

# Report Week1,2

## 1. Cryptanalysis Affine cipher

- Encrypt một đoạn văn với  $a = 7$ ,  $b = 14$ .

```
zsh: command not found: cldear
→ Assignment1_2 ls
23520569_NguyenVanHung.docx  Decrypt.py  HackAffineCipher.py  week02_code  '~$520569_NguyenVanHung.docx'
→ Assignment1_2 python3 ./week02_code/AffineCipher.py
Enter the Key 'a' in  $(a * x + b) \bmod 26$  for the Affine cipher (must be coprime with 26): 7
Enter the Key 'b' in  $(a * x + b) \bmod 26$  for the Affine cipher (an integer): 14

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

Enter the text to encrypt: Technology has transformed the way we live, work, and communicate. With the rise of smartphones, social media, and artificial intelligence, our daily routines have become more efficient and interconnected. The internet allows instant access to information, making learning and research easier than ever. However, this digital revolution also comes with challenges, such as privacy concerns and screen addiction. While technology offers countless benefits, it is essential to use it wisely and maintain a balance between online and offline activities. In the future, innovations like smart homes, self-driving cars, and advanced medical treatments will continue to shape our world, making life more convenient and exciting.

Encrypted text:
Rqclbiniea lok rdbokxidugj rlg moa mq nsfq, midg, obj ciuuybscorq. Mstlrq dskq ix kuodrplibqk, kicson uqjso, obj odrsxscson sbrqnnse qbcq, iyd josna diyrsbqk lofq vqciug uidq qxxscsqbr obj sbrqdcibbqcrqj. Rlg sbrqdbqr onnimk sbkrobr oocqkk ri sbxiduorsib, uogsbe nqod bsbe obj dqkqodcl qoksqd rlob qfqd. Limqfqd, rlsk jsesron dqfinyrsib onki ciuqk msrl clonngbeqk, kyel ok pdsfoca cibcqdbk obj kcdqqb o jjsrsib. Mlsnq rqlbiniea ixqdk ciybrnqk vqbqsrk, sr sk qkkqbrson ri ykq sr mskqna obj uosbrqsb o vonobeq vqrmqgb ibnsq obj ixns bq ocrsfrsqk. Sb rlg xyrydq, sbbiforsibk nsgq kuodr liuqk, kqnx-jdsfsbe codk, obj ofjfbqj uqjcon rdqoruqbrk mgnn cibrsbyq ri klopq iyd midnj, uogsbe nsxq uidq cibfbsqbr obj qtsrsbe.

Press Enter to continue to decryption...

Decrypted text:
Technology has transformed the way we live, work, and communicate. With the rise of smartphones, social media, and artificial intelligence, our daily routines have become more efficient and interconnected. The internet allows instant access to information, making learning and research easier than ever. However, this digital revolution also comes with challenges, such as privacy concerns and screen addiction. While technology offers countless benefits, it is essential to use it wisely and maintain a balance between online and offline activities. In the future, innovations like smart homes, self-driving cars, and advanced medical treatments will continue to shape our world, making life more convenient and exciting.
→ Assignment1_2 |
```

- Nhận thấy rằng giá trị của  $a$  và  $b$  luôn nhỏ hơn 26 vì có thực hiện phép mod, thêm vào đó giá trị của  $a$  giảm bớt đi vì  $a$  phải là số nguyên tố cùng nhau với 26. Nhờ vào đó có thể brute force các giá trị có thể có của  $a$  và  $b$  sau đó chỉ cần xem plaintext có thể hiểu được hay không để nhận biết.
- Code: [Code](#)
- Sau khi chạy code vào thực hiện giải mã thì thấy được rằng phần plaintext ứng với  $a = 7$ ,  $b = 14$  là 1 đoạn văn có thể hiểu được nên có thể nhận định đây chính là thông điệp ban đầu.

```
a = 7
b = 13
plaintext: Itrwcdadvn wph igpchudgbts iwt lpn lt axkt, ldgz, pcs rdbbjcxrpit. Lxiw iwt gxht du hbpqiewdctb, hdxpa btsxp, pcs pgixuxrx
pa xcitaaxvtct, djg spxan gdjixctb wpkt qtrdbt bdgt tuuxrxtci pcs xcitgrdcctrits. Iwt xcitgcti paadh xchipci prrth id xcudgbpidx,
bpzxcv atpgcxvc pcs gthtgrw tpxtg iwpc tktg: Wdltktg, iwxx svxipa gtdajixdc pahd rdbth lxiw rwpaatcvth, hjrw ph egxkprn rdertgch p
cs hrgtte pssxrixdc. Lwxat itwcdadvn duutgh rdjciathh qtctuxih, xi xh thhtcixpa id jht xi lxhtan pcs bpxcipxc p qpapcrt qtiltfc dcaxc
t pcs duuaxct prixxixth. Xc iwt ujijgt, xcdkpiwdch axzt hbpqi wdbth, htau-sgxkxcv rpgb, pcs pskperts btsxra igtpibctih lxaa rdcixcj
t id hupet djg ldgas, bpzxcv axut bdgt rdckctxtci pcs tmrxixcv.

a = 7
b = 14
plaintext: Technology has transformed the way we live, work, and communicate. With the rise of smartphones, social media, and artificial intelligence, our daily routines have become more efficient and interconnected. The internet allows instant access to information, making learning and research easier than ever. However, this digital revolution also comes with challenges, such as privacy concerns and screen addiction. While technology offers countless benefits, it is essential to use it wisely and maintain a balance between online and offline activities. In the future, innovations like smart homes, self-driving cars, and advanced medical treatments will continue to shape our world, making life more convenient and exciting.

a = 7
b = 15
plaintext: Epnsyzwzrj sld ecydqzcxpo esp hlj hp wtgp, hzcv, lyo nzxxynlel. Htes esp ctdp zq dxlceaszypd, dzntlw xpotl, lyo lctetqnt
lw twexwtrvay, zfc elmt czfetud clag mpxze xzco pcatatve lya twexwtrvay, fep twexwtrvay lwxzhd twdalya lwpdd oz twexwtrvay
```

## 2. Cryptanalysis SimpleSubstitutionCipher

- Dựa vào code có sẵn chạy code lần đầu tiên và có được kết quả là:

```
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = A
z = O
l = I
q = N
c = S
f = H
j = R
r = D
g = L
b = C
x = U
e = M
w = W
k = F
y = G
d = Y
h = P
p = B
v = V
m = K
a = J
POADENS FIGG WNS HIT KHIWH TI ONYE EATOER WAFE IR UOADCREH, WOAUO LNV ONPPEH TI TOE LIST OIHST PEIPDE; EATOER REDNTAYES IR HENR FRAEH
CS, WOAUO AS UERTNAHDV LIRE MHMSMD. OE DAYEC NDIHE AH OAS OIMSE AH SNYADDE RIW, WOATOER HIHE PEHETRNTEC. N SAHGDE CILESTAU SMFFAUEC T
I SERVE OAL. OE BRENKFNSTEC NHC CAHEC NT TOE UDMB, NT OIMRS LNTOLNTAUNDDV FAJEC, AH TOE SNLE RIL, NT TOE SNLE TNBDE, HEYER TNKAHG OA
S LEADS WATO ITOER LELBERS, LMUO DESS BRAHGAGH N GMEST WATO OAL; NHC WEHT OILE NT EJNUTDV LACHAGOT, IHDV TI RETARE NT INUE TI BEC. OE
HEYER MSEC TOE UISV UONLBER S WOAUO TOE REFIRL PRIYACES FIR ATS FNYIMREC LELBERS. OE PNSSEC TEH OIMRS IMT IF TOE TWEHTV-FIMR AH SNYADDE
RIW, EATOER AH SDEEPAHG IR LNKAGH OAS TIADET.
→ Assignment1
```

- Vẫn chưa đọc được nội dung của thông điệp, nhận thấy được từ “TWEHTV-FIMR” xuất hiện nên đoán đó là từ “TWENTY-FOUR” hoặc “TWENTY-FIRE” sửa TWENTY trước.
- Sau khi thực hiện mapping có được kết quả là:

```
POADEAS FIGG WAS HIT KHIWH TI OAYE EATOER WAFE IR UOADCREH, WOAUO LAV OAPPPEH TI TOE LIST OIHST PEIPDE; EATOER REDATAYES IR HEAR FRAEH
CS, WOAUO AS UERTAANDV LIRE MHMSMD. OE DAYEC ADIHE AH OAS OIMSE AH SAYADDE RIW, WOATOER HIHE PEHETRATEC. A SAHGDE CILESTAU SMFFAUEC T
I SERVE OAL. OE BREAKFASTEC ANC CAHEC AT TOE UDMB, AT OIMRS LATOLATAUADDV FAJEC, AH TOE SALE RIL, AT TOE SALE TABDE, HEYER TAKAHG OA
S LEADS WATO ITOER LELBERS, LMUO DESS BRANGAGH A GMEST WATO OAL; ANC WEHT OILE AT EJAUTDV LACHAGOT, IHDV TI RETARE AT INUE TI BEC. OE
HEYER MSEC TOE UISV UOALBERS WOAUO TOE REFIRL PRIYACES FIR ATS FAYIMREC LELBERS. OE PASSEC TEH OIMRS IMT IF TOE TWEHTV-FIMR AH SAYADDE
RIW, EATOER AN SDEEPAHG IR LAKAGH OAS TIADET.
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = A
z = O
l = I
q = A
c = S
f = N
j = R
r = D
g = L
b = C
x = U
e = M
w = W
k = F
y = G
d = Y
h = P
p = B
v = Y
m = K
a = J
POADEAS FIGG WAS NIT KHIWH TI OAYE EATOER WAFE IR UOADCREH, WOAUO LAV OAPPPEH TI TOE LIST OIHST PEIPDE; EATOER REDATAYES IR HEAR FRAEH
CS, WOAUO AS UERTAANDV LIRE MHMSMD. OE DAYEC ADINE AN OAS OIMSE AN SAYADDE RIW, WOATOER NINE PENETRATEC. A SAHGDE CILESTAU SMFFAUEC T
I SERVE OAL. OE BREAKFASTEC ANC CANEC AT TOE UDMB, AT OIMRS LATOLATAUADDV FAJEC, AN TOE SALE RIL, AT TOE SALE TABDE, NEYER TAKANG OA
S LEADS WATO ITOER LELBERS, LMUO DESS BRANGAGH A GMEST WATO OAL; ANC WENT OILE AT EJAUTDV LACHAGOT, INDY TI RETARE AT INUE TI BEC. OE
NEYER MSEC TOE UISV UOALBERS WOAUO TOE REFIRL PRIYACES FIR ATS FAYIMREC LELBERS. OE PASSEC TEN OIMRS IMT IF TOE TWENTY-FIMR AN SAYADDE
RIW, EATOER AN SDEEPAHG IR LAKAGH OAS TIADET.
→ Assignment1
```



- Đoán từ “KNIWN” chính là “KNOWN”, kết quả nhận được là:

```
POADEAS FOGG WAS NOT KNOWN TO OAYE EATOER WAFE OR UOADCREN, WOAUO LAY OAPPEN TO TOE LOST OONEST PEOPDE; EATOER REDATAYES OR NEAR FRAEN
CS, WOAUO AS UERTAANDY LORE MNMSMAD. OE DAYEC ADONE AN OAS OOMSE AN SAYADDE ROW, WOATOER NONE PENETRATEC. A SANGDE COLESTAU SMFFAUEC T
O SERYE OAL. OE BREAKFASTEC ANC CANEC AT TOE UDMB, AT OOMRS LATOELATAUADDY FAJEC, AN TOE SALE ROOL, AT TOE SALE TABDE, NEYER TAKANG OA
S LEADS WATO QTOER LELBERS, LMUO DESS BRANGANG A GMEST WATO OAL; ANC WENT OOLE AT EJAUTDY LACNAGOT, ONDY TO RETARE AT ONUE TO BEC. OE
NEYER MSEC TOE UOSY UOALBERS WOAUO TOE REFORL PROVACES FOR ATS FAYOMREC LELBERS. OE PASSEC TEN OOMRS OMT OF TOE TWENTY-FOMR AN SAYADDE
ROW, EATOER AN SDEEPANG OR LAKANG OAS TOADET.
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = A
z = O
l = O
q = A
c = S
f = N
j = R
r = D
g = L
b = C
x = U
e = M
w = W
k = F
y = G
d = Y
h = P
p = B
v = Y
a = K
a = J
POADEAS FOGG WAS NOT KNOWN TO OAYE EATOER WAFE OR UOADCREN, WOAUO LAY OAPPEN TO TOE LOST OONEST PEOPDE; EATOER REDATAYES OR NEAR FRAEN
CS, WOAUO AS UERTAANDY LORE MNMSMAD. OE DAYEC ADONE AN OAS OOMSE AN SAYADDE ROW, WOATOER NONE PENETRATEC. A SANGDE COLESTAU SMFFAUEC T
O SERYE OAL. OE BREAKFASTEC ANC CANEC AT TOE UDMB, AT OOMRS LATOELATAUADDY FAJEC, AN TOE SALE ROOL, AT TOE SALE TABDE, NEYER TAKANG OA
S LEADS WATO QTOER LELBERS, LMUO DESS BRANGANG A GMEST WATO OAL; ANC WENT OOLE AT EJAUTDY LACNAGOT, ONDY TO RETARE AT ONUE TO BEC. OE
NEYER MSEC TOE UOSY UOALBERS WOAUO TOE REFORL PROVACES FOR ATS FAYOMREC LELBERS. OE PASSEC TEN OOMRS OMT OF TOE TWENTY-FOMR AN SAYADDE
ROW, EATOER AN SDEEPANG OR LAKANG OAS TOADET.
→ Assignment1
```

- Đoán từ “OAPPEN” chính là “HAPPEN”, sau khi thực hiện mapping kết quả thu được là:

```
PHADEAS FOGG WAS NOT KNOWN TO HAVE EATHER WAFE OR UHADCREN, WHAUH LAY HAPPEN TO THE LOST HONEST PEOPDE; EATHER REDATAYES OR NEAR FRAEN
CS, WHAUH AS UERTAANDY LORE MNMSMAD. HE DAYEC ADONE AN HAS HOMSE AN SAYADDE ROW, WHATHER NONE PENETRATEC. A SANGDE COLESTAU SMFFAUEC T
O SERYE HAL. HE BREAKFASTEC ANC CANEC AT THE UDMB, AT HOMRS LATHELATAUADDY FAJEC, AN THE SALE ROOL, AT THE SALE TABDE, NEYER TAKANG HA
S LEADS WATH OTHER LELBERS, LMUH DESS BRANGANG A GMEST WATH HAL; ANC WENT HOLE AT EJAUTDY LACNAGHT, ONDY TO RETARE AT ONUE TO BEC. HE
NEYER MSEC THE UOSY UHALBERS WHAUH THE REFORL PROVACES FOR ATS FAYOMREC LELBERS. HE PASSEC TEN HOMRS OMT OF THE TWENTY-FOMR AN SAYADDE
ROW, EATHER AN SDEEPANG OR LAKANG HAS TOADET.
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = A
z = H
l = O
q = A
c = S
f = N
j = R
r = D
g = L
b = C
x = U
e = M
w = W
k = F
y = G
d = Y
h = P
p = B
v = Y
m = K
a = J
PHADEAS FOGG WAS NOT KNOWN TO HAVE EATHER WAFE OR UHADCREN, WHAUH LAY HAPPEN TO THE LOST HONEST PEOPDE; EATHER REDATAYES OR NEAR FRAEN
CS, WHAUH AS UERTAANDY LORE MNMSMAD. HE DAYEC ADONE AN HAS HOMSE AN SAYADDE ROW, WHATHER NONE PENETRATEC. A SANGDE COLESTAU SMFFAUEC T
O SERYE HAL. HE BREAKFASTEC ANC CANEC AT THE UDMB, AT HOMRS LATHELATAUADDY FAJEC, AN THE SALE ROOL, AT THE SALE TABDE, NEYER TAKANG HA
S LEADS WATH OTHER LELBERS, LMUH DESS BRANGANG A GMEST WATH HAL; ANC WENT HOLE AT EJAUTDY LACNAGHT, ONDY TO RETARE AT ONUE TO BEC. HE
NEYER MSEC THE UOSY UHALBERS WHAUH THE REFORL PROVACES FOR ATS FAYOMREC LELBERS. HE PASSEC TEN HOMRS OMT OF THE TWENTY-FOMR AN SAYADDE
ROW, EATHER AN SDEEPANG OR LAKANG HAS TOADET.
→ Assignment1
```

- Đoán từ “TWENTY-FOMR” chính là “TWENTY-FOUR” sau khi thực hiện mapping thu được kết quả là:

```

PHADEAS FOGG WAS NOT KNOWN TO HAVE EATHER WAFE OR UHADCREN, WHAUH LAY HAPPEN TO THE LOST HONEST PEOPDE; EATHER REDATAYES OR NEAR FRAEN
CS, WHAUH AS UERTAANDY LORE MNMSMAD. HE DAYEC ADONE AN HAS HOMSE AN SAYADDE ROW, WHATHER NONE PENETRATEC. A SANGDE COLESTAU SMFFAUET T
O SERVE HAL. HE BREAKFASTEC ANC CANEC AT THE UDMB, AT HOMRS LATHELATAUADDY FAJEC, AN THE SALE ROOL, AT THE SALE TABDE, NEVER TAKANG HA
S LEADS WATH OTHER LELBERS, LMUH DESS BRANGANG A GMEST WATH HAL; ANC WENT HOLE AT EJAUTDY LACNAGHT, ONDY TO RETARE AT ONUE TO BEC. HE
NEVER MSEC THE UOSY UHALBERS WHAUH THE REFORL PROVACES FOR ATS FAYOMREC LELBERS. HE PASSEC TEN HOMRS OMT QF THE TWENTY-FOMR AN SAYADDE
ROW, EATHER AN SDEEPANG OR LAKANG HAS TOADET.
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = A
z = H
l = O
q = A
c = S
f = N
j = R
r = D
g = L
b = C
x = U
e = U
w = W
k = F
y = G
d = Y
h = P
p = B
v = Y
m = K
a = J
PHADEAS FOGG WAS NOT KNOWN TO HAVE EATHER WAFE OR UHADCREN, WHAUH LAY HAPPEN TO THE LOST HONEST PEOPDE; EATHER REDATAYES OR NEAR FRAEN
CS, WHAUH AS UERTAANDY LORE UNUSUAD. HE DAYEC ADONE AN HAS HOUSE AN SAYADDE ROW, WHATHER NONE PENETRATEC. A SANGDE COLESTAU SUFFAUET T
O SERVE HAL. HE BREAKFASTEC ANC CANEC AT THE UDUB, AT HOURS LATHELATAUADDY FAJEC, AN THE SALE ROOL, AT THE SALE TABDE, NEVER TAKANG HA
S LEADS WATH OTHER LELBERS, LMUH DESS BRANGANG A GMEST WATH HAL; ANC WENT HOLE AT EJAUTDY LACNAGHT, ONDY TO RETARE AT ONUE TO BEC. HE
NEVER USEC THE UOSY UHALBERS WHAUH THE REFORL PROVACES FOR ATS FAYOUREC LELBERS. HE PASSEC TEN HOURS OUT OF THE TWENTY-FOUR AN SAYADDE
ROW, EATHER AN SDEEPANG OR LAKANG HAS TOADET.
→ Assignment1

```

- Đoán từ “HAYE” chính là từ “HAVE” sau khi thực hiện mapping thu được kết quả là:

```

PHADEAS FOGG WAS NOT KNOWN TO HAVE EATHER WAFE OR UHADCREN, WHAUH LAY HAPPEN TO THE LOST HONEST PEOPDE; EATHER REDATAYES OR NEAR FRAEN
CS, WHAUH AS UERTAANDY LORE UNUSUAD. HE DAYEC ADONE AN HAS HOUSE AN SAVADDE ROW, WHATHER NONE PENETRATEC. A SANGDE COLESTAU SUFFAUET T
O SERVE HAL. HE BREAKFASTEC ANC CANEC AT THE UDUB, AT HOURS LATHELATAUADDY FAJEC, AN THE SALE ROOL, AT THE SALE TABDE, NEVER TAKANG HA
S LEADS WATH OTHER LELBERS, LMUH DESS BRANGANG A GMEST WATH HAL; ANC WENT HOLE AT EJAUTDY LACNAGHT, ONDY TO RETARE AT ONUE TO BEC. HE
NEVER USEC THE UOSY UHALBERS WHAUH THE REFORL PROVACES FOR ATS FAYOUREC LELBERS. HE PASSEC TEN HOURS OUT OF THE TWENTY-FOUR AN SAVADDE
ROW, EATHER AN SDEEPANG OR LAKANG HAS TOADET.
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = A
z = H
l = O
q = A
c = S
f = N
j = R
r = D
g = L
b = C
x = U
e = U
w = W
k = F
y = G
d = V
h = P
p = B
v = Y
m = K
a = J
PHADEAS FOGG WAS NOT KNOWN TO HAVE EATHER WAFE OR UHADCREN, WHAUH LAY HAPPEN TO THE LOST HONEST PEOPDE; EATHER REDATAYES OR NEAR FRAEN
CS, WHAUH AS UERTAANDY LORE UNUSUAD. HE DAYEC ADONE AN HAS HOUSE AN SAVADDE ROW, WHATHER NONE PENETRATEC. A SANGDE COLESTAU SUFFAUET T
O SERVE HAL. HE BREAKFASTEC ANC CANEC AT THE UDUB, AT HOURS LATHELATAUADDY FAJEC, AN THE SALE ROOL, AT THE SALE TABDE, NEVER TAKANG HA
S LEADS WATH OTHER LELBERS, LMUH DESS BRANGANG A GMEST WATH HAL; ANC WENT HOLE AT EJAUTDY LACNAGHT, ONDY TO RETARE AT ONUE TO BEC. HE
NEVER USEC THE UOSY UHALBERS WHAUH THE REFORL PROVACES FOR ATS FAYOUREC LELBERS. HE PASSEC TEN HOURS OUT OF THE TWENTY-FOUR AN SAVADDE
ROW, EATHER AN SDEEPANG OR LAKANG HAS TOADET.
→ Assignment1

```



- Đoán từ “WATH” chính là “WITH” thực hiện mapping và thu được kết quả là:

```
PHIDEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR UNHILCREN, WHIWH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIENDS, WHIWH IS CERTAINLY MORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE COLESTIU SUFFICIENT TO SERVE HIM. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS LATELY ADDED TO THE SALE ROOM, AT THE SALE TABLE, NEVER TAKING HIS LEASURES WITH OTHER MEMBERS, BUT LESS BRINGING A GUEST WITH HIM; AND WENT HOME AT EARLY LICHNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE NEVER USED THE USUAL UNHILCREN WHICH THE REFORM PROVIDES FOR ITS FAVOURABLE MEMBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE ROW, EITHER IN SLEEPING OR MAKING HIS TOILET.
```

→ Assignment1 python3 Decrypt.py

n = E  
o = T  
s = I  
z = H  
l = O  
q = A  
c = S  
f = N  
j = R  
r = D  
g = L  
b = C  
x = U  
e = U  
w = W  
k = F  
y = G  
d = V  
h = P  
p = B  
v = Y  
m = K  
a = J

```
PHIDEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR UNHILCREN, WHIWH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIENDS, WHIWH IS CERTAINLY MORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE COLESTIU SUFFICIENT TO SERVE HIM. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS LATELY ADDED TO THE SALE ROOM, AT THE SALE TABLE, NEVER TAKING HIS LEASURES WITH OTHER MEMBERS, BUT LESS BRINGING A GUEST WITH HIM; AND WENT HOME AT EARLY LICHNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE NEVER USED THE USUAL UNHILCREN WHICH THE REFORM PROVIDES FOR ITS FAVOURABLE MEMBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE ROW, EITHER IN SLEEPING OR MAKING HIS TOILET.
```

→ Assignment1

- Xuất hiện 2 từ “PEOPDE” và “SDEEPING” nên đoán 2 từ đó chính là “PEOPLE” và “SLEEPING”, sau khi thực hiện mapping thu được kết quả là:

```
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR UNHILCREN, WHIWH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIENDS, WHIWH IS CERTAINLY MORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE COLESTIU SUFFICIENT TO SERVE HIM. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS LATELY ADDED TO THE SALE ROOM, AT THE SALE TABLE, NEVER TAKING HIS LEASURES WITH OTHER MEMBERS, BUT LESS BRINGING A GUEST WITH HIM; AND WENT HOME AT EARLY LICHNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE NEVER USED THE USUAL UNHILCREN WHICH THE REFORM PROVIDES FOR ITS FAVOURABLE MEMBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE ROW, EITHER IN SLEEPING OR MAKING HIS TOILET.
```

→ Assignment1 python3 Decrypt.py

n = E  
o = T  
s = I  
z = H  
l = O  
q = A  
c = S  
f = N  
j = R  
r = D  
g = L  
b = C  
x = U  
e = U  
w = W  
k = F  
y = G  
d = V  
h = P  
p = B  
v = Y  
m = K  
a = J

```
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR UNHILCREN, WHIWH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIENDS, WHIWH IS CERTAINLY MORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE COLESTIU SUFFICIENT TO SERVE HIM. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS LATELY ADDED TO THE SALE ROOM, AT THE SALE TABLE, NEVER TAKING HIS LEASURES WITH OTHER MEMBERS, BUT LESS BRINGING A GUEST WITH HIM; AND WENT HOME AT EARLY LICHNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE NEVER USED THE USUAL UNHILCREN WHICH THE REFORM PROVIDES FOR ITS FAVOURABLE MEMBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE ROW, EITHER IN SLEEPING OR MAKING HIS TOILET.
```

→ Assignment1

- Đoán từ “WHIUH” chính là từ “WHICH”, sau khi thực hiện mapping thì có được kết quả là:

```

./Assignment1
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR CHILDREN, WHICH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIEN
CS, WHICH IS CERTAINLY LORE UNUSUAL. HE LIVEC ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATEC. A SINGLE COLESTIC SUFFICEC T
O SERVE HIL. HE BREAKFASTEC ANC CINEC AT THE CLUB, AT HOURS LATHELATICALLY FIJEC, IN THE SALE ROOL, AT THE SALE TABLE, NEVER TAKING HI
S LEALS WITH OTHER LELBERS, LUCH LESS BRINGING A GUEST WITH HIL; ANC WENT HOLE AT EJACTLY LICNIGHT, ONLY TO RETIRE AT ONCE TO BEC. HE
NEVER USEC THE COSY CHALBERS WHICH THE REFORL PROVIDES FOR ITS FAVOUREC LELBERS. HE PASSEC TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE
ROW, EITHER IN SLEEPING OR LAKING HIS TOILET.
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = I
z = H
l = O
q = A
c = S
f = N
j = R
r = L
g = L
b = C
x = C
e = U
w = W
k = F
y = G
d = V
h = P
p = B
v = Y
m = K
a = J
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR CHILDREN, WHICH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIEN
DS, WHICH IS CERTAINLY LORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE DOLESTIC SUFFICED T
O SERVE HIL. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS LATHELATICALLY FIJED, IN THE SALE ROOL, AT THE SALE TABLE, NEVER TAKING HI
S LEALS WITH OTHER LELBERS, LUCH LESS BRINGING A GUEST WITH HIL; AND WENT HOLE AT EJACTLY LIDNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE
NEVER USED THE COSY CHALBERS WHICH THE REFORL PROVIDES FOR ITS FAVOURED LELBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE
ROW, EITHER IN SLEEPING OR LAKING HIS TOILET.
→ Assignment1

```

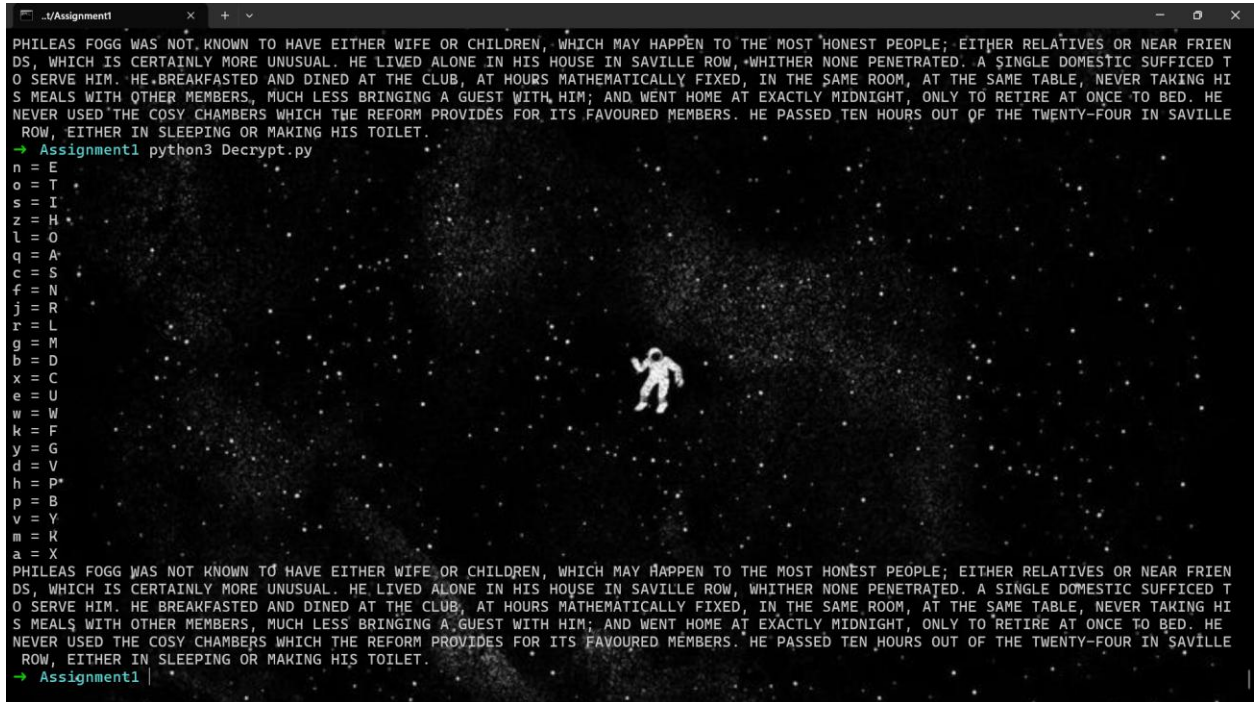
- Đoán từ “FRIENCS” chính là “FRIENDS”, sau khi thực hiện mapping thì thu được kết quả là:

```

./Assignment1
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR CHILDREN, WHICH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIEN
DS, WHICH IS CERTAINLY LORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE DOLESTIC SUFFICED T
O SERVE HIL. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS LATHELATICALLY FIJED, IN THE SALE ROOL, AT THE SALE TABLE, NEVER TAKING HI
S LEALS WITH OTHER LELBERS, LUCH LESS BRINGING A GUEST WITH HIL; AND WENT HOLE AT EJACTLY LIDNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE
NEVER USED THE COSY CHALBERS WHICH THE REFORL PROVIDES FOR ITS FAVOURED LELBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE
ROW, EITHER IN SLEEPING OR LAKING HIS TOILET.
→ Assignment1 python3 Decrypt.py
n = E
o = T
s = I
z = H
l = O
q = A
c = S
f = N
j = R
r = L
g = L
b = D
x = C
e = U
w = W
k = F
y = G
d = V
h = P
p = B
v = Y
m = K
a = J
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR CHILDREN, WHICH LAY HAPPEN TO THE LOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIEN
DS, WHICH IS CERTAINLY LORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE DOLESTIC SUFFICED T
O SERVE HIL. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS LATHELATICALLY FIJED, IN THE SALE ROOL, AT THE SALE TABLE, NEVER TAKING HI
S LEALS WITH OTHER LELBERS, LUCH LESS BRINGING A GUEST WITH HIL; AND WENT HOLE AT EJACTLY LIDNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE
NEVER USED THE COSY CHALBERS WHICH THE REFORL PROVIDES FOR ITS FAVOURED LELBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE
ROW, EITHER IN SLEEPING OR LAKING HIS TOILET.
→ Assignment1

```

- TỪ “EJACTLY” chính là “EXACTLY” và “LIDNIGHT” là “MIDNIGHT”, thực hiện mapping và thu được kết quả là:



```
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR CHILDREN, WHICH MAY HAPPEN TO THE MOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIENDS, WHICH IS CERTAINLY MORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE DOMESTIC SUFFICED TO SERVE HIM. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS MATHEMATICALLY FIXED, IN THE SAME ROOM, AT THE SAME TABLE, NEVER TAKING HIS MEALS WITH OTHER MEMBERS, MUCH LESS BRINGING A GUEST WITH HIM; AND WENT HOME AT EXACTLY MIDNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE NEVER USED THE COSY CHAMBERS WHICH THE REFORM PROVIDES FOR ITS FAVOURED MEMBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE ROW, EITHER IN SLEEPING OR MAKING HIS TOILET.
```

```
→ Assignment1 python3 Decrypt.py
```

```
n = E  
o = T  
s = I  
z = H  
l = O  
q = A  
c = S  
f = N  
j = R  
r = L  
g = M  
b = D  
x = C  
e = U  
w = W  
k = F  
y = G  
d = V  
h = P  
p = B  
v = Y  
m = K  
a = X
```

```
PHILEAS FOGG WAS NOT KNOWN TO HAVE EITHER WIFE OR CHILDREN, WHICH MAY HAPPEN TO THE MOST HONEST PEOPLE; EITHER RELATIVES OR NEAR FRIENDS, WHICH IS CERTAINLY MORE UNUSUAL. HE LIVED ALONE IN HIS HOUSE IN SAVILLE ROW, WHITHER NONE PENETRATED. A SINGLE DOMESTIC SUFFICED TO SERVE HIM. HE BREAKFASTED AND DINED AT THE CLUB, AT HOURS MATHEMATICALLY FIXED, IN THE SAME ROOM, AT THE SAME TABLE, NEVER TAKING HIS MEALS WITH OTHER MEMBERS, MUCH LESS BRINGING A GUEST WITH HIM; AND WENT HOME AT EXACTLY MIDNIGHT, ONLY TO RETIRE AT ONCE TO BED. HE NEVER USED THE COSY CHAMBERS WHICH THE REFORM PROVIDES FOR ITS FAVOURED MEMBERS. HE PASSED TEN HOURS OUT OF THE TWENTY-FOUR IN SAVILLE ROW, EITHER IN SLEEPING OR MAKING HIS TOILET.
```

```
→ Assignment1
```

- Thông điệp đã được chuyển về bản raw và có thể hiểu được dễ dàng.



### 3. Polyalphabetic

#### - Ma trận 2x2

- Ở phần code mẫu có sai ở phần xử lí khoảng trắng, sau khi chỉnh lại một chút thì đã giải mã đúng plaintext

```
.Assignment1.2 x + v
→ Assignment1.2 git:(main) X python3 HillCipher2.py
Hill Cipher (2x2 Matrix)
Enter 4 integers (space-separated) to form the key matrix.(a b c d):
Key: 1 4 1 1

Key Matrix:
1 4
1 1

Inverse Key Matrix:
17 10
9 17

Enter the plaintext to encrypt: Alice was beginning to get very tired of sitting by her sister on the bank and of having nothing to do
, once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, "and what is the u
se of a book," thought Alice, "without pictures or conversations?" So she was considering in her own mind, as well as she could, for t
he hot day made her feel very sleepy and stupid, whether the pleasure of making a daisy-chain would be worth the trouble of getting up
and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her.

Encrypted Text: **
SLQKO AUS RFMONAIVE ZM UCX LZJP ZBHVH RZ XGBZBLT TZ XLL JCAJXV FL GXL BUBX ANH RH MGIVIG TMHNPLT XH HR, OMSG EF DPQKY WXL HHL SUIFTJ L
LGM HXL FPCY XLL JCAJXB NUS HVMDIVK, HSN GB HHD QW DQVNVHVM GZ TOBLZLJYMMWHF IV GB, "ANN ZHHZ BQ LXL OMI SF F FPCY," VAQIINT TRTSG, "C
EVAQIB IQVNVHVM GZ TOBLZLJYMMWHF?" WG UZO AUS GQHFULUVIVM OP UUV YKJ ZIVD, DC OWPL LM KXL GOMFX, IEF VAG LMH DDU KMDG LUV VJWP LZJP KD
UJHN ANX VNVVXN, ZXLVAUV VAM TBPUSKLI SB ROKIVG G DDCAG-AHHIV AKMEH EO AEFVA VAC XVFYVBP IT WKRMIVI-AP PZO VXQWIVE ZXL DDCAYMC, OXLF F
GXTHFYF Y YDGBU VEBHJD PGBP WIVA OOCI JAN UNIGI FA FUV.

Cipher Letter Frequencies (most common first):
V: 39
L: 32
H: 29
I: 25
A: 24
G: 23
X: 22
F: 20
B: 20
M: 19
```

```
.Assignment1.2 x + v
Cipher Letter Frequencies (most common first):
V: 39
L: 32
H: 29
I: 25
A: 24
G: 23
X: 22
F: 20
B: 20
M: 19
U: 18
Z: 18
N: 16
D: 16
P: 15
T: 15
O: 14
K: 13
J: 13
Q: 12
C: 12
Y: 12
S: 11
W: 11
E: 8
R: 7

Press Enter to continue to decryption...

Decrypted Text:
ALICE WAS BEGINNING TO GET VERY TIRED OF SITTING BY HER SISTER ON THE BANK AND OF HAVING NOTHING TO DO, ONCE OR TWICE SHE HAD PEEPED I
NTO THE BOOK HER SISTER WAS READING, BUT IT HAD NO PICTURES OR CONVERSATIONS IN IT, "AND WHAT IS THE USE OF A BOOK," THOUGHT ALICE, "W
ITHOUT PICTURES OR CONVERSATIONS?" SO SHE WAS CONSIDERING IN HER OWN MIND, AS WELL AS SHE COULD, FOR THE HOT DAY MADE HER FEEL VERY SL
EEPY AND STUPID, WHETHER THE PLEASURE OF MAKING A DAISY-CHAIN WOULD BE WORTH THE TROUBLE OF GETTING UP AND PICKING THE DAISIES, WHEN S
UDDENLY A WHITE RABBIT WITH PINK EYES RAN CLOSE BY HER.
→ Assignment1.2 git:(main) X
```

- Code: [code](#)



### - Ma trận 3x3:-

- Ở code phần decrypt cũng bị sai ở phần xử lí khoảng trắng nên sau khi thực hiện sửa lại thì đã chạy được:

```
Assignment1.2 X python3 HillCipher3.py
Hill Cipher (3x3 Matrix)
Enter 9 integers (space-separated) to form the key matrix.(row-wise):
Key: 1 4 1 1 2 0 0 5 5

Key Matrix:
1 4 1
1 2 0
0 5 5

Inverse Key Matrix:
24 3 16
1 25 5
25 1 16

Enter the plaintext to encrypt: Alice was beginning to get very tired of sitting by her sister on the bank and of having nothing to do
, once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, "and what is the use
of a book," thought Alice, "without pictures or conversations?" So she was considering in her own mind, as well as she could, for the
hot day made her feel very sleepy and stupid, whether the pleasure of making a daisy-chain would be worth the trouble of getting up
and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her.

Encrypted Text:
AWROK AVK RKQSVNBEZ VQ AYD JVCN HCQBM FR RIFMJB IY OPB QIAABB HO EYP ZKAL DAC PY IOQPYZ RTAAOIR AV HF, QFGK ML DXUME YGD KHP JXOIXJ B
IET AAW GXJI HMM TVSDQM NLK THEPOIR, WPN NU AZG CE SLUONZZG GW RJOQMMTGFMGOZ QI BG, "TNU VPGM FX EAY SIN GR S CXVI," PFJOBUA AWROK, "A
NUAJCN XFYMHDMO EN VCXDLBMMJGZX?" YP YVW WGO WCPXAKLBOIR PI WIM ZIW VLIC, QK SHAG MK YZP EBCZL, NRW DAU SBF ZPU WIAL DZM GFMX CDBD IP
JMRL YNQ NDXYLU, VPJQANM YMP RBTULGDN GR WMYOIR M GPASC-EQJEI TBCZL FZ RYZOH AQP LPTXXX OY DVQIOIR CY XOT MAMIOIR ZHD LDOCIJ, KPWE Z
JAEPEQU Y GGXFU MHNDTL LUKH GSIL AAKI AHG RMYG AX ZRM S

Cipher Letter Frequencies (most common first):
A: 31
I: 30
M: 28
O: 25
G: 23
P: 22
R: 21
N: 19
Z: 19
Y: 19
L: 18
D: 17
X: 17
B: 16
K: 15
V: 15
Q: 15
C: 15
E: 14
J: 14
W: 13
H: 13
U: 13
F: 12
T: 11
S: 10
```

```
Assignment1.2 X
Cipher Letter Frequencies (most common first):
A: 31
I: 30
M: 28
O: 25
G: 23
P: 22
R: 21
N: 19
Z: 19
Y: 19
L: 18
D: 17
X: 17
B: 16
K: 15
V: 15
Q: 15
C: 15
E: 14
J: 14
W: 13
H: 13
U: 13
F: 12
T: 11
S: 10

Press Enter to continue to decryption...

Decrypted Text:
ALICE WAS BEGINNING TO GET VERY TIRED OF SITTING BY HER SISTER ON THE BANK AND OF HAVING NOTHING TO DO, ONCE OR TWICE SHE HAD PEEPED I
NTO THE BOOK HER SISTER WAS READING, BUT IT HAD NO PICTURES OR CONVERSATIONS IN IT, "AND WHAT IS THE USE OF A BOOK," THOUGHT ALICE, "W
ITHOUT PICTURES OR CONVERSATIONS?" SO SHE WAS CONSIDERING IN HER OWN MIND, AS WELL AS SHE COULD, FOR THE HOT DAY MADE HER FEEL VERY SL
EEPY AND STUPID, WHETHER THE PLEASURE OF MAKING A DAISY-CHAIN WOULD BE WORTH THE TROUBLE OF GETTING UP AND PICKING THE DAISIES, WHEN S
UDDENLY A WHITE RABBIT WITH PINK EYES RAN CLOSE BY HER. X

Assignment1.2 git:(main) X
```

- Code: [code](#)

- **Ma trận 4x4:**

- o Dựa thêm ý tưởng của code trên triển khai với ma trận 4x4

```

Assignment1.2
→ Assignment1.2 git:(main) X python3 HillCipher4.py
Hill Cipher (4x4 Matrix)
Enter 16 integers, (space-separated) to form the key matrix (row-wise):
1 4 1 1 2 0 0 5 0 5 0 5 4 4 1 1

Key_matrix
1 4 1 1
2 0 0 5
0 5 0 5
4 4 1 1

Inverse Key Matrix:
17 0 0 9
12 5 21 14
0 11 20 1
14 21 0 12

Enter the plaintext to encrypt: Alice was beginning to get very tired of sitting by her sister on the bank and of having nothing to do
, once or twice she had peeped into the book her sister was reading, but it had no pictures or conversations in it, "and what is the use
of a book," thought Alice, "without pictures or conversations?" So she was considering in her own mind, as well as she could, for the
hot day made her feel very sleepy and stupid, whether the pleasure of making a daisy-chain would be worth the trouble of getting up
and picking the daisies, when suddenly a White Rabbit with pink eyes ran close by her.
Encrypted Text:
CKNCG USS FQIINAVY QV QBC LNKW EJYAM XA BDPSQSQX EW KHL UYKQEM TW ULJ YAYB RSF RC LKRBD A ZBQFRSS WF IT, FRXL BD NWQSJ CGV ZLX UNCOZP X
FYX WLN DAQG GAG BZKGXT USS KXJJPV, NTF IB XBN SG MHWQGV UC RNWHEZDDRCPE JH EH, "ZGT ZICO DB ELD GGE OU C SJCL," HSDLFTM AORWS, "I
CDIFIL WHQGGQVP UC RNWHEZDDRCPE?" VT BXG USS LQERPXWNWEB UK HQX XKO NLON, JR NJTV IM CNG MIUNC, CEL QUN ZAZ NOI WXJY XDC BPVC XHML TL
HYKT VMZ VSAKXY, AAHQTV OJG TTIGACGZ KL IGAOQN M DSMMN-WKHSI FQQT I YT PNFVV SAH AJTNJZV SW TIMZERX MW PWO DJLRLRP GLH DSMMMWA, KQAG X
NIJVDAD Q ZJANV NMHWIU ZCNO AWKH UXDB RND QNNHR DV DQP.
Press Enter to continue to decryption...
Decrypted Text:
ALICE WAS BEGINNING TO GET VERY TIRED OF SITTING BY HER SISTER ON THE BANK AND OF HAVING NOTHING TO DO, ONCE OR TWICE SHE HAD PEEPED I
NTO THE BOOK HER SISTER WAS READING, BUT IT HAD NO PICTURES OR CONVERSATIONS IN IT, "AND WHAT IS THE USE OF A BOOK," THOUGHT ALICE, "W
ITHOUT PICTURES OR CONVERSATIONS?" SO SHE WAS CONSIDERING IN HER OWN MIND, AS WELL AS SHE COULD, FOR THE HOT DAY MADE HER FEEL VERY SL
EEPY AND STUPID, WHETHER THE PLEASURE OF MAKING A DAISY-CHAIN WOULD BE WORTH THE TROUBLE OF GETTING UP AND PICKING THE DAISIES, WHEN S
UDDENLY A WHITE RABBIT WITH PINK EYES RAN CLOSE BY HER.
→ Assignment1.2 git:(main) X

```

- o Code: [code](#)