Week1,2_Tasks_Cryptanalysis

Trần Hữu Đức
23520321

Task 1: Cryptanalysis Affine cipher (brute force a,b). Python code:

```
import string

def mod_inverse(a, m):
    a = a % m
    for x in range(1, m):
        if (a * x) % m == 1:
            return x
    return None


def affine_decrypt(text, a, b):
    a_inv = mod_inverse(a, 26)
    if a_inv is None:
        return None

    alphabets = string.ascii_uppercase
    result = []
    for char in text:
        if char.isupper():
            y = ord(char) - ord('A')
            x = (a_inv * (y - b)) % 26
            result.append(alphabets[x])
        elif char.islower():
            y = ord(char.upper()) - ord('A')
            x = (a_inv * (y - b)) % 26
            result.append(alphabets[x].lower())
        else:
            result.append(char)
    return ''.join(result)

def brute_force_affine_cipher(ciphertext):
    for a in range(1, 26):
        if mod_inverse(a, 26) is not None:
            for b in range(0, 26):
                decrypted_text = affine_decrypt(ciphertext, a, b)
                if decrypted_text:
                    print(f"Trying a = {a}, b = {b}")
                    print(f"Decrypted text: {decrypted_text}\n")
                input("\nPress Enter to continue to decryption...")

def main():
    ciphertext = input("Enter the encrypted text: ")
    brute_force_affine_cipher(ciphertext)

if __name__ == "__main__":
    main()
```

Task 2: Cryptanalysis SimpleSubstitutionCipher

- generate the random key:

```
Simple Substitution Cipher
Enter a 26-letter key for the substitution cipher (or press Enter to
generate a random key):

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

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

- Encryp the pliantext (abount 100 to 200 words)

```
Enter the text to encrypt: The Harry Potter stories feature imagery and
motifs drawn from Arthurian myth and fairytales. Harry's ability to draw the
Sword of Gryffindor from the Sorting Hat resembles the Arthurian sword in
the stone legend.[22] His life with the Dursleys has been compared to
Cinderella.[23] Hogwarts resembles a medieval university-cum-castle with
several professors who belong to an Order of Merlin; Old Professor Binns
still lectures about the International Warlock Convention of 1289; and a
real historical person, a 14th-century scribe, Sir Nicolas Flamel, is
described as a holder of the Philosopher's Stone.[24] Other medieval
elements in Hogwarts include coats-of-arms and medieval weapons on the
walls, letters written on parchment and sealed with wax, the Great Hall of
Hogwarts, which is similar to the Great Hall of Camelot, the use of Latin
```

```
phrases, the tents put up for Quidditch tournaments, which are similar to
the "marvellous tents" put up for knightly tournaments, imaginary animals
like dragons and unicorns that exist around Hogwarts, and the banners with
heraldic animals for the four Houses of Hogwarts

Encrypted text:
Lgu Gpmmb Skllum zlkmiuz fuplymu ioprumb pqa oklifz ampeq fmko Pmlgymipq
oblg pqa fpimblpnuz. Gpmmb'z pvinilb lk ampe lgu Zekma kf Rmbffiqakm fmko
lgu Zkmliqr Gpl muzuovnuz lgu Pmlgymipq zekma iq lgu zlkqu nuruqa.[22] Giz
nifu eilg lgu Aymznubz gpz vuuq xkospmua lk Xiqaumunnp.[23] Gkrepmlz
muzuovnuz p ouaiucpn yqicumzilb-xyo-xpzlnu eilg zucumpn smkfuzzkmz egk
vunkqr lk pq Kmaum kf Oumniq; Kna Smkfuzzkm Viqqz zlinn nuxlymuz pvkyl lgu
Iqlumqplikqpn Epmnkxd Xkqcuqlikq kf 1289; pqa p mupn gizlkmixpn sumzkq, p
14lg-xuqlymb zxmivu, Zim Qixknpz Fnpoun, iz auzxmivua pz p gknaum kf lgu
Sginkzksgum'z Zlkqu.[24] Klgum ouaiucpn unuouqlz iq Gkrepmlz iqxnyau
xkplz-kf-pmoz pqa ouaiucpn eupskqz kq lgu epnnz, nullumz emilluq kq
spmxgouql pqa zupnua eilg epj, lgu Rmupl Gpnn kf Gkrepmlz, egixg iz zioinpm
lk lgu Rmupl Gpnn kf Xpounkl, lgu yzu kf Npliq sgmpzuz, lgu luqlz syl ys fkm
Wyiaailxg lkymqpouqlz, egixg pmu zioinpm lk lgu "opmcunnkyz luqlz" syl ys
fkm dqirglnb lkymqpouqlz, iopriqpmb pqiopnz nidu amprkqz pqa yqixkmqz lgpl
ujizl pmkyqa Gkrepmlz, pqa lgu vpqqumz eilg gumpnaix pqiopnz fkm lgu fkym
Gkyzuz kf Gkrepmlz
```

- Decrypt without key: Present the detail how to guest the key step by step;

Đoạn code decrypt bằng tần suất xuất hiện của kí tự:

```python
from collections import Counter
import string

english_frequencies = 'ETAOINSHRDLCUMWFGYPBVKJXQZ'

cipher_text = input("Enter the encrypted text: ")

cipher_counts = Counter(char.upper() for char in cipher_text if char.isalpha())

sorted_cipher = ''.join([item[0] for item in cipher_counts.most_common()])

mapping = {}
for i, letter in enumerate(sorted_cipher):
    if i < len(english_frequencies):
        mapping[letter] = english_frequencies[i]
    else:
        mapping[letter] = letter
```

```
decrypted_text = []
for char in cipher_text:
    if char.isalpha():
        if char.isupper():
            decrypted_text.append(mapping.get(char, char))
        else:
            decrypted_text.append(mapping.get(char.upper(), char).lower())
    else:
        decrypted_text.append(char)
decrypted_text = ''.join(decrypted_text)

print("Mapping used:")
for key in sorted(mapping.keys()):
    print(key, "=", mapping[key])

print("\nDecrypted text:")
print(decrypted_text)
```

Sau khi chạy đoạn code với đoạn Ciphertext được tạo trước đó thì kết quả trả về:

```
Enter the encrypted text: Lgu Gpmmb Skllum zlkmiuz fuplymu ioprumb pqa
oklifz ampeq fmko Pmlgymipq oblg pqa fpimblpnuz. Gpmmb'z pvinilb lk ampe lgu
Zekma kf Rmbffiqakm fmko lgu Zkmliqr Gpl muzuovnuz lgu Pmlgymipq zekma iq
lgu zlkqu nuruqa.[22] Giz nifu eilg lgu Aymznubz gpz vuuq xkospmua lk
Xiqaumunnp.[23] Gkrepmlz muzuovnuz p ouaiucpn yqicumzilb-xyo-xpzlnu eilg
zucumpn smkfuzzkmz egk vunkqr lk pq Kmaum kf Oumniq; Kna Smkfuzzkm Viqqz
zlinn nuxlymuz pvkyl lgu Iqlumqplikqpn Epmnkxd Xkqcuqlikq kf 1289; pqa p
mupn gizlkmixpn sumzkq, p 14lg-xuqlymb zxmivu, Zim Qixknpz Fnpoun, iz
auzxmivua pz p gknaum kf lgu Sginkzksgum'z Zlkqu.[24] Klgum ouaiucpn
unuouqlz iq Gkrepmlz iqxnyau xkplz-kf-pmoz pqa ouaiucpn eupskqz kq lgu
epnnz, nullumz emilluq kq spmxgouql pqa zupnua eilg epj, lgu Rmupl Gpnn kf
Gkrepmlz, egixg iz zioinpm lk lgu Rmupl Gpnn kf Xpounkl, lgu yzu kf Npliq
sgmpzuz, lgu luqlz syl ys fkm Wyiaailxg lkymqpouqlz, egixg pmu zioinpm lk
lgu "opmcunnkyz luqlz" syl ys fkm dqirglnb lkymqpouqlz, iopriqpmb pqiopnz
nidu amprkqz pqa yqixkmqz lgpl ujizl pmkyqa Gkrepmlz, pqa lgu vpqqumz eilg
gumpnaix pqiopnz fkm lgu fkym Gkyzuz kf Gkrepmlz
Mapping used:
A = L
B = P
C = V
D = K
E = W
F = U
G = R
```

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

Decrypted text:
Tre Raoop Yntteo itnosei ueatmoe scageop ahl cntsui loawh uonc Aotrmosah
cptr ahl uasoptadei. Raoop'i absdstp tn loaw tre Iwnol nu Gopuushlno uonc
tre Inotshg Rat oeiecbdei tre Aotrmosah iwnol sh tre itnhe degehl.[22] Rsi
dsue wstr tre Lmoidepi rai beeh fncyaoel tn Fshleoedda.[23] Rngwaoti
oeiecbdei a celsevad mhsveoistp-fmc-faitde wstr ieveoad yonueiinoi wrn
bednhg tn ah Noleo nu Ceodsh; Ndl Yonueiino Bshhi itsdd deftmoei abnmt tre
Shteohatsnhad Waodnfk Fnhvehtsnh nu 1289; ahl a oead rsitnosfad yeoinh, a
14tr-fehtmop ifosbe, Iso Hsfndai Udaced, si leifosbel ai a rndleo nu tre
Yrsdninyreo'i Itnhe.[24] Ntreo celsevad edecehti sh Rngwaoti shfdmle
fnati-nu-aoci ahl celsevad weaynhi nh tre waddi, detteoi wostteh nh
yaofrceht ahl ieadel wstr waj, tre Goeat Radd nu Rngwaoti, wrsfr si iscsdao
tn tre Goeat Radd nu Facednt, tre mie nu Datsh yroaiei, tre tehti ymt my uno
Xmsllstfr tnmohacehti, wrsfr aoe iscsdao tn tre "caoveddnmi tehti" ymt my
uno khsgrtdp tnmohacehti, scagshaop ahscadi dske loagnhi ahl mhsfnohi trat
ejsit aonmhl Rngwaoti, ahl tre bahheoi wstr reoadlsf ahscadi uno tre unmo
Rnmiei nu Rngwaoti
```

Chúng ta sẽ bắt dầu đoán chữ

- Ở đầu của đoạn Text có `Tre Raoop Yntteo` khả năng sẽ là The + danh từ vì thế chúng ta sẽ thử mapping kí tự đang gán giá trị “R” thành“H” thì ta được đoạn decrypt sau

```
Decrypted text:
The Haoop Yntteo itnosei ueatmoe scageop ahl cntsui loawh uonc Aothmosah
cpth ahl uasoptadei. Haoop'i absdstp tn loaw the Iwnol nu Gopuushlno uonc
the Inotshg Hat oeiecbdei the Aothmosah iwnol sh the itnhe degehl.[22] Hsi
dsue wsth the Lmoidepi hai beeh fncyaoel tn Fshleoedda.[23] Hngwaoti
oeiecbdei a celsevad mhsveoistp-fmc-faitde wsth ieveoad yonueiinoi whn
bednhg tn ah Noleo nu Ceodsh; Ndl Yonueiino Bshhi itsdd deftmoei abnmt the
```

Shteohatsnhad Waodnfk Fnhvehtsnh nu 1289; ahl a oead hsitnosfad yeoinh, a 14th-fehtmop ifosbe, Iso Hsfndai Udaced, si leifosbel ai a hndleo nu the Yhsdninyheo'i Itnhe.[24] Ntheo celsevad edecehti sh Hngwaoti shfdmle fnati-nu-aoci ahl celsevad weaynhi nh the waddi, detteoi wostteh nh yaofhceht ahl ieadel wsth waj, the Goeat Hadd nu Hngwaoti, whsfh si iscsdao tn the Goeat Hadd nu Facednt, the mie nu Datsh yhoaiei, the tehti ymt my uno Xmsllstfh tnmohacehti, whsfh aoe iscsdao tn the "caoveddnmi tehti" ymt my uno khsghtdp tnmohacehti, scagshaop ahscadi dske loagnhi ahl mhsfnohi that ejsit aonmhl Hngwaoti, ahl the bahheoi wsth heoadlsf ahscadi uno the unmo Hnmiei nu Hngwaoti

- Tiếp theo, Haoop'i absdstp tn loaw, kí tự “tn” có thể sẽ là “to” vậy chúng ta thử thay kí tự đang gán giá trị “N” thành “O” ta được

The Haoop Yotteo itoosei ueatmoe scageop ahl cotsui loawh uooc Aothmosah cpth ahl uasoptadei. Haoop'i absdstp to loaw the Iwool ou Gopuushloo uooc the Iootshg Hat oeiecbdei the Aothmosah iwool sh the itohe degehl.[22] Hsi dsue wsth the Lmoidepi hai beeh focyaoel to Fshleoedda.[23] Hogwaoti oeiecbdei a celsevad mhsveoistp-fmc-faitde wsth ieveoad yooueiiooi who bedohg to ah Ooleo ou Ceodsh; Odl Yooueiioo Bshhi itsdd deftmoei abomt the Shteohatsohad Waodofk Fohvehtsoh ou 1289; ahl a oead hsitoosfad yeoioh, a 14th-fehtmop ifosbe, Iso Hsfodai Udaced, si leifosbel ai a hodleo ou the Yhsdoioyheo'i Itohe.[24] Otheo celsevad edecehti sh Hogwaoti shfdmle foati-ou-aoci ahl celsevad weayohi oh the waddi, detteoi wostteh oh yaofhceht ahl ieadel wsth waj, the Goeat Hadd ou Hogwaoti, whsfh si iscsdao to the Goeat Hadd ou Facedot, the mie ou Datsh yhoaiei, the tehti ymt my uoo Xmsllstfh tomohacehti, whsfh aoe iscsdao to the "caoveddomi tehti" ymt my uoo khsghtdp tomohacehti, scagshaop ahscadi dske loagohi ahl mhsfoohi that ejsit aoomhl Hogwaoti, ahl the bahheoi wsth heoadlsf ahscadi uoo the uomo Homiei ou Hogwaoti

- Tiếp theo, Hsi osue wsth the Lmoioepi kí tự “wsth” có thể là “with” nên ta thay kí tự đang gán giá trị “S” thành “I” ta được

The Haoop Yotteo itooiei ueatmoe icageop ahl cotiui loawh uooc Aothmoiah cpth ahl uaioptadei. Haoop'i abiditp to loaw the Iwool ou Gopuuihloo uooc the Iootihg Hat oeiecbdei the Aothmoiah iwool ih the itohe degehl.[22] Hii diue with the Lmoidepi hai beeh focyaoel to Fihleoedda.[23] Hogwaoti oeiecbdei a celievad mhiveoiitp-fmc-faitde with ieveoad yooueiiooi who bedohg to ah Ooleo ou Ceodih; Odl Yooueiioo Bihhi itidd deftmoei abomt the Ihteohatiohad Waodofk Fohvehtioh ou 1289; ahl a oead hiitooifad yeoioh, a 14th-fehtmop ifoibe, Iio Hifodai Udaced, ii leifoibel ai a hodleo ou the Yhidoioyheo'i Itohe.[24] Otheo celievad edecehti ih Hogwaoti ihfdmle foati-ou-aoci ahl celievad weayohi oh the waddi, detteoi woitteh oh yaofhceht ahl ieadel with waj, the Goeat Hadd ou Hogwaoti, whifh ii iicidao to the Goeat Hadd ou Facedot, the mie ou Datih yhoaiei, the tehti ymt my uoo Xmillitfh tomohacehti, whifh aoe iicidao to the "caoveddomi tehti" ymt my uoo khightdp tomohacehti, icagihaop ahicadi dike loagohi ahl mhifoohi that ejiit aoomhl Hogwaoti, ahl the bahheoi with heoadlif ahicadi uoo the uomo Homiei ou Hogwaoti

- Tiếp theo, ahl the bahheoi with heoadlif kí tự “ahl” có thể là “all” nên ta thay kí tự đang gán giá trị “H” thành “L” ta được

The Haoop Yotteo itooiei ueatmoe icageop all cotiui loawl uooc Aothmoial cpth all uaioptadei. Haoop'i abiditp to loaw the Iwool ou Gopuuilloo uooc the Iootilg Hat oeiecbdei the Aothmoial iwool il the itole degell.[22] Hii diue with the Lmoidepi hai beel focyaoel to Filleoedda.[23] Hogwaoti oeiecbdei a celievad mliveoiitp-fmc-faitde with ieveoad yooueiiooi who bedolg to al Ooleo ou Ceodil; Odl Yooueiioo Billi itidd deftmoei abomt the Ilteolatiolad Waodofk Folveltiol ou 1289; all a oead hiitooifad yeoiol, a 14th-feltmop ifoibe, Iio Lifodai Udaced, ii leifoibel ai a hodleo ou the Yhidoioyheo'i Itole.[24] Otheo celievad edecelti il Hogwaoti ilfdmle foati-ou-aoci all celievad weayoli ol the waddi, detteoi woittel ol yaofhcelt all ieadel with waj, the Goeat Hadd ou Hogwaoti, whifh ii iicidao to the Goeat Hadd ou Facedot, the mie ou Datil yhoaiei, the telti ymt my uoo Xmillitfh tomolacelti, whifh aoe iicidao to the "caoveddomi telti" ymt my uoo klightdp tomolacelti, icagilaop alicadi dike loagoli all mlifooli that ejiit aooml Hogwaoti, all the balleoi with heoadlif alicadi uoo the uomo Homiei ou Hogwaoti

- Tiếp theo, Haoop'i kí tự ‘i sẽ là ‘s nên ta thay kí tự đang gán giá trị “I” thành “S” ta được

The Haoop Yotteo stooies ueatmoe icageop all cotius loawl uooc Aothmoial cpth all uaioptades. Haoop's abiditp to loaw the Swool ou Gopuuilloo uooc the Sootilg Hat oesecbdes the Aothmoial swool il the stole degell.[22] His diue with the Lmosdeps has beel focyaoel to Filleoedda.[23] Hogwaots oesecbdes a celievad mliveositp-fmc-fastde with seveoad yooeussoos who bedolg to al Ooleo ou Ceodil; Odl Yooeussoo Bills stidd deftmoes abomt the Ilteolatiolad Waodofk Folveltiol ou 1289; all a oead histooifad yeosol, a 14th-feltmop sfoibe, Sio Lifodas Udaced, is lesfoibel as a hodleo ou the Yhidosoyheo's Stole.[24] Otheo celievad edecelts il Hogwaots ilfdmle foats-ou-aocs all celievad weayols ol the wadds, detteos woittel ol yaofhcelt all seadel with waj, the Goeat Hadd ou Hogwaots, whifh is sicidao to the Goeat Hadd ou Facedot, the mse ou Datil yhoases, the telts ymt my uoo Xmillitfh tomolacelts, whifh aoe sicidao to the "caoveddoms telts" ymt my uoo klightdp tomolacelts, icagilaop alicads dike loagols all mlifools that ejist aooml Hogwaots, all the balleos with heoadlif alicads uoo the uomo Homses ou Hogwaots

- Tiếp theo, ejist có thể là exist nên ta thay kí tự đang gán giá trị “J” thành “X” ta được

The Haoop Yotteo stooies ueatmoe icageop all cotius loawl uooc Aothmoial cpth all uaioptades. Haoop's abiditp to loaw the Swool ou Gopuuilloo uooc the Sootilg Hat oesecbdes the Aothmoial swool il the stole degell.[22] His diue with the Lmosdeps has beel focyaoel to Filleoedda.[23] Hogwaots oesecbdes a celievad mliveositp-fmc-fastde with seveoad yooeussoos who bedolg to al Ooleo ou Ceodil; Odl Yoouessoo Bills stidd deftmoes abomt the Ilteolatiolad Waodofk Folveltiol ou 1289; all a oead histooifad yeosol, a 14th-feltmop sfoibe, Sio Lifodas Udaced, is lesfoibel as a hodleo ou the Yhidosoyheo's Stole.[24] Otheo celievad edecelts il Hogwaots ilfdmle foats-ou-aocs all celievad weayols ol the wadds, detteos woittel ol yaofhcelt all seadel with wax, the Goeat Hadd ou Hogwaots, whifh is sicidao to the Goeat Hadd ou Facedot, the mse ou Datil yhoases, the telts ymt my uoo Xmillitfh tomolacelts, whifh aoe sicidao to the "caoveddoms telts" ymt my uoo klightdp tomolacelts, icagilaop alicads dike loagols all mlifools that exist aooml Hogwaots, all the balleos with heoadlif alicads uoo the uomo Homses ou Hogwaots

- Tiếp theo, `has beel` sẽ là has been nên ta thay kí tự đang gán giá trị “L” thành “N”, lúc này ta đang có “all” bị đổi thành “anl” vậy ta sẽ đổi lại thành “and” nên ta thay kí tự đang gán giá trị “L” thành “D” ta được ta được

The Haoop Yotteo stooies ueatmoe icageop and cotius doawn uooc Aothmoian cpth and uaioptades. Haoop's abiditp to doaw the Swood ou Gopuuindoo uooc the Sooting Hat oesecbdes the Aothmoian swood in the stone degend.[22] His diue with the Dmosdeps has been focyaoed to Findeoedda.[23] Hogwaots oesecbdes a cedievad mniveositp-fmc-fastde with seveoad yoouessoos who bedong to an Oodeo ou Ceodin; Odd Yoouessoo Binns stidd deftmoes abomt the Inteonationad Waodofk Fonvention ou 1289; and a oead histooifad yeoson, a 14th-fentmop sfoibe, Sio Nifodas Udaced, is desfoibed as a hoddeo ou the Yhidosoyheo's Stone.[24] Otheo cedievad edecents in Hogwaots infdmde foats-ou-aocs and cedievad weayons on the wadds, detteos woitten on yaofhcent and seaded with wax, the Goeat Hadd ou Hogwaots, whifh is sicidao to the Goeat Hadd ou Facedot, the mse ou Datin yhoases, the tents ymt my uoo Xmidditfh tomonacents, whifh aoe sicidao to the "caoveddoms tents" ymt my uoo knightdp tomonacents, icaginaop anicads dike doagons and mnifoons that exist aoomnd Hogwaots, and the banneos with heoaddif anicads uoo the uomo Homses ou Hogwaots

- Tiếp theo, `whifh aoe` có thể sẽ là “which are” nên ta thay kí tự đang gán giá trị “F” thành “C” và “O” thành “R” ta được

The Harrp Yotter stories ueatmre icagerp and cotius drawn uroc Arthmrian cpth and uairptades. Harrp's abiditp to draw the Sword ou Grpuuindor uroc the Sorting Hat resecbdes the Arthmrian sword in the stone degend.[22] His diue with the Dmrsdeps has been cocyared to Cinderedda.[23] Hogwarts resecbdes a cedievad mniversitp-cmc-castde with severad yrouessors who bedong to an Order ou Cerdin; Odd Yrouessor Binns stidd dectmres abomt the Internationad Wardock Convention ou 1289; and a read historicad yerson, a 14th-centmrp scribe, Sir Nicodas Udaced, is described as a hodder ou the Yhidosoyher's Stone.[24] Other cedievad edecents in Hogwarts incdmde coats-ou-arcs and cedievad weayons on the wadds, detters written on yarchcent and seaded with wax, the Great Hadd ou Hogwarts, which is sicidar to the Great Hadd ou Cacedot, the mse ou Datin yhrases, the tents ymt my uor Xmidditch tomrnacents, which are sicidar to the "carveddoms tents" ymt my uor knightdp tomrnacents, icaginarp anicads dike dragons and mnicorns that exist aromnd Hogwarts, and the banners with heraddic anicads uor the uomr Homses ou Hogwarts

- Tiếp theo, is desccibed as a hoddec ou the Yhidosoyhec's Stone có thể sẽ là “is described as a holder of … “ nên ta thay kí tự đang gán giá trị “C” thành “R”, “D” thành “L” và “U” thành “F” ta được

The Harrp Yotter stories featmre iragerp and rotifs drawn fror Arthmrian rpth and fairptales. Harrp's abilitp to draw the Sword of Grpffindor fror the Sorting Hat reserbles the Arthmrian sword in the stone legend.[22] His life with the Dmrsleps has been coryared to Cinderella.[23] Hogwarts reserbles a redieval mniversitp-cmr-castle with several yrofessors who belong to an Order of Rerlin; Old Yrofessor Binns still lectmres abomt the International Warlock Convention of 1289; and a real historical yerson, a 14th-centmrp scribe, Sir Nicolas Flarel, is described as a holder of the Yhilosoyher's Stone.[24] Other redieval elerents in Hogwarts inclmde coats-of-arrs and redieval weayons on the walls, letters written on yarchrent and sealed with wax, the Great Hall of Hogwarts, which is sirilar to the Great Hall of Carelot, the mse of Latin yhrases, the tents ymt my for Xmidditch tomrnarents, which are sirilar to the "rarvelloms tents" ymt my for knightlp tomrnarents, iraginarp anirals like dragons and mnicorns that exist aromnd Hogwarts, and the banners with heraldic anirals for the fomr Homses of Hogwarts

- Tiếp theo, The Harrp Yotter stories featmre có thể sẽ là “The Harry Potter stories feature” nên ta thay kí tự đang gán giá trị “P” thành “Y”, “Y” thành “P” và “M” thành “U” ta được

The Harry Potter stories feature iragery and rotifs drawn fror Arthurian ryth and fairytales. Harry's ability to draw the Sword of Gryffindor fror the Sorting Hat reserbles the Arthurian sword in the stone legend.[22] His life with the Dursleys has been corpared to Cinderella.[23] Hogwarts reserbles a redieval university-cur-castle with several professors who belong to an Order of Rerlin; Old Professor Binns still lectures about the International Warlock Convention of 1289; and a real historical person, a 14th-century scribe, Sir Nicolas Flarel, is described as a holder of the Philosopher's Stone.[24] Other redieval elerents in Hogwarts include coats-of-arrs and redieval weapons on the walls, letters written on parchrent and sealed with wax, the Great Hall of Hogwarts, which is sirilar to the Great Hall of Carelot, the use of Latin phrases, the tents put up for Xuidditch tournarents, which are sirilar to the "rarvellous tents" put up for knightly tournarents, iraginary anirals like dragons and unicorns that exist around Hogwarts, and the banners with heraldic anirals for the four Houses of Hogwarts

- Tiếp theo, sirilar to có thể là “similar to” nên ta thay kí tự đang gán giá trị “R” thành “M” ta được

```
The Harry Potter stories feature imagery and motifs drawn from Arthurian
myth and fairytales. Harry's ability to draw the Sword of Gryffindor from
the Sorting Hat resembles the Arthurian sword in the stone legend.[22] His
life with the Dursleys has been compared to Cinderella.[23] Hogwarts
resembles a medieval university-cum-castle with several professors who
belong to an Order of Merlin; Old Professor Binns still lectures about the
International Warlock Convention of 1289; and a real historical person, a
14th-century scribe, Sir Nicolas Flamel, is described as a holder of the
Philosopher's Stone.[24] Other medieval elements in Hogwarts include
coats-of-arms and medieval weapons on the walls, letters written on
parchment and sealed with wax, the Great Hall of Hogwarts, which is similar
to the Great Hall of Camelot, the use of Latin phrases, the tents put up for
Xuidditch tournaments, which are similar to the "marvellous tents" put up
for knightly tournaments, imaginary animals like dragons and unicorns that
exist around Hogwarts, and the banners with heraldic animals for the four
Houses of Hogwarts
```

- Tiếp theo, `Xuidditch tournaments` sẽ là "Quidditch tournaments" nên ta thay kí tự đang gán giá trị "X" thành "Q" ta được

```
The Harry Potter stories feature imagery and motifs drawn from Arthurian
myth and fairytales. Harry's ability to draw the Sword of Gryffindor from
the Sorting Hat resembles the Arthurian sword in the stone legend.[22] His
life with the Dursleys has been compared to Cinderella.[23] Hogwarts
resembles a medieval university-cum-castle with several professors who
belong to an Order of Merlin; Old Professor Binns still lectures about the
International Warlock Convention of 1289; and a real historical person, a
14th-century scribe, Sir Nicolas Flamel, is described as a holder of the
Philosopher's Stone.[24] Other medieval elements in Hogwarts include
coats-of-arms and medieval weapons on the walls, letters written on
parchment and sealed with wax, the Great Hall of Hogwarts, which is similar
to the Great Hall of Camelot, the use of Latin phrases, the tents put up for
Quidditch tournaments, which are similar to the "marvellous tents" put up
for knightly tournaments, imaginary animals like dragons and unicorns that
exist around Hogwarts, and the banners with heraldic animals for the four
Houses of Hogwarts
```

Vậy ta đã hoàn thành giải mã đoạn text bị mã hóa, đoạn code python:

```python
from collections import Counter
import string

english_frequencies = 'ETAOINSHRDLCUMWFGYPBVKJXQZ'

cipher_text = input("Enter the encrypted text: ")

cipher_counts = Counter(char.upper() for char in cipher_text if char.isalpha())
```

```
sorted_cipher = ''.join([item[0] for item in cipher_counts.most_common()])

mapping = {}
for i, letter in enumerate(sorted_cipher):
    if i < len(english_frequencies):
        mapping[letter] = english_frequencies[i]
    else:
        mapping[letter] = letter

mapping['G'] = 'H'
mapping['K'] = 'O'
mapping['I'] = 'I'
mapping['Q'] = 'N'
mapping['Z'] = 'S'
mapping['J'] = 'X'
mapping['A'] = 'D'
mapping['X'] = 'C'
mapping['M'] = 'R'
mapping['O'] = 'M'
mapping['N'] = 'L'
mapping['F'] = 'F'
mapping['B'] = 'Y'
mapping['S'] = 'P'
mapping['Y'] = 'U'
mapping['W'] = 'Q'


decrypted_text = []
for char in cipher_text:
    if char.isalpha():
        if char.isupper():
            decrypted_text.append(mapping.get(char, char))
        else:
            decrypted_text.append(mapping.get(char.upper(), char).lower())
    else:
        decrypted_text.append(char)
decrypted_text = ''.join(decrypted_text)


print("Mapping used:")
```

```
for key in sorted(mapping.keys()):
    print(key, "=", mapping[key])

print("\nDecrypted text:")
print(decrypted_text)
```

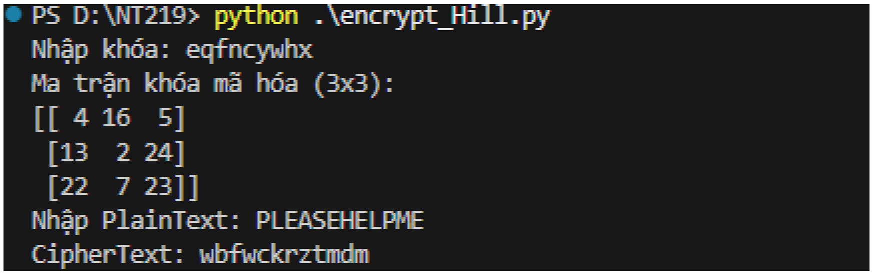
Task 3: Polyalphabetic
- Generate the Encrypt matric (2x2, 3x3, 4x4) for Polyalphabetic
2<-->2; 3<-->3; 4<-->4;
- Compute Decrypt Matrix (Invert mode 26)
- Your Encrypt, Decrypt code

Python encrypt code:

```
import math
import numpy as np

def filter_key(key):
    return ''.join([c for c in key.lower() if c.isalpha()])

def generateKeyMatrix(key, n):
    if len(key) != n * n:
        raise ValueError("Độ dài khóa không phù hợp với kích thước ma trận {}x{}".format(n, n))
    matrix = []
    for i in range(n):
        row = []
        for j in range(n):
            row.append(ord(key[i * n + j]) - ord('a'))
        matrix.append(row)
    matrix = np.array(matrix)

    if int(round(np.linalg.det(matrix))) == 0:
        raise ValueError("Invalid Key! Ma trận khóa không khả nghịch.")
    return matrix

def multiplyMatrixVector(matrix, vector):
    num_vector = np.array([[ord(c) - ord('a')] for c in vector])
    result = np.dot(matrix, num_vector) % 26
    return ''.join(chr(int(num) + ord('a')) for num in result.flatten())

def hillEncrypt(plaintext, keyMatrix):
```

```python
    n = keyMatrix.shape[0]
    plaintext = ''.join(plaintext.lower().split())
    if len(plaintext) % n != 0:
        plaintext += 'x' * (n - (len(plaintext) % n))
    ciphertext = ""
    for i in range(0, len(plaintext), n):
        block = plaintext[i:i+n]
        ciphertext += multiplyMatrixVector(keyMatrix, block)
    return ciphertext

if __name__ == "__main__":
    raw_key = input("Nhập khóa: ")
    key = filter_key(raw_key)

    key_length = len(key)
    n = int(math.sqrt(key_length))
    if n * n != key_length:
        raise ValueError("Độ dài khóa (sau khi lọc) phải là số chính phương, ví dụ 4, 9, 16, ...")

    encryptMatrix = generateKeyMatrix(key, n)
    print("Ma trận khóa mã hóa ({}x{}):".format(n, n))
    print(encryptMatrix)

    plaintext = input("Nhập PlainText: ")
    ciphertext = hillEncrypt(plaintext, encryptMatrix)
    print("CipherText:", ciphertext)
```

Kết quả:



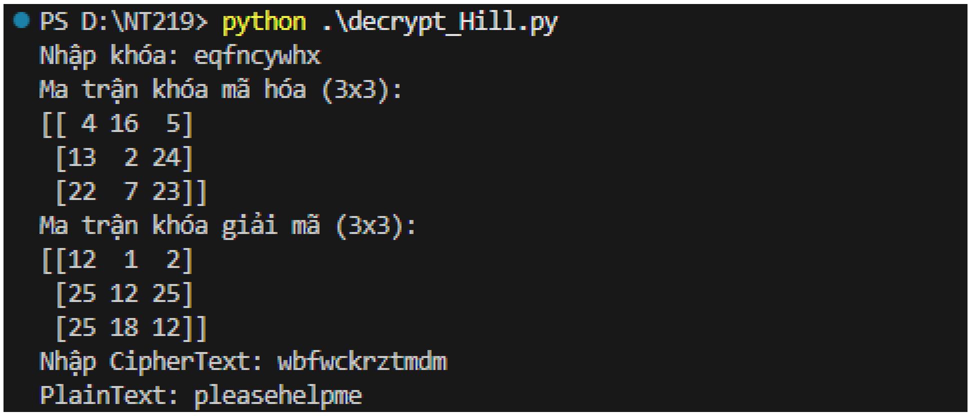
```
PS D:\NT219> python .\encrypt_Hill.py
Nhập khóa: eqfncywhx
Ma trận khóa mã hóa (3x3):
[[ 4 16  5]
 [13  2 24]
 [22  7 23]]
Nhập PlainText: PLEASEHELPME
CipherText: wbfwckrztmdm
```

Python decrypt code:

```python
import math
import numpy as np
import sympy

def filter_key(key):
    return ''.join([c for c in key.lower() if c.isalpha()])

def modInverse(a, m):
    a = a % m
    for x in range(1, m):
        if (a * x) % m == 1:
            return x
    raise ValueError("modInverse không tồn tại!")

def generateKeyMatrix(key, n):
    if len(key) != n * n:
        raise ValueError("Độ dài khóa không phù hợp với kích thước ma trận
{}x{}".format(n, n))
    matrix = []
    for i in range(n):
        row = []
        for j in range(n):
            row.append(ord(key[i * n + j]) - ord('a'))
        matrix.append(row)
    matrix = np.array(matrix)
    if int(round(np.linalg.det(matrix))) == 0:
        raise ValueError("Invalid Key! Ma trận khóa không khả nghịch.")
    return matrix

def computeDecryptMatrix(keyMatrix):
    n = keyMatrix.shape[0]
    det = int(round(np.linalg.det(keyMatrix))) % 26
    if det == 0:
        raise ValueError("Determinant bằng 0, khóa không hợp lệ!")
    inv_det = modInverse(det, 26)

    sympy_matrix = sympy.Matrix(keyMatrix.tolist())
    adjugate = sympy_matrix.adjugate()
    inv_matrix = (inv_det * adjugate) % 26
    inv_matrix = np.array(inv_matrix).astype(np.int64)
    return inv_matrix
```

```
def multiplyMatrixVector(matrix, vector):
    num_vector = np.array([[ord(c) - ord('a')] for c in vector])
    result = np.dot(matrix, num_vector) % 26
    return ''.join(chr(int(num) + ord('a')) for num in result.flatten())

def hillDecrypt(ciphertext, decryptMatrix):
    n = decryptMatrix.shape[0]
    ciphertext = ''.join(ciphertext.lower().split())
    plaintext = ""
    for i in range(0, len(ciphertext), n):
        block = ciphertext[i:i+n]
        plaintext += multiplyMatrixVector(decryptMatrix, block)
    return plaintext

if __name__ == "__main__":
    raw_key = input("Nhập khóa: ")
    key = filter_key(raw_key)

    key_length = len(key)
    n = int(math.sqrt(key_length))
    if n * n != key_length:
        raise ValueError("Độ dài khóa (sau khi lọc) phải là số chính phương, ví dụ 4, 9, 16, ...")

    keyMatrix = generateKeyMatrix(key, n)
    print("Ma trận khóa mã hóa ({}x{}):".format(n, n))
    print(keyMatrix)

    decryptMatrix = computeDecryptMatrix(keyMatrix)
    print("Ma trận khóa giải mã ({}x{}):".format(n, n))
    print(decryptMatrix)

    ciphertext = input("Nhập CipherText: ")
    plaintext = hillDecrypt(ciphertext, decryptMatrix)
    print("PlainText:", plaintext)
```

Kết quả:



```
● PS D:\NT219> python .\decrypt_Hill.py
  Nhập khóa: eqfncywhx
  Ma trận khóa mã hóa (3x3):
  [[ 4 16  5]
   [13  2 24]
   [22  7 23]]
  Ma trận khóa giải mã (3x3):
  [[12  1  2]
   [25 12 25]
   [25 18 12]]
  Nhập CipherText: wbfwckrztmdm
  PlainText: pleasehelpme
```