs lortmvw urgh mlgrzmlo kirzirgrvs, dzxfsrmt zm livls sfxh ls rmdzinlgrzm gvxhmzoztb, yrzgvxhmzoztb, ivmvulyov vmvitb, lmw vmerizmnvmglo sfsglrmlyrorgb. EMF-HXN losz lxgrevob vmtltvs rm rmgvimlgrzmlo xzzkvilgrzm, kligmvirmt urgh ovlwrmt fmrevisrgrvs lmw ivsvlixh rmsgrgfgrzms uziowurwv gz vmhlmxv rgs lxlwvnrx kiztilns, dzsgvi qzrmg ivsvlixh kizqvxgs, lmw kiznzgv sgfwvmg lmw dlxfogb vjxhlmtvs.

Ghv fmrevisrgb rs losz wvvkob rmezoevw rm lwwivssrmt tozylo xhloovmtvs ghizfth rgs ivsvlixh lmw vwfxlgrzmlo kiztilns. EMF-HXN kolxvs l sgizmt vnkhlsrs zm sfsglrmlyov wvevozknvmg, vmerizmnvmglo xzmsvielgrzm, lmw gvxhmzoztrxlo rmmzelgrzm, lortmrmt rgs tzlos urgh ghv Fmrgvw Mlgrzms’ Sfsglrmlyov Wvevozknvmg Tzlos (SWTs). Ghv rmsgrgfgrzm vmxzfiltvs rgs dlxfogb lmw sgfwvmgs gz kfisfv ivsvlixh ghlg hls l nvlmrmtdfo rnklxg zm yzgh ghv ozxlo lmw tozylo xznnfmrgb.

Rm gvins zd sgfwvmg ordv, EMF-HXN zddvis l eryilmg lmw wbmlnrx vmerizmnvmg. Urgh l sgfwvmg yzwb zd zevi 60,000 lmw l dlxfogb zd hrthob aflordrvw kizdvsszis lmw ivsvlixhvis, ghv fmrevisrgb kizerwvs l irxh lxlwvnrx lmw szxrlo vjkvirvmxv. Ghv xlnkfsvs liv vafrkkvw urgh nzwvim dlxrorgrvs, rmxofwrmt oryilirvs, olyzilgzirvs, skzigs xznkovjvs, lmw wzinrgzirvs, xivlgrmt l sfkkzigrev ovlimrmt vmerizmnvmg. Sgfwvmgs losz hlev lxxvss gz l elirvgb zd vjgilxfiirxfoli lxgrergrvs, xofys, lmw zitlmrclgrzms, loozurmt ghvn gz vmtltv rm xfogfilo, szxrlo, lmw kizdvssrzmlo wvevozknvmg lozmtsrwv ghvri sgfwrvs.

Rm xzmxofsrzm, Ervgmln Mlgrzmlo Fmrevisrgb - Hz Xhr Nrmh Xrgb sglmws ls l ovlwrmt vwfxlgrzmlo rmsgrgfgrzm rm Ervgmln, xzmgiryfgrmt srtmrdrxlmgob gz ghv xzfmgib’s rmgvoovxgflo, sxrvmgrdrx, lmw vxzmznrx kiztivss. Rgs xznnrgnvmg gz lxlwvnrx vjxvoovmxv, ivsvlixh rmmzelgrzm, lmw szxrvglo rnklxg hls kzsrgrzmvw rg ls l xifxrlo kolbvi rm shlkrmt ghv dfgfiv zd Ervgmln lmw ghv yizlwvi ivtrzm. Ls rg xzmgrmfvs gz vezoev lmw vjklmw, EMF-HXN ivnlrms wvwrxlgvw gz dzsgvirmt ghv mvjg tvmvilgrzm zd ovlwvis lmw rmmzelgzis uhz uroo wirev sfsglrmlyov tizugh lmw tozylo kiztivss.

**→ Bài làm:**

* Sau khi tiến hành phân tích đoạn văn bản mã bằng CrypTool Online, nhận thấy ký tự **V** xuất hiện nhiều nhất (39 lần). Trong tiếng Anh, chữ cái phổ biến nhất là **E**, do đó có thể giả định rằng **V ↔ E**. Quan sát tiếp, cụm **GHV** xuất hiện nhiều lần, nếu thay thế thì sẽ khớp với từ “THE”. Từ đây suy ra ánh xạ: **G → T, H → H, V → E**. Như vậy, có thể thấy rằng quy tắc mã hoá gần giống với Atbash, trong đó **G → T** và **V → E** tuân theo quy luật, còn **H → H** là một trường hợp đặc biệt.
* Tiếp tục, chữ **L** xuất hiện đơn lẻ. Trong tiếng Anh, chữ cái phổ biến nhất đứng một mình là “A”. Vì vậy có thể phỏng đoán rằng **L → A** (trường hợp đặc biệt thứ hai). Sau cụm “GHV”, xuất hiện từ **LMW**, nếu thay thế sẽ cho ra “AND” (vì đây là một từ tiếng anh thông dụng gồm ba chữ cái và bắt đầu bằng chữ **A**). Do đó xác định thêm ánh xạ: **M → N, W → D**.
* Xét tiếp từ **RS** (hai ký tự lặp lại nhiều trong bản mã). Thực hiện theo quy luật Atbash, suy ra **R → I**. Khi đó, từ **RS** khớp với từ “IS”(1 từ tiếng anh thông dụng nhất gồm 2 chữ cái và bắt đầu bằng **I**) trong tiếng Anh. Như vậy, **S → S** là một trường hợp đặc biệt khác.
* Dựa vào nguyên tắc của Atbash: **A ↔ Z, L ↔ O**, trong bản mã ta đã xác định **L → A**, nên có thể suy ra thêm rằng **O → L**.
* Từ các phân tích trên, ta xây dựng được một phần bảng thay thế ký tự trong hệ mã như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Mã hóa | Gốc | Mã hóa | Gốc | Mã hóa | Gốc | Mã hóa | Gốc |
| A | L(db) | H | H (db) | O | Z(db) | V | E |
| B | Y | I | R | P | K | W | D |
| C | X | J | Q | Q | J | X | C |
| D | W | K | P | R | I | Y | B |
| E | V | L | A(db) | S | S(db) | Z | O(db) |
| F | U | M | N | T | G |  |  |
| G | T | N | M | U | F |  |  |

* Sau khi ánh xạ đoạn mã theo bảng chữ cái trên ta được đoạn văn đã được giải mã sau:

THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR J.K. ROWLING, IS ONE OF THE MOST POPULAR AND INFLUENTIAL WORKS OF MODERN LITERATURE. SPANNING SEVEN BOOKS, THE SERIES FOLLOWS THE LIFE OF A YOUNG BOY, HARRY POTTER, WHO DISCOVERS ON HIS 11TH BIRTHDAY THAT HE IS A WIZARD. HE IS INVITED TO ATTEND HOGWARTS SCHOOL OF WITCHCRAFT AND WIZARDRY, WHERE HE LEARNS ABOUT HIS MAGICAL HERITAGE, DEVELOPS CLOSE FRIENDSHIPS, AND COMBATS THE DARK FORCES THAT THREATEN THE WIZARDING WORLD.

THE CENTRAL PLOT REVOLVES AROUND HARRY'S ONGOING BATTLE WITH LORD VOLDEMORT, A DARK WIZARD INTENT ON CONQUERING BOTH THE MAGICAL AND NON-MAGICAL WORLDS. AS HARRY GROWS OLDER, HE LEARNS MORE ABOUT HIS MYSTERIOUS PAST, HIS CONNECTION TO VOLDEMORT, AND THE PROPHECY THAT TIES THEIR FATES TOGETHER. THROUGHOUT THE SERIES, THEMES OF FRIENDSHIP, LOYALTY, BRAVERY, AND THE POWER OF LOVE ARE EXPLORED, WITH A RICH WORLD FILLED WITH MAGICAL CREATURES, SPELLS, AND DEEP MYSTOLOGY.

THE BOOKS, STARTING WITH HARRY POTTER AND THE PHILOSOPHER'S STONE (1997) AND CONCLUDING WITH HARRY POTTER AND THE DEATHLY HALLOWS (2007), HAVE SOLD OVER 500 MILLION COPIES WORLDWIDE, BEEN TRANSLATED INTO MORE THAN 80 LANGUAGES, AND ADAPTED INTO A SUCCESSFUL FILM SERIES. THE SERIES IS KNOWN NOT ONLY FOR ITS ENCHANTING WORLD-BUILDING BUT ALSO FOR ADDRESSING DARKER, COMPLEX THEMES SUCH AS MORTALITY, PREJUDICE, AND THE ABUSE OF POWER. THE HARRY POTTER SERIES HAS LEFT AN INDELIBLE MARK ON POPULAR CULTURE, CREATING A GLOBAL PHENOMENON, INSPIRING COUNTLESS SPIN-OFFS, AND CEMENTING ITS PLACE AS A LITERARY PHENOMENON.

VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY (VNU-HCM) IS ONE OF THE MOST PRESTIGIOUS AND COMPREHENSIVE HIGHER EDUCATION INSTITUTIONS IN VIETNAM, KNOWN FOR ITS EXCELLENCE IN RESEARCH, INNOVATION, AND EDUCATION. FOUNDED IN 1995 BY THE VIETNAMESE GOVERNMENT, VNU-HCM WAS ESTABLISHED AS A KEY CENTER FOR TRAINING, RESEARCH, AND TECHNOLOGY TRANSFER WITH THE MISSION OF CONTRIBUTING TO THE COUNTRY’S SOCIO-ECONOMIC DEVELOPMENT. AS A FLAGSHIP UNIVERSITY, IT HAS PLAYED A PIVOTAL ROLE IN PRODUCING HIGHLY SKILLED PROFESSIONALS, SCIENTISTS, AND LEADERS ACROSS MULTIPLE FIELDS.

VNU-HCM OPERATES UNDER A DISTINCTIVE STRUCTURE AS A MULTI-DISCIPLINARY AND MULTI-CAMPUS SYSTEM, COMPRISING SEVERAL MEMBER UNIVERSITIES AND RESEARCH INSTITUTES. THESE INCLUDE SOME OF THE MOST WELL-ESTABLISHED INSTITUTIONS IN THE REGION, SUCH AS THE UNIVERSITY OF SCIENCE, UNIVERSITY OF TECHNOLOGY, UNIVERSITY OF SOCIAL SCIENCES AND HUMANITIES, INTERNATIONAL UNIVERSITY, UNIVERSITY OF ECONOMICS AND LAW, AND OTHERS. EACH OF THESE MEMBER INSTITUTIONS OPERATES SEMI-INDEPENDENTLY BUT COLLABORATES UNDER THE UMBRELLA OF VNU-HCM, MAKING IT A UNIQUE HIGHER EDUCATION MODEL IN VIETNAM THAT PROMOTES INTERDISCIPLINARY LEARNING AND RESEARCH.

LOCATED IN HO CHI MINH CITY, THE COUNTRY'S ECONOMIC AND CULTURAL HUB, VNU-HCM BENEFITS FROM CLOSE TIES WITH INDUSTRIES, BUSINESSES, AND GOVERNMENT AGENCIES. THIS PROXIMITY FOSTERS COLLABORATION IN RESEARCH, INTERNSHIPS, AND JOB PLACEMENT, ENSURING THAT ITS GRADUATES ARE WELL-PREPARED TO MEET THE DEMANDS OF AN EVOLVING WORKFORCE. THE UNIVERSITY IS COMMITTED TO PRODUCING GRADUATES WHO ARE NOT ONLY ACADEMICALLY PROFICIENT BUT ALSO EQUIPPED WITH PRACTICAL SKILLS AND A GLOBAL OUTLOOK.

VNU-HCM IS RENOWNED FOR ITS STRONG EMPHASIS ON SCIENTIFIC RESEARCH AND TECHNOLOGICAL INNOVATION. IT HOUSES NUMEROUS RESEARCH CENTERS, INSTITUTES, AND LABS THAT FOCUS ON A VARIOUS AREAS OF SCIENCE, ENGINEERING, SOCIAL SCIENCES, ECONOMICS, AND MORE. THE UNIVERSITY'S RESEARCH AGENDA IS ALIGNED WITH NATIONAL PRIORITIES, FOCUSING ON AREAS SUCH AS INFORMATION TECHNOLOGY, BIOTECHNOLOGY, RENEWABLE ENERGY, AND ENVIRONMENTAL SUSTAINABILITY. VNU-HCM ALSO ACTIVELY ENGAGES IN INTERNATIONAL COOPERATION, PARTNERING WITH LEADING UNIVERSITIES AND RESEARCH INSTITUTIONS WORLDWIDE TO ENHANCE ITS ACADEMIC PROGRAMS, FOSTER JOINT RESEARCH PROJECTS, AND PROMOTE STUDENT AND FACULTY EXCHANGES.

THE UNIVERSITY IS ALSO DEEPLY INVOLVED IN ADDRESSING GLOBAL CHALLENGES THROUGH ITS RESEARCH AND EDUCATIONAL PROGRAMS. VNU-HCM PLACES A STRONG EMPHASIS ON SUSTAINABLE DEVELOPMENT, ENVIRONMENTAL CONSERVATION, AND TECHNOLOGICAL INNOVATION, ALIGNING ITS GOALS WITH THE UNITED NATIONS’ SUSTAINABLE DEVELOPMENT GOALS (SDGS). THE INSTITUTION ENCOURAGES ITS FACULTY AND STUDENTS TO PURSUE RESEARCH THAT HAS A MEANINGFUL IMPACT ON BOTH THE LOCAL AND GLOBAL COMMUNITY.

IN TERMS OF STUDENT LIFE, VNU-HCM OFFERS A VIBRANT AND DYNAMIC ENVIRONMENT. WITH A STUDENT BODY OF OVER 60,000 AND A FACULTY OF HIGHLY QUALIFIED PROFESSORS AND RESEARCHERS, THE UNIVERSITY PROVIDES A RICH ACADEMIC AND SOCIAL EXPERIENCE. THE CAMPUSES ARE EQUIPPED WITH MODERN FACILITIES, INCLUDING LIBRARIES, LABORATORIES, SPORTS COMPLEXES, AND DORMITORIES, CREATING A SUPPORTIVE LEARNING ENVIRONMENT. STUDENTS ALSO HAVE ACCESS TO A VARIETY OF EXTRACURRICULAR ACTIVITIES, CLUBS, AND ORGANIZATIONS, ALLOWING THEM TO ENGAGE IN CULTURAL, SOCIAL, AND PROFESSIONAL DEVELOPMENT ALONGSIDE THEIR STUDIES.

IN CONCLUSION, VIETNAM NATIONAL UNIVERSITY - HO CHI MINH CITY STANDS AS A LEADING EDUCATIONAL INSTITUTION IN VIETNAM, CONTRIBUTING SIGNIFICANTLY TO THE COUNTRY'S INTELLECTUAL, SCIENTIFIC, AND ECONOMIC PROGRESS. ITS COMMITMENT TO ACADEMIC EXCELLENCE, RESEARCH INNOVATION, AND SOCIETAL IMPACT HAS POSITIONED IT AS A CRUCIAL PLAYER IN SHAPING THE FUTURE OF VIETNAM AND THE BROADER REGION. AS IT CONTINUES TO EVOLVE AND EXPAND, VNU-HCM REMAINS DEDICATED TO FOSTERING THE NEXT GENERATION OF LEADERS AND INNOVATORS WHO WILL DRIVE SUSTAINABLE GROWTH AND GLOBAL PROGRESS.

**A blue background with black text

AI-generated content may be incorrect.**

**A blue background with black text

AI-generated content may be incorrect.**

**Đoạn văn được mã hóa:**

67\* 7-881 0+66\*8 %\*8$\*%, &8$66\*= \_1 \_8$6$%7 -567+8 #.@. 8+&!$=^, $% +=\* +3 67\* ~+%6 0+05!-8 -=( $=3!5\*=6$-! 3-=6-%1 %-^-% +3 ~+(\*8= !$6\*8-658\*. %0-==$=^ %\*4\*= \_++@%, 67\* %\*8$\*% 3+!!+&% 67\* !$3\* +3 - 1+5=^ \_+1, 7-881 0+66\*8, &7+ ($%)+4\*8% += 7$% ``67 \_$867(-1 67-6 7\* $% - &$2-8(. 7\* $% $=4$6\*( 6+ -66\*=( 7+^&-86% %)7++! +3 &$6)7)8-36 -=( &$2-8(81, &7\*8\* 7\* !\*-8=% -\_+56 7$% ~-^$)-! 7\*8$6-^\*, (\*4\*!+0% )!+%\* 38$\*=(%7$0%, -=( )+=38+=6% 67\* (-8@ 3+8)\*% 67-6 678\*-6\*= 67\* &$2-8($=^ &+8!(.

67\* )\*=68-! 0!+6 8\*4+!4\*% -8+5=( 7-881'% +=^+$=^ \_-66!\* &$67 !+8( 4+!(\*~+86, - (-8@ &$2-8( $=6\*=6 += )+=95\*8$=^ \_+67 67\* ~-^$)-! -=( =+=)~-^$)-! &+8!(%. -% 7-881 ^8+&% +!(\*8, 7\* !\*-8=% ~+8\* -\_+56 7$% +&= ~1%6\*8$+5% 0-%6, 7$% )+==\*)6$+= 6+ 4+!(\*~+86, -=( 67\* 08+07\*)1 67-6 6$\*% 67\*$8 3-6\*% 6+^\*67\*8. 678+5^7+56 67\* %\*8$\*%, 67\*~\*% +3 38$\*=(%7$0, !+1-!61, \_8-4\*81, -=( 67\* 0+&\*8 +3 !+4\* -8\* \*+0!+8\*(, &$67 - 8$)7 &+8!( 3$!!\*( &$67 ~-^$)-! )8\*-658\*%, %0\*!!%, -=( (\*\*0 ~167+!+^1.

67\* \_++@%, %6-86$=^ &$67 7-881 0+66\*8 -=( 67\* 07$!+%+07\*8'% %6+=\* %`886^ -=( )+=)!5($=^ &$67 $7-881 0+66\*8 -=( 67\* (\*-67!1 7-!!+&% %1996^, 7-4\* %+!( +4\*8 499 ~$!!$+= )+0$\*% &+8!(&$(\*, \_\*\*= 68-=%!-6\*( $=6+ ~+8\* 67-= 79 !-=^5-^\*%, -=( -(-06\*( $=6+ - %5))\*%%35! 3$!~ %\*8$\*%. 67\* %\*8$\*% $% @=+&= =+6 +=!1 3+8 $6% \*=)7-=6$=^ &+8!()\_5$!($=^ \_56 -!%+ 3+8 -((8\*%%$=^ (-8@\*8, )+~0!\*+ 67\*~\*% %5)7 -% ~+86-!$61, 08\*#5($)\*, -=( 67\* -\_5%\* +3 0+&\*8. 67\* 7-881 0+66\*8 %\*8$\*% 7-% !\*36 -= $=(\*!$\_!\* ~-8@ += 0+05!-8 )5!658\*, 3+%6\*8$=^ - ^!+\_-! 3-= \_-%\*, $=%0$8$=^ )+5=6!\*%% %0$=)+33%, -=( )\*~\*=6$=^ $6% 0!-)\* -% - !$6\*8-81 07\*=+~\*=+=.

**→ Bài làm:**

* Sau khi tiến hành phân tích đoạn văn bản mã bằng CrypTool Online, nhận thấy ký tự **\*** xuất hiện nhiều nhất (133 lần). Trong tiếng Anh, chữ cái phổ biến nhất là **E**, do đó có thể giả định rằng **\* ↔ E**. Quan sát tiếp, cụm **67\*** xuất hiện nhiều lần, nếu thay thế thì sẽ khớp với từ “THE”. Từ đây suy ra ánh xạ: **6 → T, 7 → H, \* → E**.
* Tiếp đó, ta thấy đoạn văn có cụm 67-6, sau khi ánh xạ với các kí tự đã xác định từ trước thì nó là THAT. - →A.
* Ta thấy kí tự + xuất hiện 108 lần, dựa vào độ phổ biến của các chữ cái tiếng anh thì chữ xuất hiện nhiều nhất sau E, A, T là O. Ta dự đoán + → O.
* Từ tiếp sau từ 67\* là 7-881 ánh xạ với những chữ cái đã biết thì ta được từ HA\*\*1. Ta thấy được kí tự 8 xuất hiện 103 lần vậy nên nó sẽ là 1 trong những chữ cái thông dụng là S, R, N; ngoài ra kí tự 1 cuối cùng là kí tự kết thúc và thường là Y. Dự đoán 1 →Y. Vậy là từ của mình sẽ là HARRY vì nếu thay S hoặc N vào thì tên đó rất hiếm. 8 →R
* Từ tiếp là 0+66\*8 sau khi ánh xạ thì thu được 0OTTER. Nhìn qua khả năng cao sẽ là HARRY POTTER để thành 1 cụm có nghĩa. Vậy 0→ P.
* Từ %\*8$\*%: ta thấy % xuất hiện 63 lần và $ xuất hiện 60 lần. Chúng có thể là những kí tự thay thế cho S, I. Và sau khi sắp xếp thì nó ra chữ SERIES là có nghĩa. %→S và $→I.
* **Sau khi ánh xạ các từ vào đoạn mã thì ta được đoạn sau:**

THE HARRY POTTER SERIES, &RITTE= \_Y \_RITISH A5THOR #.@. RO&!I=^, IS O=E O3 THE ~OST POP5!AR A=( I=3!5E=TIA! 3A=TASY SA^AS O3 ~O(ER= !ITERAT5RE. SPA==I=^ SE4E= \_OO@S, THE SERIES 3O!!O&S THE !I3E O3 A YO5=^ \_OY, HARRY POTTER, &HO (IS)O4ERS O= HIS ``TH \_IRTH(AY THAT HE IS A &I2AR(. HE IS I=4ITE( TO ATTE=( HO^&ARTS S)HOO! O3 &IT)H)RA3T A=( &I2AR(RY, &HERE HE !EAR=S A\_O5T HIS ~A^I)A! HERITA^E, (E4E!OPS )!OSE 3RIE=(SHIPS, A=( )O=3RO=TS THE (AR@ 3OR)ES THAT THREATE= THE &I2AR(I=^ &OR!(.

THE )E=TRA! P!OT RE4O!4ES ARO5=( HARRY'S O=^OI=^ \_ATT!E &ITH !OR( 4O!(E~ORT, A (AR@ &I2AR( I=TE=T O= )O=95ERI=^ \_OTH THE ~A^I)A! A=( =O=)~A^I)A! &OR!(S. AS HARRY ^RO&S O!(ER, HE !EAR=S ~ORE A\_O5T HIS O&= ~YSTERIO5S PAST, HIS )O==E)TIO= TO 4O!(E~ORT, A=( THE PROPHE)Y THAT TIES THEIR 3ATES TO^ETHER. THRO5^HO5T THE SERIES, THE~ES O3 3RIE=(SHIP, !OYA!TY, \_RA4ERY, A=( THE PO&ER O3 !O4E ARE EOP!ORE(, &ITH A RI)H &OR!( 3I!!E( &ITH ~A^I)A! )REAT5RES, SPE!!S, A=( (EEP ~YTHO!O^Y.

THE \_OO@S, STARTI=^ &ITH HARRY POTTER A=( THE PHI!OSOPHER'S STO=E S`RRT^ A=( )O=)!5(I=^ &ITH IHARRY POTTER A=( THE (EATH!Y HA!!O&S SY99T^, HA4E SO!( O4ER 499 ~I!!IO= )OPIES &OR!(&I(E, \_EE= TRA=S!ATE( I=TO ~ORE THA= H9 !A=^5A^ES, A=( A(APTE( I=TO A S5))ESS35! 3I!~ SERIES. THE SERIES IS @=O&= =OT O=!Y 3OR ITS E=)HA=TI=^ &OR!()\_5I!(I=^ \_5T A!SO 3OR A((RESSI=^ (AR@ER, )O~P!EO THE~ES S5)H AS ~ORTA!ITY, PRE#5(I)E, A=( THE A\_5SE O3 PO&ER. THE HARRY POTTER SERIES HAS !E3T A= I=(E!I\_!E ~AR@ O= POP5!AR )5!T5RE, 3OSTERI=^ A ^!O\_A! 3A= \_ASE, I=SPIRI=^ )O5=T!ESS SPI=)O33S, A=( )E~E=TI=^ ITS P!A)E AS A !ITERARY PHE=O~E=O=.

* Cụm &RITTE= ta thấy nó chỉ trùng với từ WRITTEN. &→W, = →N.
* Sau WRITTEN là \_Y và từ có 2 kí tự có Y cuối sau V3/ed là BY. \_→B.
* Cụm A5THOR thì trùng với AUTHOR. Vậy 5→U.
* Ta thấy cụm IS ONE O3 THE ~OST POPU!AR nó sẽ trùng với IS ONE OF THE MOST POPULAR. 3→F, ~ →M, !→L.
* MO(ERN là MODERN. ( →D.
* SPANNIN^ là SPANNING. ^→G.
* SE4EN là SEVEN. 4 →V.
* BOO@S là BOOKS. @→K.
* DIS(OVERS là DISCOVER. )→C.
* WI2ARD là WIZARD. 2→Z.
* **Đoạn văn sau khi ánh xạ các kí tự:**

THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR #.K. ROWLING, IS ONE OF THE MOST POPULAR AND INFLUENTIAL FANTASY SAGAS OF MODERN LITERATURE. SPANNING SEVEN BOOKS, THE SERIES FOLLOWS THE LIFE OF A YOUNG BOY, HARRY POTTER, WHO DISCOVERS ON HIS ``TH BIRTHDAY THAT HE IS A WIZARD. HE IS INVITED TO ATTEND HOGWARTS SCHOOL OF WITCHCRAFT AND WIZARDRY, WHERE HE LEARNS ABOUT HIS MAGICAL HERITAGE, DEVELOPS CLOSE FRIENDSHIPS, AND CONFRONTS THE DARK FORCES THAT THREATEN THE WIZARDING WORLD.

THE CENTRAL PLOT REVOLVES AROUND HARRY'S ONGOING BATTLE WITH LORD VOLDEMORT, A DARK WIZARD INTENT ON CON9UERING BOTH THE MAGICAL AND NONCMAGICAL WORLDS. AS HARRY GROWS OLDER, HE LEARNS MORE ABOUT HIS OWN MYSTERIOUS PAST, HIS CONNECTION TO VOLDEMORT, AND THE PROPHECY THAT TIES THEIR FATES TOGETHER. THROUGHOUT THE SERIES, THEMES OF FRIENDSHIP, LOYALTY, BRAVERY, AND THE POWER OF LOVE ARE EXPLORED, WITH A RICH WORLD FILLED WITH MAGICAL CREATURES, SPELLS, AND DEEP MYTHOLOGY.

THE BOOKS, STARTING WITH HARRY POTTER AND THE PHILOSOPHER'S STONE S`RRTG AND CONCLUDING WITH HARRY POTTER AND THE DEATHLY HALLOWS SY99TG, HAVE SOLD OVER V99 MILLION COPIES WORLDWIDE, BEEN TRANSLATED INTO MORE THAN H9 LANGUAGES, AND ADAPTED INTO A SUCCESSFUL FILM SERIES. THE SERIES IS KNOWN NOT ONLY FOR ITS ENCHANTING WORLDCBUILDING BUT ALSO FOR ADDRESSING DARKER, COMPLEO THEMES SUCH AS MORTALITY, PRE#UDICE, AND THE ABUSE OF POWER. THE HARRY POTTER SERIES HAS LEFT AN INDELIBLE MARK ON POPULAR CULTURE, FOSTERING A GLOBAL FAN BASE, INSPIRING COUNTLESS SPINCOFFS, AND CEMENTING ITS PLACE AS A LITERARY PHENOMENON.

* Ta thấy HIS ‘’TH BIRTHDAY: thì nó sẽ là 1 số thự tự mà 2 số giống nhau và kết thúc là TH thì chỉ có ELEVENTH -> 11TH. ‘ →1.
* PRE#UDICE là PREJUDICE. #->J.
* CON9UERING là CONQUERING. 9->Q.
* **Đoạn văn sau khi ánh xạ:**

****

1. Bảng ánh xạ của 3.2

THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR J.K. ROWLING, IS ONE OF THE MOST POPULAR AND INFLUENTIAL FANTASY SAGAS OF MODERN LITERATURE. SPANNING SEVEN BOOKS, THE SERIES FOLLOWS THE LIFE OF A YOUNG BOY, HARRY POTTER, WHO DISCOVERS ON HIS 11TH BIRTHDAY THAT HE IS A WIZARD. HE IS INVITED TO ATTEND HOGWARTS SCHOOL OF WITCHCRAFT AND WIZARDRY, WHERE HE LEARNS ABOUT HIS MAGICAL HERITAGE, DEVELOPS CLOSE FRIENDSHIPS, AND CONFRONTS THE DARK FORCES THAT THREATEN THE WIZARDING WORLD.

THE CENTRAL PLOT REVOLVES AROUND HARRY'S ONGOING BATTLE WITH LORD VOLDEMORT, A DARK WIZARD INTENT ON CONQUERING BOTH THE MAGICAL AND NONCMAGICAL WORLDS. AS HARRY GROWS OLDER, HE LEARNS MORE ABOUT HIS OWN MYSTERIOUS PAST, HIS CONNECTION TO VOLDEMORT, AND THE PROPHECY THAT TIES THEIR FATES TOGETHER. THROUGHOUT THE SERIES, THEMES OF FRIENDSHIP, LOYALTY, BRAVERY, AND THE POWER OF LOVE ARE EOPLORED, WITH A RICH WORLD FILLED WITH MAGICAL CREATURES, SPELLS, AND DEEP MYTHOLOGY.

THE BOOKS, STARTING WITH HARRY POTTER AND THE PHILOSOPHER'S STONE S1RRTG AND CONCLUDING WITH IHARRY POTTER AND THE DEATHLY HALLOWS SYQQTG, HAVE SOLD OVER VQQ MILLION COPIES WORLDWIDE, BEEN TRANSLATED INTO MORE THAN HQ LANGUAGES, AND ADAPTED INTO A SUCCESSFUL FILM SERIES. THE SERIES IS KNOWN NOT ONLY FOR ITS ENCHANTING WORLDCBUILDING BUT ALSO FOR ADDRESSING DARKER, COMPLEO THEMES SUCH AS MORTALITY, PREJUDICE, AND THE ABUSE OF POWER. THE HARRY POTTER SERIES HAS LEFT AN INDELIBLE MARK ON POPULAR CULTURE, FOSTERING A GLOBAL FAN BASE, INSPIRING COUNTLESS SPINCOFFS, AND CEMENTING ITS PLACE AS A LITERARY PHENOMENON.

* + Hiệu chỉnh (thay đổi ký tự chọn lọc) các lỗi chính tả và từ ngữ.
  + **Đoạn văn sau khi hiệu chỉnh:**

THE HARRY POTTER SERIES, WRITTEN BY BRITISH AUTHOR J.K. ROWLING, IS ONE OF THE MOST POPULAR AND INFLUENTIAL FANTASY SAGAS OF MODERN LITERATURE. SPANNING SEVEN BOOKS, THE SERIES FOLLOWS THE LIFE OF A YOUNG BOY, HARRY POTTER, WHO DISCOVERS ON HIS 11TH BIRTHDAY THAT HE IS A WIZARD. HE IS INVITED TO ATTEND HOGWARTS SCHOOL OF WITCHCRAFT AND WIZARDRY, WHERE HE LEARNS ABOUT HIS MAGICAL HERITAGE, DEVELOPS CLOSE FRIENDSHIPS, AND CONFRONTS THE DARK FORCES THAT THREATEN THE WIZARDING WORLD.

THE CENTRAL PLOT REVOLVES AROUND HARRY'S ONGOING BATTLE WITH LORD VOLDEMORT, A DARK WIZARD INTENT ON CONQUERING BOTH THE MAGICAL AND NON-MAGICAL WORLDS. AS HARRY GROWS OLDER, HE LEARNS MORE ABOUT HIS OWN MYSTERIOUS PAST, HIS CONNECTION TO VOLDEMORT, AND THE PROPHECY THAT TIES THEIR FATES TOGETHER. THROUGHOUT THE SERIES, THEMES OF FRIENDSHIP, LOYALTY, BRAVERY, AND THE POWER OF LOVE ARE EXPLORED, WITH A RICH WORLD FILLED WITH MAGICAL CREATURES, SPELLS, AND DEEP MYTHOLOGY.

THE BOOKS, STARTING WITH HARRY POTTER AND THE PHILOSOPHER'S STONE (1997) AND CONCLUDING WITH HARRY POTTER AND THE DEATHLY HALLOWS (2007), HAVE SOLD OVER 500 MILLION COPIES WORLDWIDE, BEEN TRANSLATED INTO MORE THAN 80 LANGUAGES, AND ADAPTED INTO A SUCCESSFUL FILM SERIES. THE SERIES IS KNOWN NOT ONLY FOR ITS ENCHANTING WORLD-BUILDING BUT ALSO FOR ADDRESSING DARKER, COMPLEX THEMES SUCH AS MORTALITY, PREJUDICE, AND THE ABUSE OF POWER. THE HARRY POTTER SERIES HAS LEFT AN INDELIBLE MARK ON POPULAR CULTURE, FOSTERING A GLOBAL FAN BASE, INSPIRING COUNTLESS SPIN-OFFS, AND CEMENTING ITS PLACE AS A LITERARY PHENOMENON.

## Playfair cipher

A screenshot of a computer

AI-generated content may be incorrect.

- Ma trận được xây dựng từ key HARRYPOTTER là:

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

1. Giải mã bằng cách

* Chia bản mã thành từng cặp chữ cái.
* Với mỗi cặp chữ cái:
* Nếu hai chữ cùng hàng: thay thế từng chữ bằng chữ đứng ngay bên trái nó trong cùng hàng. Nếu chữ đó là chữ đầu tiên của hàng thì thay bằng chữ cuối cùng của hàng.
* Nếu hai chữ cùng cột: thay thế từng chữ bằng chữ nằm ngay phía trên nó trong cùng cột. Nếu chữ đó đang ở ô đầu tiên của cột thì thay bằng chữ cuối cùng của cột.
* Nếu hai chữ nằm ở hai hàng và hai cột khác nhau: tạo thành một hình chữ nhật. Khi đó, thay mỗi chữ bằng chữ nằm cùng hàng với nó nhưng ở cột của chữ kia.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| AR | YW | YP | HC | BV | EB | YG | MP | NC | YG |
| HA | RX | RY | PO | TX | TE | RI | SA | SE | RI |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CN | TD | NC | WT | MG | RM | FT | QP | LE | WT |
| ES | OF | SE | VE | NF | AN | TA | SY | NO | VE |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ML | RE | FB | EB | QE | BQ | EB | IY | GB | … |
| IS | WR | IT | TE | NB | YB | RI | TI | SH | … |

* Văn bản sau khi giải mã:

HARRY POTTER IS A SERIES OF SEVEN FANTASY NOVELS WRITTEN BY BRITISH AUTHOR JK ROWLING. THE NOVELS CHRONICLE THE LIVES OF A YOUNG WIZARD HARRY POTTER AND HIS FRIENDS HERMIONE GRANGER AND RON WEASLEY, ALL OF WHOM ARE STUDENTS AT HOGWARTS SCHOOL OF WITCHCRAFT AND WIZARDRY. THE MAIN STORY ARC CONCERNS HARRY’S CONFLICT WITH LORD VOLDEMORT, A DARK WIZARD WHO INTENDS TO BECOME IMMORTAL, OVERTHROW THE WIZARD GOVERNING BODY KNOWN AS THE MINISTRY OF MAGIC, AND SUBJUGATE ALL WIZARDS AND MUGGLES.

A close-up of a blue background

AI-generated content may be incorrect.

* Mã nguồn của chương trình:

ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

def sanitize(*s*):

*s* = *s*.upper()

*s* = "".join(ch for ch in *s* if 'A' <= ch <= 'Z')

return *s*.replace('J', 'I')

def print\_grid(*grid*):

print("\nMa trận:")

for row in *grid*:

print("| " + " ".join(row) + " |")

print("----------------------------\n")

def build\_square(*key*, *print\_key\_square*=True):

*key* = sanitize(*key*)

seen = set()

order = []

for ch in *key*:

if ch not in seen:

seen.add(ch)

order.append(ch)

for ch in ALPHABET:

if ch == 'J':

continue

if ch not in seen:

seen.add(ch)

order.append(ch)

grid = [order[i\*5:(i+1)\*5] for i in range(5)]

if *print\_key\_square*:

print\_grid(grid)

pos = {grid[r][c]: (r, c) for r in range(5) for c in range(5)}

pos['J'] = pos['I']

return grid, pos

def digraphs(*text*, *filler*='X'):

t = sanitize(*text*)

pairs = []

i = 0

while i < len(t):

a = t[i]

if i + 1 < len(t):

b = t[i+1]

if a == b:

pairs.append((a, *filler*))

i += 1

else:

pairs.append((a, b))

i += 2

else:

pairs.append((a, *filler*))

i += 1

return pairs

def enc\_pair(*a*, *b*, *pos*, *grid*):

r1, c1 = *pos*[*a*]

r2, c2 = *pos*[*b*]

if r1 == r2:

return *grid*[r1][(c1+1)%5], *grid*[r2][(c2+1)%5]

if c1 == c2:

return *grid*[(r1+1)%5][c1], *grid*[(r2+1)%5][c2]

return *grid*[r1][c2], *grid*[r2][c1]

def dec\_pair(*a*, *b*, *pos*, *grid*):

r1, c1 = *pos*[*a*]

r2, c2 = *pos*[*b*]

if r1 == r2:

return *grid*[r1][(c1-1)%5], *grid*[r2][(c2-1)%5]

if c1 == c2:

return *grid*[(r1-1)%5][c1], *grid*[(r2-1)%5][c2]

return *grid*[r1][c2], *grid*[r2][c1]

def playfair\_encrypt(*key*, *text*):

grid, pos = build\_square(*key*)

out = []

for a, b in digraphs(*text*):

x, y = enc\_pair(a, b, pos, grid)

out.append(x + y)

return "".join(out)

def playfair\_decrypt(*key*, *text*):

grid, pos = build\_square(*key*)

t = sanitize(*text*)

if len(t) % 2 != 0:

raise ValueError("Văn bản mã hóa phải có số lượng ký tự chẵn.")

out = []

for i in range(0, len(t), 2):

a, b = t[i], t[i+1]

x, y = dec\_pair(a, b, pos, grid)

out.append(x + y)

return "".join(out)

if \_\_name\_\_ == "\_\_main\_\_":

print("Playfair Cipher Tool")

option\_input = input("1 - Encrypt\n2 - Decrypt\nChọn: ").strip()

try:

option = int(option\_input)

except ValueError:

print("Lựa chọn không hợp lệ. Thoát.")

exit()

key = input("Key: ").strip()

text = input("Text: ").strip()

if option == 1:

print("\nKết quả Mã hóa:")

ciphertext = playfair\_encrypt(key, text)

print("Văn bản mã hóa:", ciphertext)

elif option == 2:

print("\nKết quả Giải mã:")

try:

plaintext = playfair\_decrypt(key, text)

print("Văn bản giải mã:", plaintext)

except ValueError as e:

print("Lỗi:", e)

else:

print("Lựa chọn không hợp lệ. Vui lòng chọn 1 hoặc 2.")

* **Quá trình mã hóa:**

#### Bước 1: Nhập dữ liệu

* Người dùng nhập key và text.
* Hai giá trị này được truyền vào hàm playfair\_encrypt(key, text).

#### Bước 2: Tạo ma trận Playfair (5x5)

* Chương trình loại bỏ ký tự trùng trong khóa.
* Ghép phần còn thiếu của bảng chữ cái vào sau khóa để tạo ma trận 5x5.
* Ký tự I và J được gộp chung, vì Playfair chỉ có 25 ô.  
   → Ma trận này được dùng để xác định vị trí các ký tự khi mã hóa.
* Bước 3: Xử lý văn bản gốc
* Chuyển tất cả chữ cái về chữ hoa hoặc chữ thường thống nhất.
* Loại bỏ ký tự không phải chữ cái.
* Ghép các ký tự thành từng cặp.
* Nếu hai chữ cái trong một cặp trùng nhau, chèn thêm ký tự X vào giữa.
* Nếu số ký tự lẻ, thêm X vào cuối chuỗi.

#### Bước 4: Áp dụng quy tắc Playfair để mã hóa từng cặp. Với mỗi cặp ký tự:

* Cùng hàng: thay mỗi ký tự bằng ký tự bên phải nó trong cùng hàng.
* Cùng cột: thay mỗi ký tự bằng ký tự phía dưới nó trong cùng cột.
* Khác hàng, khác cột: mỗi ký tự được thay bằng ký tự nằm cùng hàng nhưng ở cột của ký tự còn lại (tạo thành hình chữ nhật).
* **Quá trình giải mã:**

#### Bước 1: Nhập dữ liệu

* Người dùng nhập key và ciphertext.
* Hai giá trị được truyền vào hàm playfair\_decrypt(key, text).

#### Bước 2: Tạo lại ma trận 5x5

* Dựa trên khóa nhập vào, chương trình tạo lại ma trận Playfair giống như khi mã hóa.  
   → Điều này đảm bảo quá trình giải mã dùng đúng ma trận ban đầu.

#### Bước 3: Chia văn bản mã hóa thành cặp ký tự

* Văn bản mã hóa được tách thành các cặp hai ký tự như lúc mã hóa.

#### Bước 4: Áp dụng quy tắc giải mã Playfair. Với mỗi cặp (x, y):

* Cùng hàng: thay mỗi ký tự bằng ký tự bên trái nó trong cùng hàng (vòng lại cuối nếu ở đầu hàng).
* Cùng cột: thay mỗi ký tự bằng ký tự phía trên nó trong cùng cột (vòng lại cuối nếu ở đầu cột).
* Khác hàng, khác cột: mỗi ký tự được thay bằng ký tự nằm cùng hàng nhưng ở cột của ký tự còn lại (ngược với mã hóa).

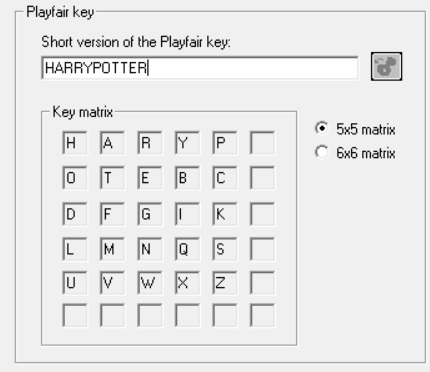
#### Bước 5: Kết hợp kết quả

* Ghép các cặp ký tự đã giải mã lại thành một chuỗi hoàn chỉnh.
* Nếu có ký tự đệm (X) được thêm trong quá trình mã hóa, người dùng có thể loại bỏ thủ công để khôi phục văn bản gốc chính xác.
* So sánh kết quả chạy chương trình với Cryptool:
* Kết quả chạy chương trình:

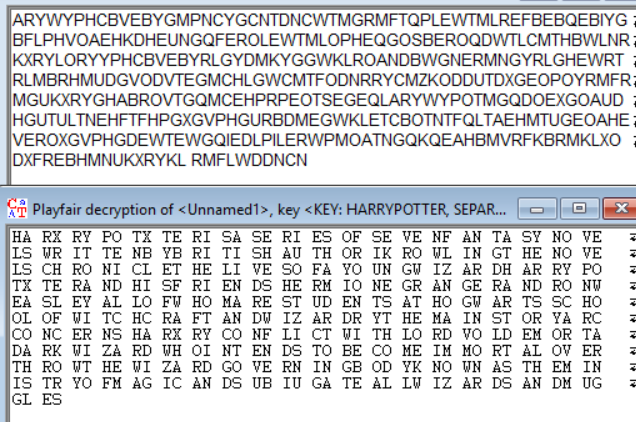


1. Sau khi chạy chương trình

* Crytool:



1. Ma trận key trong Cryptool



1. Văn bản đã mã hóa và văn bản đã giải mã

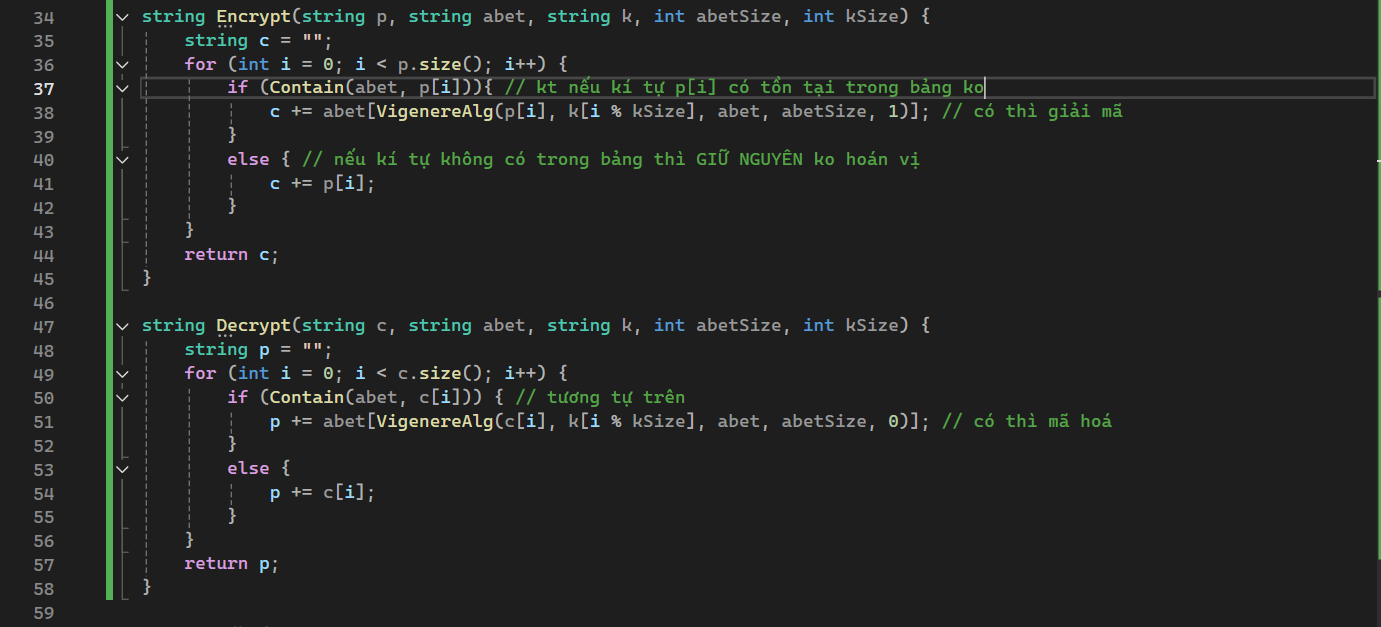
* Đối chiếu thấy kết quả lúc chạy chương trình và trên Cryptool là trùng nhau.

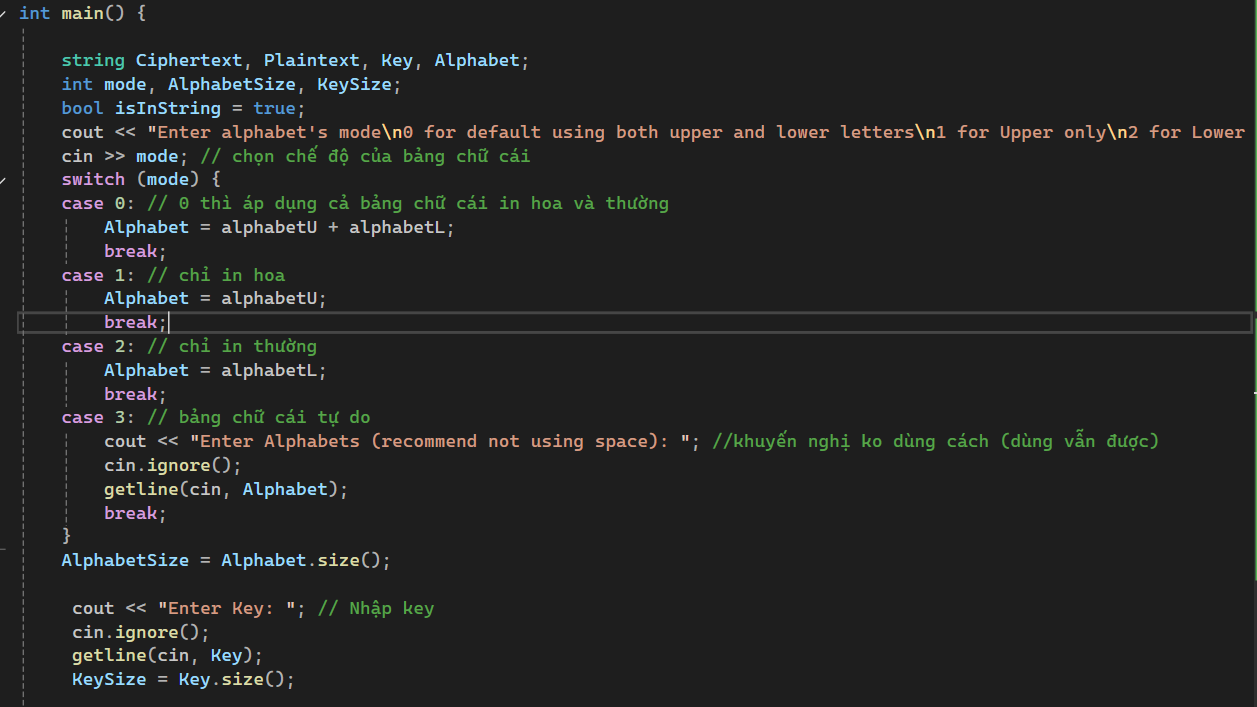
## Polyalphabetic ciphers – Vigenère

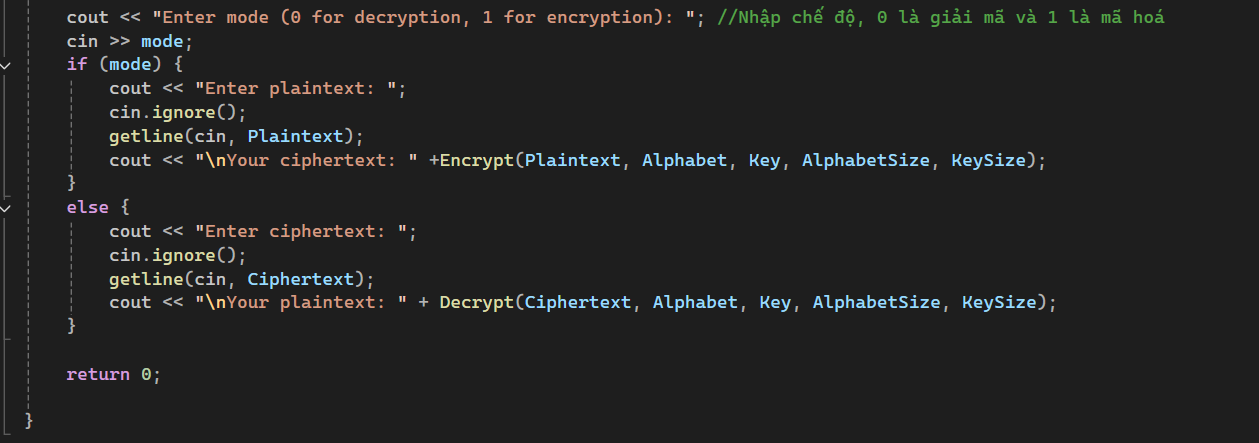
A close-up of a message

AI-generated content may be incorrect.









1. Mã nguồn Vigenère (C++)

* Quy trình giải mã và mã hoá trong code:

+ Bước 1: Yêu cầu người dùng chọn 1 trong 4 chế độ của bảng chữ cái:

-Nhập 0: Bảng chữ cái kết hợp giữa thường và in hoa. Hoa trước thường sau (có sẵn)

-Nhập 1: Bảng chữ cái in hoa. (có sẵn)

-Nhập 2: Bảng chữ cái thường. (có sẵn)

-Nhập 3: Bảng chữ cái tự chọn. (không có săn  
=> Lưu ý: Nếu nhập 3, người dùng sẽ phải tự nhập bảng chữ cái.

+ Bước 2: Yêu cầu người dùng nhập khoá (key)

+ Bước 3: Yêu cầu người dùng chọn 1 trong 2 chế độ:

-Nhập 0: Chế độ giải mã.

-Nhập 1: Chế độ mã hoá.

+ Bước 4: Yêu cầu người dùng nhập văn bản được mã hoá (nếu chọn chế độ giải mã) hoặc văn bản cần mã hoá (nếu chọn chế độ mã hoá)

+ Bước 5: Thuật toán xét từng ký tự trong văn bản và phân ra 2 trường hợp:  
 -Trường hợp 1: Kí tự có trong bảng chữ cái, thuật toán giải tương ứng:

* Với giải mã: p[i] = (c[i]-k[i mod m]+ h ) mod h
* Với mã hoá: c[i] = (p[i] + k[i mod m]) mod h
* Trong đó, h là số lượng ký tự trong bảng chữ cái, m là kích thước khoá

- Trường hợp 2: Kí tự không có trong bảng chữ cái, thuật toán giữ nguyên không biến đổi kí tự.

+ Bước 6: In ra kết quả.

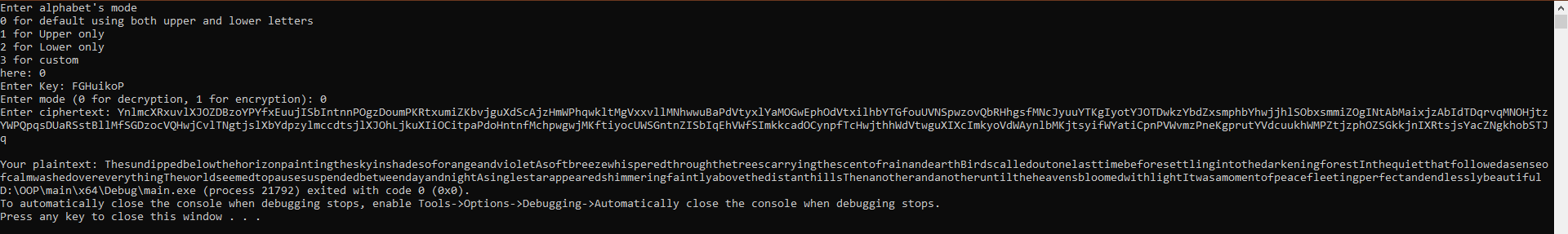
**Ví dụ:**

* Plaintext:

The sun dipped below the horizon, painting the sky in shades of orange and violet. A soft breeze whispered through the trees, carrying the scent of rain and earth. Birds called out one last time before settling into the darkening forest. In the quiet that followed, a sense of calm washed over everything. The world seemed to pause, suspended between day and night. A single star appeared, shimmering faintly above the distant hills. Then another, and another, until the heavens bloomed with light. It was a moment of peace — fleeting, perfect, and endlessly beautiful.

* Key: FGHuikoP
* Ciphertext(Cryptool online):

YnlmcXRxuvlXJOZDBzoYPYfxEuujISbIntnnPOgzDoumPKRtxumiZKbvjguXdScAjzHmWPhqwkltMgVxxvllMNhwwuBaPdVtyxlYaMOGwEphOdVtxilhbYTGfouUVNSpwzovQbRHhgsfMNcJyuuYTKgIyotYJOTDwkzYbdZxsmphbYhwjjhlSObxsmmiZOgINtAbMaixjzAbIdTDqrvqMNOHjtzYWPQpqsDUaRSstBllMfSGDzocVQHwjCvlTNgtjslXbYdpzylmccdtsjlXJOhLjkuXIiOCitpaPdoHntnfMchpwgwjMKftiyocUWSGntnZISbIqEhVWfSImkkcadOCynpfTcHwjthhWdVtwguXIXcImkyoVdWAynlbMKjtsyifWYatiCpnPVWvmzPneKgprutYVdcuukhWMPZtjzphOZSGkkjnIXRtsjsYacZNgkhobSTJq

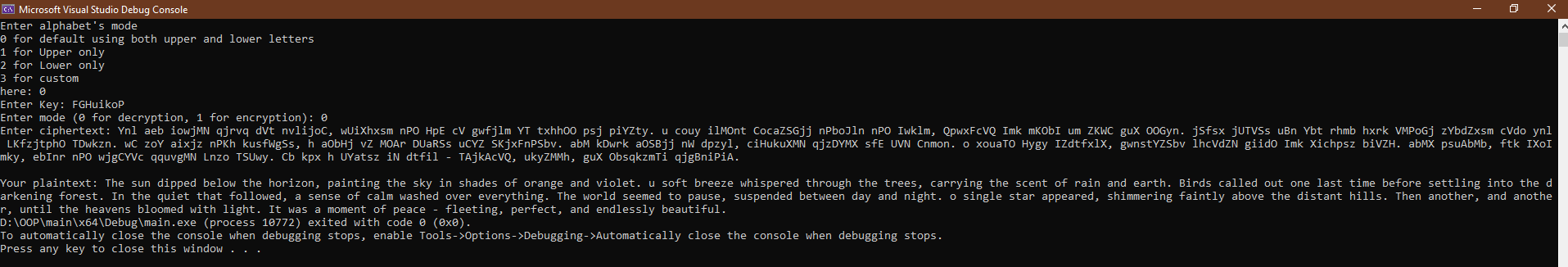


*Giải mã ciphertext của cryptool online bằng code trên*

**⇒Kết quả thu được là văn bản gốc đã lược bỏ ký tự đặc biệt (‘ ‘, ‘-’, …).**

Ciphertext(My algorithm)

Ynl aeb iowjMN qjrvq dVt nvlijoC, wUiXhxsm nPO HpE cV gwfjlm YT txhhOO psj piYZty. u couy ilMOnt CocaZSGjj nPboJln nPO Iwklm, QpwxFcVQ Imk mKObI um ZKWC guX OOGyn. jSfsx jUTVSs uBn Ybt rhmb hxrk VMPoGj zYbdZxsm cVdo ynl LKfzjtphO TDwkzn. wC zoY aixjz nPKh kusfWgSs, h aObHj vZ MOAr DUaRSs uCYZ SKjxFnPSbv. abM kDwrk aOSBjj nW dpzyl, ciHukuXMN qjzDYMX sfE UVN Cnmon. o xouaTO Hygy IZdtfxlX, gwnstYZSbv lhcVdZN giidO Imk Xichpsz biVZH. abMX psuAbMb, ftk IXoImky, ebInr nPO wjgCYVc qquvgMN Lnzo TSUwy. Cb kpx h UYatsz iN dtfil - TAjkAcVQ, ukyZMMh, guX ObsqkzmTi qjgBniPiA.

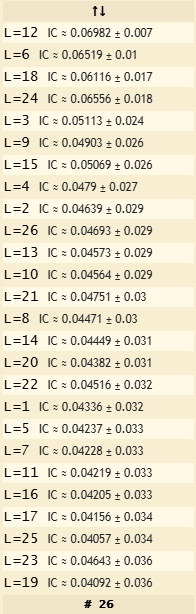
*Giải mã ciphertext vừa thu được bằng code trên*

**⇒ Kết quả thu được là văn bản gốc**

A close-up of a text

AI-generated content may be incorrect.

* Bước 1: Ta giả sử bảng chữ cái của quá trình mã hoá và giải mã là bảng chữ cái tiếng anh (26 ký tự, in thường). Đồng thời ta phân tích dựa vào IoC (Chỉ số trùng hợp), thu được bảng sau:



1. Chỉ số trùng hợp dựa theo L.

Trong đó: L là độ dài của khoá K, Ic là chỉ số trùng hợp.

Biết rằng Ic của 1 văn bản tiếng anh xấp xỉ 0.0667. Vậy nên ta thử chọn L = 6 do kết quả Ic gần nhất với với 0.0667.

* Bước 2: Tạm thời bỏ các bỏ ký tự đặc biệt trong ciphertext (‘‘, ‘**,**’ , ‘**.**’). Ciphertext sẽ được chia thành 6 chuỗi riêng biệt (L = 6). Mỗi chuỗi i(0 - 5) là tập hợp các ký tự ở vị trí j (từ i cách nhau L số). Ví dụ với i = 0 và L = 6: chuỗi c0 = c[0]+c[6]+c[12]+c[18] +...

⇒ 6 chuỗi thu được là:

c0 = Pbpyylvlthtajlcttswhyzjvsvzutlfhkpoapsobyvplpksulhvjwfvvuauathzjjhpk

c1= pvgachukcpwkjugocevuwgwpgtvuguutvrgguioueiepqkuitvrvtyypvchkovwtcpqg

c2 = oqzbbqqzfpzazppmfaeqxpxepuareufqatedfaeqddwqzsumuudpuqefqzumguoqdezy

c3 = ilwnblwzcwchcyznchunywuwunnimhbbxyygcluxsuylucahziiupvcblxxfhibxxumu

c4 = uamwgacwwwkbyzzpkkvwjibitpzzieiimzlqkqznxxgivbvlqvbbijvmvkmkqviqbkiq

c5 = ivvzkmkkgftxnbhxtxwytebezftfztmkvmxgtmxhmazmwtbovmxtvkzbxhghvllmkmg

* Bước 3: Tiến hành phân tích vét cạn Caesar từng chuỗi:



1. Vét cạn Caesar của c0



1. Vét cạn Caesar của c1



1. Vét cạn Caesar của c2



1. Vét cạn Caesar của c3



1. Vét cạn Caesar của c4



1. Vét cạn Caesar của c5

⇒ Nếu dựa theo kết quả tần suất cao nhất của từng chuỗi, ta sẽ thu được khoá số: KeyInt = {7, 2, 12, 20, 8, 9} ⇒ Key = HCMUIT (Khoá có nghĩa nên có vẻ đúng!).

Bước 5: Tiến hành thêm lại các ký tự đặc biệt và dùng khoá để giải mã. Ta thu được plaintext sau:

in computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. these deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

## Advanced Task

A blue background with black text

AI-generated content may be incorrect.

Sử dụng mã HILL:

* Cách hoạt động:

**+ Bước mã hóa:**

* Xử lý đầu vào: Tách riêng các ký tự chữ và ghi nhớ vị trí của các ký tự đặc biệt (dấu cách, số, chấm câu,...).
* Đệm: Nếu số lượng ký tự chữ là số lẻ, thêm một ký tự đệm vào cuối để tạo thành cặp.
* Nhân ma trận: Lấy từng cặp số (tương ứng với 2 ký tự) và nhân chúng với ma trận khóa K để tạo ra cặp số mới (cặp ký tự đã mã hóa).
* Tái tạo chuỗi: Chuyển các cặp số mới thành chuỗi ký tự mã hóa và chèn lại các ký tự đặc biệt vào đúng vị trí ban đầu.

**+ Bước giải mã:**

* Xử lý đầu vào: Tương tự như mã hóa, tách riêng các ký tự chữ và ghi nhớ vị trí các ký tự đặc biệt.
* Tìm khóa giải mã: Tính ma trận nghịch đảo K−1 từ ma trận khóa K đã cho.
* Nhân ma trận: Lấy từng cặp số của bản mã và nhân chúng với ma trận nghịch đảo K−1 để khôi phục lại cặp số ban đầu.
* Tái tạo chuỗi: Chuyển các cặp số đã được khôi phục thành chuỗi văn bản gốc và chèn lại các ký tự đặc biệt.
* Các hàm khác:

### + Các Hàm Hỗ trợ

* Chuyển đổi văn bản ↔ số: Hàm text\_to\_number và number\_to\_text để chuyển đổi qua lại giữa chuỗi ký tự và danh sách các con số tương ứng.
* Tính toán ma trận khóa nghịch đảo:
  + mod\_inverse: Tìm nghịch đảo modular của một số. get\_key\_matrix\_inverse: Dùng mod\_inverse để tính toán ma trận nghịch đảo của ma trận khóa K.

ALPHABET = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz"

MODULO = len(ALPHABET)

INDEX = {ch: i for i, ch in enumerate(ALPHABET)}

def text\_to\_number(text):

nums = []

for ch in text:

if ch in INDEX:

nums.append(INDEX[ch])

return nums

def number\_to\_text(nums):

return "".join(ALPHABET[n] for n in nums)

def mod\_inverse(a, m):

a %= m

for x in range(1, m):

if (a \* x) % m == 1:

return x

return None

def get\_key\_matrix\_inverse(key):

det = (key[0][0] \* key[1][1] - key[0][1] \* key[1][0]) % MODULO

inv = mod\_inverse(det, MODULO)

if inv is None:

raise ValueError("Ma trận khóa không có nghịch đảo (det không nguyên tố cùng MODULO).")

adj = [

[key[1][1], -key[0][1]],

[-key[1][0], key[0][0]]

]

return [[(adj[i][j] \* inv) % MODULO for j in range(2)] for i in range(2)]

def hill\_encrypt(plaintext, key):

# ghi lại vị trí ký tự KHÔNG thuộc A-Z/a-z

structure = [(i, ch) for i, ch in enumerate(plaintext) if ch not in INDEX]

letters = "".join(ch for ch in plaintext if ch in INDEX)

if len(letters) % 2 == 1:

letters += "X"

P = text\_to\_number(letters)

C = []

for i in range(0, len(P), 2):

p1, p2 = P[i], P[i + 1]

c1 = (key[0][0] \* p1 + key[0][1] \* p2) % MODULO

c2 = (key[1][0] \* p1 + key[1][1] \* p2) % MODULO

C.extend([c1, c2])

result = list(number\_to\_text(C))

for pos, ch in structure:

if pos <= len(result):

result.insert(pos, ch)

else:

result.append(ch)

return "".join(result)

def hill\_decrypt(ciphertext, key):

structure = [(i, ch) for i, ch in enumerate(ciphertext) if ch not in INDEX]

letters = "".join(ch for ch in ciphertext if ch in INDEX)

if len(letters) % 2 == 1:

raise ValueError("Bản mã có số ký tự chữ lẻ.")

inv\_key = get\_key\_matrix\_inverse(key)

C = text\_to\_number(letters)

P = []

for i in range(0, len(C), 2):

c1, c2 = C[i], C[i + 1]

p1 = (inv\_key[0][0] \* c1 + inv\_key[0][1] \* c2) % MODULO

p2 = (inv\_key[1][0] \* c1 + inv\_key[1][1] \* c2) % MODULO

P.extend([p1, p2])

result = list(number\_to\_text(P))

for pos, ch in structure:

if pos <= len(result):

result.insert(pos, ch)

else:

result.append(ch)

return "".join(result)

if \_\_name\_\_ == "\_\_main\_\_":

try:

key\_nums = list(map(int, input("Nhập khóa (4 số cách nhau bởi dấu cách): ").split()))

if len(key\_nums) != 4:

raise ValueError("Khóa lỗi.")

key = [[key\_nums[0], key\_nums[1]], [key\_nums[2], key\_nums[3]]]

print (key)

get\_key\_matrix\_inverse(key)

choice = input("e - Encrypt \n d - Decrypt"\n).lower()

if choice == 'e':

plaintext = input("Nhập văn bản mã hóa: ")

print(f"-> Cipher Text: {hill\_encrypt(plaintext, key)}")

elif choice == 'd':

ciphertext = input("Nhập văn bản giải mã: ")

print(f"-> Plain Text: {hill\_decrypt(ciphertext, key)}")

else:

print("Lựa chọn không hợp lệ.")

except ValueError as e:

print(f"Lỗi: {e}")

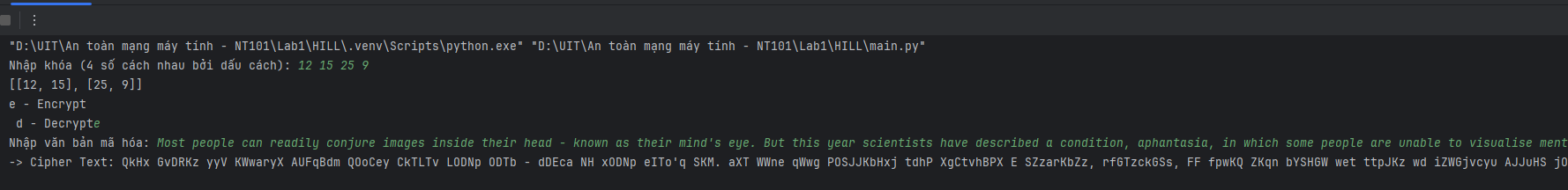
except Exception as e:

print(f"Lỗi: {e}")

* Plaintext:

Most people can readily conjure images inside their head - known as their mind's eye. But this year scientists have described a condition, aphantasia, in which some people are unable to visualise mental images. Niel Kenmuir, from Lancaster, has always had a blind mind's eye. He knew he was different even in childhood. "My stepfather, when I couldn't sleep, told me to count sheep, and he explained what he meant, I tried to do it and I couldn't," he says. "I couldn't see any sheep jumping over fences, there was nothing to count." Our memories are often tied up in images, think back to a wedding or first day at school. As a result, Niel admits, some aspects of his memory are "terrible", but he is very good at remembering facts. And, like others with aphantasia, he struggles to recognise faces. Yet he does not see aphantasia as a disability, but simply a different way of experiencing life.

* Thực hiện chương trình:

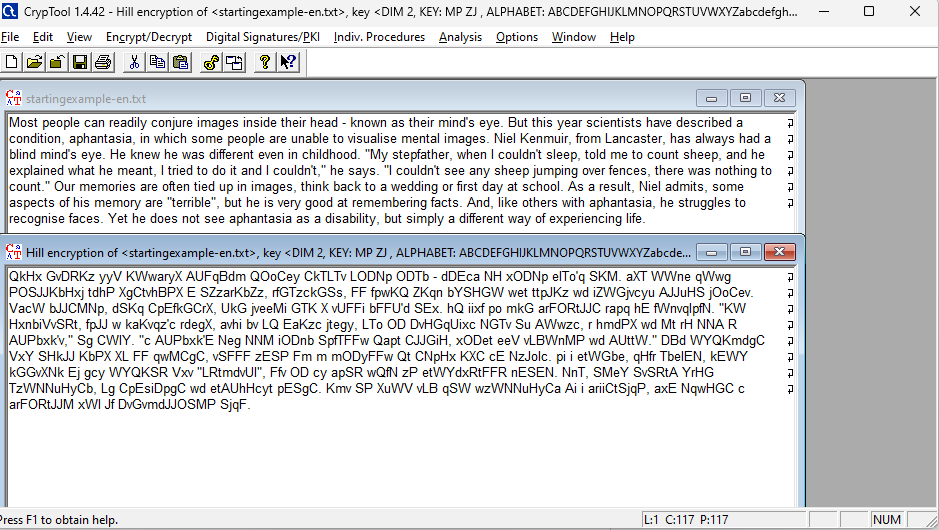


1. Kết quả khi thực hiện chương trình

* Ciphertext:

QkHx GvDRKz yyV KWwaryX AUFqBdm QOoCey CkTLTv LODNp ODTb - dDEca NH xODNp eITo'q SKM. aXT WWne qWwg POSJJKbHxj tdhP XgCtvhBPX E SZzarKbZz, rfGTzckGSs, FF fpwKQ ZKqn bYSHGW wet ttpJKz wd iZWGjvcyu AJJuHS jOoCev. VacW bJJCMNp, dSKq CpEfkGCrX, UkG jveeMi GTK X vUFFi bFFU'd SEx. hQ iixf po mkG arFORtJJC rapq hE fWnvqIpfN. "KW HxnbiVvSRt, fpJJ w kaKvqz'c rdegX, avhi bv LQ EaKzc jtegy, LTo OD DvHGqUixc NGTv Su AWwzc, r hmdPX wd Mt rH NNA R AUPbxk'v," Sg CWIY. "c AUPbxk'E Neg NNM iODnb SpfTFFw Qapt CJJGiH, xODet eeV vLBWnMP wd AUttW." DBd WYQKmdgC VxY SHkJJ KbPX XL FF qwMCgC, vSFFF zESP Fm m mODyFFw Qt CNpHx KXC cE NzJoIc. pi i etWGbe, qHfr TbeIEN, kEWY kGGvXNk Ej gcy WYQKSR Vxv "LRtmdvUl", Ffv OD cy apSR wQfN zP etWYdxRtFFR nESEN. NnT, SMeY SvSRtA YrHG TzWNNuHyCb, Lg CpEsiDpgC wd etAUhHcyt pESgC. Kmv SP XuWV vLB qSW wzWNNuHyCa Ai i ariiCtSjqP, axE NqwHGC c arFORtJJM xWI Jf DvGvmdJJOSMP SjqF.

* Kiểm thử trên Cryptool cho kết quả giống nhau:



1. Kiểm chứng bằng Cryptool

* Kiểm thử với giải mã: k= [[37, 22], [3, 51]]
* CipherText:

mOmgVxmg kL zyC IkjZJ gPUtSyOySq tpzrmn el zyC ikjzy'O vqGxrnb, xBpUkLE wGipb el S ycvBFkL Jhtp vzwGmg vzyu Tf oxqbVxPh U fuGUtkjKYB kuUD: mJRA TuGAn xr PvZJ yWPv Anl xiZO yp UJR FfzWsz el riAnhn Gi G iwWXxO yV AbllBkL zBh gJRiSABHHQ CBk zymEb lJKinzrPh, Gi An IplBFmchEDU ts iTVKKhn. Kl Mo dvkLq, zJRe UoEYVszBFzWg BfzTVFfhggJ FfzWsz yd zymEB ymnuUS jU czycv riAnhn el zyy ueoy utpQyyu, VmkLIKPh wzwWT qGflZnnVxyd. ZYy uBFYO IOS jxBw kUt zBf z oioEyukuyd el Mrcv-evEYcv aQZlIp oxslBFVxydM oZ OCIQ CBk lEoUcvkLG DRhpUk. UF YkjVxUmRhl, uNTsKLh vzoSp Ui ZiqkjD ICIW xiZ zymED fDRMFVxPh blBd kL zymEp ikxblFpynGKJ mw FblrDBBPh zruzcv MowrgCM oV AGfBdn nBk AnaXJRL hwWXxO yd CopzrVxyd, Xjynkj.

-> Plain Text: Sometime in the early Cretaceous period of the Earth's history, hunting wasps of a certain type became bees by adopting a vegetarian diet: they began to rely more and more on the pollen of plants as a source of protein for themselves and their offspring, as an alternative to insects. In so doing, they accidentally transported pollen on their bodies to other plants of the same species, bringing about pollination. The stage was thus set for a succession of ever-closer mutual adaptations of bees and flowering plants. In particular, flowers began to reward bees for their unwitting role in their reproduction by providing richer sources of pollen and another source of nutrition, nectar.

**HẾT**