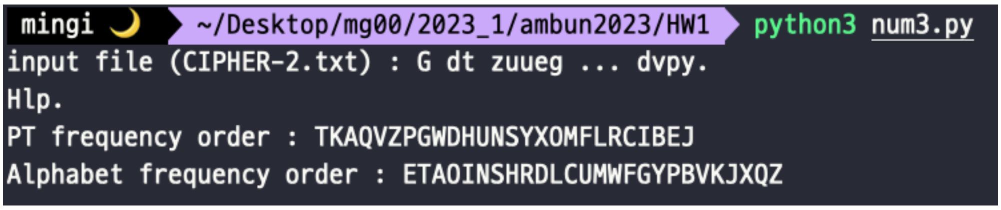
문제 3번 해결 방법:

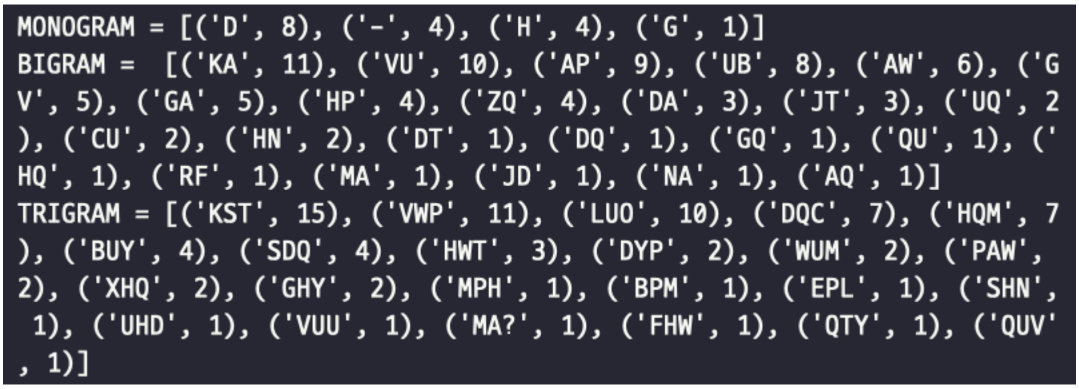
20192210 김민기

우선 주어진 암호문을 기존처럼 알파벳 빈도분석 진행

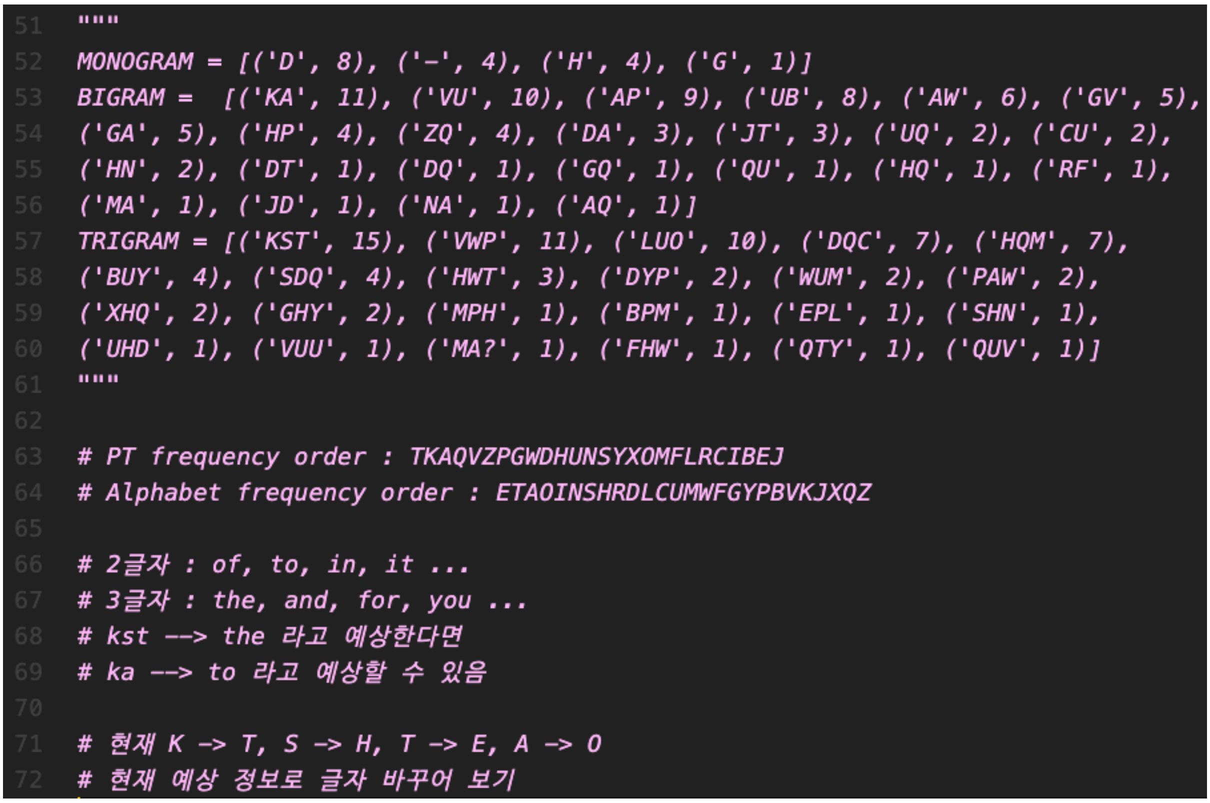


```
mingi 🌙  ~/Desktop/mg00/2023_1/ambun2023/HW1  python3 num3.py
input file (CIPHER-2.txt) : G dt zuueg ... dvpy.
Hlp.
PT frequency order : TKAQVZPGWDHUNSYXOMFLRCIBEJ
Alphabet frequency order : ETAOINSHRDLCUMWFGYPBVKJXQZ
```

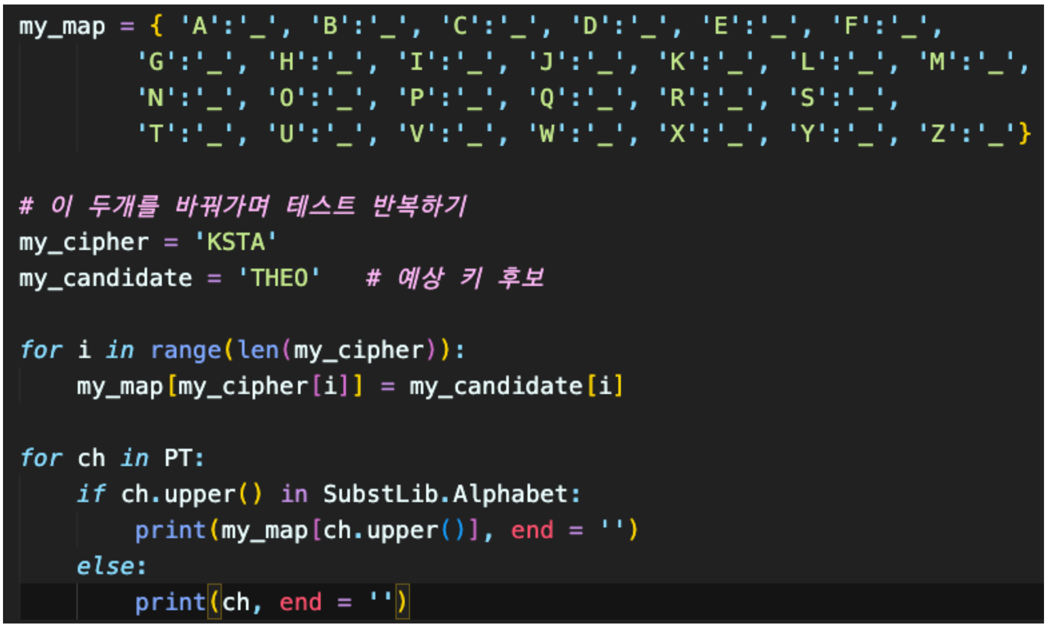
추가로 암호문에서 한글자, 두글자, 세글자로 된 단어들의 빈도 분석을 진행



```
MONOGRAM = [('D', 8), ('-', 4), ('H', 4), ('G', 1)]
BIGRAM =  [('KA', 11), ('VU', 10), ('AP', 9), ('UB', 8), ('AW', 6), ('G
V', 5), ('GA', 5), ('HP', 4), ('ZQ', 4), ('DA', 3), ('JT', 3), ('UQ', 2
), ('CU', 2), ('HN', 2), ('DT', 1), ('DQ', 1), ('GQ', 1), ('QU', 1), ('
HQ', 1), ('RF', 1), ('MA', 1), ('JD', 1), ('NA', 1), ('AQ', 1)]
TRIGRAM = [('KST', 15), ('VWP', 11), ('LUO', 10), ('DQC', 7), ('HQM', 7
), ('BUY', 4), ('SDQ', 4), ('HWT', 3), ('DYP', 2), ('WUM', 2), ('PAW',
2), ('XHQ', 2), ('GHY', 2), ('MPH', 1), ('BPM', 1), ('EPL', 1), ('SHN',
 1), ('UHD', 1), ('VUU', 1), ('MA?', 1), ('FHW', 1), ('QTY', 1), ('QUV'
, 1)]
```

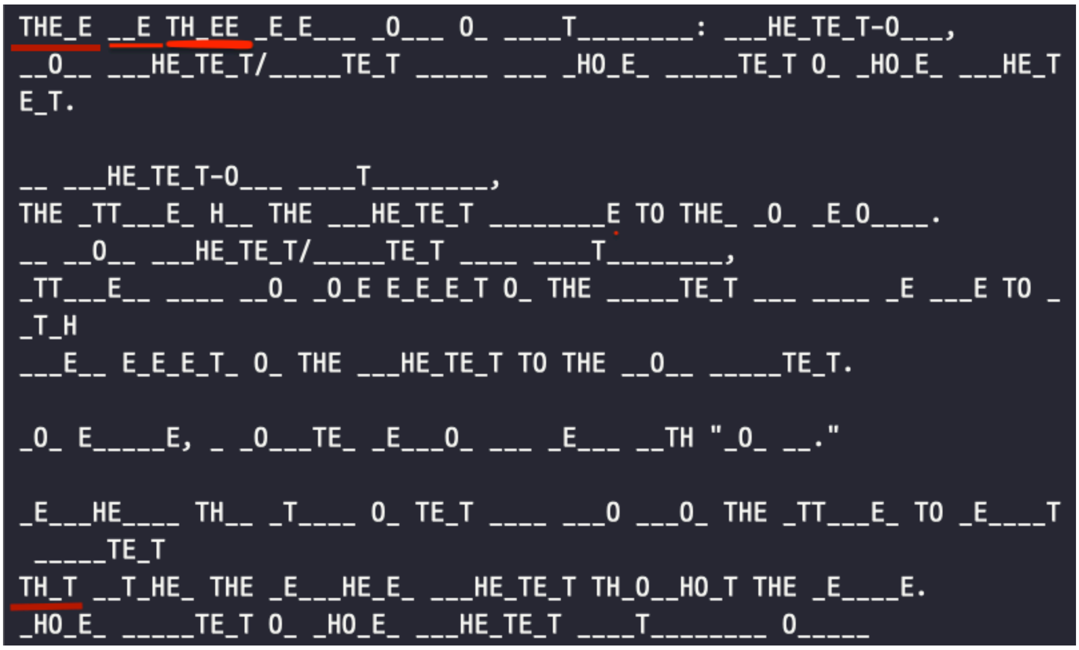


```
"""
MONOGRAM = [('D', 8), ('-', 4), ('H', 4), ('G', 1)]
BIGRAM =  [('KA', 11), ('VU', 10), ('AP', 9), ('UB', 8), ('AW', 6), ('GV', 5),
('GA', 5), ('HP', 4), ('ZQ', 4), ('DA', 3), ('JT', 3), ('UQ', 2), ('CU', 2),
('HN', 2), ('DT', 1), ('DQ', 1), ('GQ', 1), ('QU', 1), ('HQ', 1), ('RF', 1),
('MA', 1), ('JD', 1), ('NA', 1), ('AQ', 1)]
TRIGRAM = [('KST', 15), ('VWP', 11), ('LUO', 10), ('DQC', 7), ('HQM', 7),
('BUY', 4), ('SDQ', 4), ('HWT', 3), ('DYP', 2), ('WUM', 2), ('PAW', 2),
('XHQ', 2), ('GHY', 2), ('MPH', 1), ('BPM', 1), ('EPL', 1), ('SHN', 1),
('UHD', 1), ('VUU', 1), ('MA?', 1), ('FHW', 1), ('QTY', 1), ('QUV', 1)]
"""

# PT frequency order : TKAQVZPGWDHUNSYXOMFLRCIBEJ
# Alphabet frequency order : ETAOINSHRDLCUMWFGYPBVKJXQZ

# 2글자 : of, to, in, it ...
# 3글자 : the, and, for, you ...
# kst --> the 라고 예상한다면
# ka --> to 라고 예상할 수 있음

# 현재 K -> T, S -> H, T -> E, A -> O
# 현재 예상 정보로 글자 바꾸어 보기
```



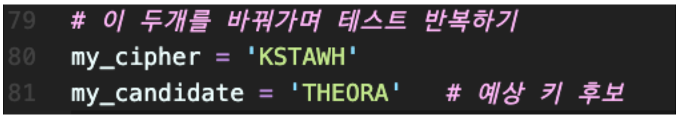
```
my_map = { 'A':'_', 'B':'_', 'C':'_', 'D':'_', 'E':'_', 'F':'_',
        'G':'_', 'H':'_', 'I':'_', 'J':'_', 'K':'_', 'L':'_', 'M':'_',
        'N':'_', 'O':'_', 'P':'_', 'Q':'_', 'R':'_', 'S':'_',
        'T':'_', 'U':'_', 'V':'_', 'W':'_', 'X':'_', 'Y':'_', 'Z':'_'}

# 이 두개를 바꿔가며 테스트 반복하기
my_cipher = 'KSTA'
my_candidate = 'THEO'   # 예상 키 후보

for i in range(len(my_cipher)):
    my_map[my_cipher[i]] = my_candidate[i]

for ch in PT:
    if ch.upper() in SubstLib.Alphabet:
        print(my_map[ch.upper()], end = '')
    else:
        print(ch, end = '')
```

코드 실행 결과 :

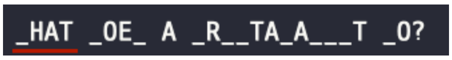


```
THE_E __E TH_EE _E_E___ _O___ O_ ____T________: ___HE_TE_T-O___,
__O__ ___HE_TE_T/_____TE_T _____ ___ _HO_E_ _____TE_T O_ _HO_E_ ___HE_T
E_T.

__ ___HE_TE_T-O___ ____T________,
THE _TT___E_ H__ THE ___HE_TE_T ________E TO THE_ _O_ _E_O____.
__ __O__ ___HE_TE_T/_____TE_T ____ ____T________,
_TT___E__ ____ __O_ _O_E E_E_E_T O_ THE _____TE_T ___ ____ _E ___E TO _
_T_H
___E__ E_E_E_T_ O_ THE ___HE_TE_T TO THE __O__ _____TE_T.

_O_ E_____E, _ _O___TE_ _E___O_ ___ _E___ __TH "_O_ __."

_E___HE____ TH__ _T____ O_ TE_T ____ ___O ___O_ THE _TT___E_ TO _E____T
 _____TE_T
TH_T __T_HE_ THE _E___HE_E_ ___HE_TE_T TH_O__HO_T THE _E____E.
_HO_E_ _____TE_T O_ _HO_E_ ___HE_TE_T ____T________ O_____
```

THERE, ARE, THREE, THAT 으로 유추 (W → R, H → A)

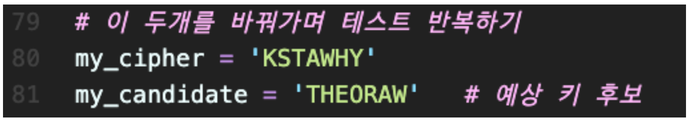


```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher = 'KSTAWH'
my_candidate = 'THEORA'   # 예상 키 후보
```



```
_HAT _OE_ A _R__TA_A___T _O?
```

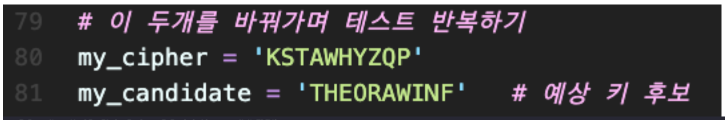
WHAT 으로 유추 (Y → W)



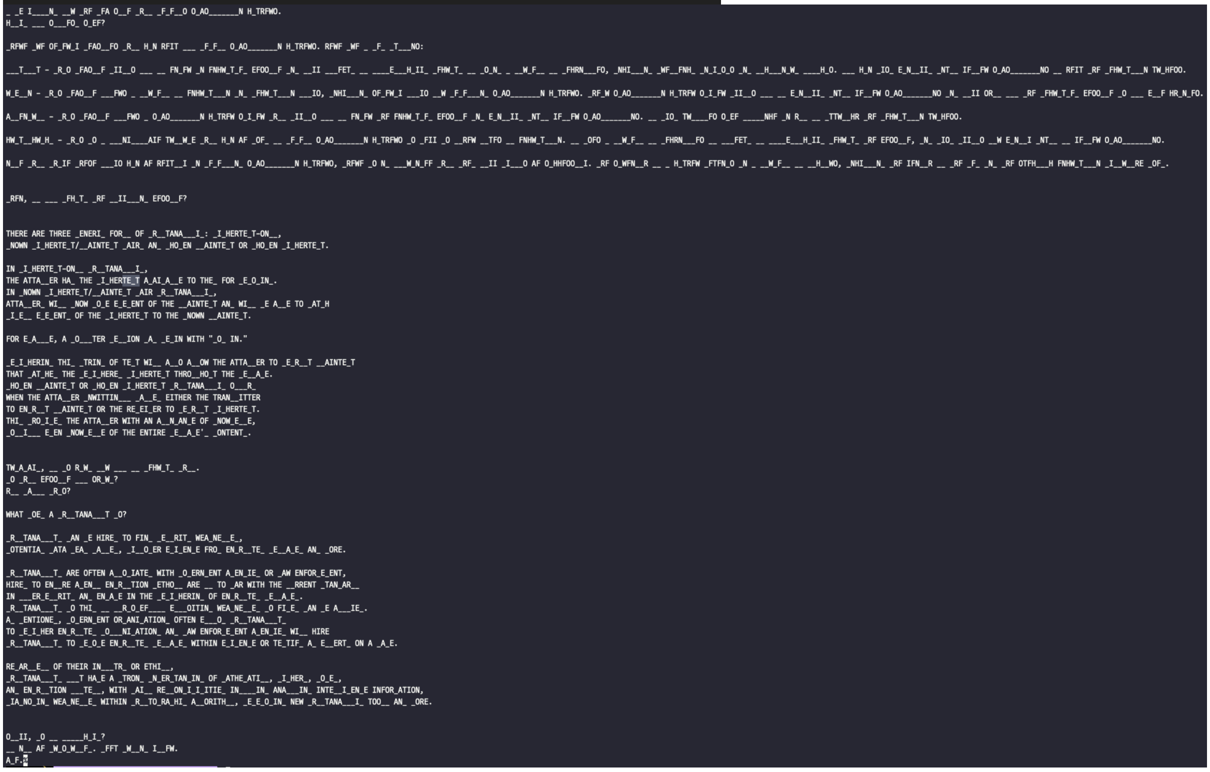
```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher = 'KSTAWHY'
my_candidate = 'THEORAW'   # 예상 키 후보
```

W_TH 라는 단어가 많이 보여서 WITH 로 예측 (Z → I)

I_ 을 IN 으로 예측 + BIGRAM에서 높은 빈도를 차지한 AP 를 OF로 예측 (Q → N, P → F)



```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher = 'KSTAWHYZQP'
my_candidate = 'THEORAWINF'    # 예상 키 후보
```

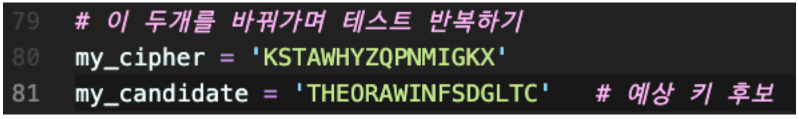


```
_ _E I___N_ __W _RF _FA O__F _R__ _F_F__O O_AO_______N H_TRFWO.
H__I_ ___ O___FO_ O_EF?

_RFWF _WF OF_FW_I _FAO__FO _R__ H_N RFIT ___ _F_F__ O_AO_______N H_TRFWO. RFWF _WF _ _F_ _T___NO:

___T___T - _R_O _FAO__F _II__O ___ __ FN_FW _N FNHW_T_F_ EFOO__F _N_ __II ___FET_ __ ____E___H_II_ _FHW_T_ __ _O_N_ _ __W_F__ __ _FHRN___FO, _NHI___N_ _WF__FNH_ _N_I_O_O _N_ __H___N_W_ ____H_O. ___ H_N _IO_ E_N__II_ _NT__ IF__FW O_AO_______NO __ RFIT _RF _FHW_T___N TW_HFOO.

W_E__N - _R_O _FAO__F ___FWO _ __W_F__ __ FNHW_T___N _N_ _FHW_T___N ___IO, _NHI___N_ OF_FW_I ___IO __W _F_F___N_ O_AO_______N H_TRFWO. _RF_W O_AO_______N H_TRFW O_I_FW _II__O ___ __ E_N__II_ _NT__ IF__FW O_AO_______NO _N_ __II OR__ ___ _RF _FHW_T_F_ EFOO__F _O ___ E__F HR_N_FO.

A__FN_W__ - _R_O _FAO__F ___FWO _ O_AO_______N H_TRFW O_I_FW _R__ _II__O ___ __ FN_FW _RF FNHW_T_F_ EFOO__F _N_ E_N__II_ _NT__ IF__FW O_AO_______NO. __ _IO_ TW____FO O_EF _____NHF _N R__ __ _TTW__HR _RF _FHW_T___N TW_HFOO.

HW_T__HW_H_ - _R_O _O _ ___NI____AIF TW__W_E _R__ H_N AF _OF_ __ _F_F__ O_AO_______N H_TRFWO _O _FII _O __RFW __TFO __ FNHW_T___N. __ _OFO _ __W_F__ __ _FHRN___FO __ ___FET_ __ ____E___H_II_ _FHW_T_ _RF EFOO__F, _N_ _IO_ _II__O __W E_N__I _NT__ __ IF__FW O_AO_______NO.

N__F _R__ _R_IF _RFOF ___IO H_N AF RFIT__I _N _F_F___N_ O_AO_______N H_TRFWO, _RFWF _O N_ ___W_N_FF _R__ _RF_ __II _I___O AF O_HHFOO__I. _RF O_WFN__R __ _ H_TRFW _FTFN_O _N _ __W_F__ __ __H__WO, _NHI___N_ _RF IFN__R __ _RF _F_ _N_ _RF OTFH___H FNHW_T___N _I__W__RE _OF_.


_RFN, __ ___ _FH_T_ _RF __II___N_ EFOO__F?


THERE ARE THREE _ENERI_ FOR__ OF _R__TANA___I_: _I_HERTE_T-ON__,
_NOWN _I_HERTE_T/__AINTE_T _AIR_ AN_ _HO_EN __AINTE_T OR _HO_EN _I_HERTE_T.

IN _I_HERTE_T-ON__ _R__TANA___I_,
THE ATTA__ER HA_ THE _I_HERTE_T A_AI_A__E TO THE_ FOR _E_O_IN_.
IN _NOWN _I_HERTE_T/__AINTE_T _AIR _R__TANA___I_,
ATTA__ER_ WI__ _NOW _O_E E_E_ENT OF THE __AINTE_T AN_ WI__ _E A__E TO _AT_H
_I_E__ E_E_ENT_ OF THE _I_HERTE_T TO THE _NOWN __AINTE_T.

FOR E_A___E, A _O___TER _E__ION _A_ _E_IN WITH "_O_ IN."

_E_I_HERIN_ THI_ _TRIN_ OF TE_T WI__ A__O A__OW THE ATTA__ER TO _E_R__T __AINTE_T
THAT _AT_HE_ THE _E_I_HERE_ _I_HERTE_T THRO__HO_T THE _E__A_E.
_HO_EN __AINTE_T OR _HO_EN _I_HERTE_T _R__TANA___I_ O___R_
WHEN THE ATTA__ER _NWITTIN___ _A__E_ EITHER THE TRAN__ITTER
TO EN_R__T __AINTE_T OR THE RE_EI_ER TO _E_R__T _I_HERTE_T.
THI_ _RO_I_E_ THE ATTA__ER WITH AN A__N_AN_E OF _NOW_E__E,
_O__I___ E_EN _NOW_E__E OF THE ENTIRE _E__A_E'_ _ONTENT_.


TW_A_AI_, __ _O R_W_ __W ___ __ _FHW_T_ _R__.
_O _R__ EFOO__F ___ OR_W_?
R__ _A___ _R_O?

WHAT _OE_ A _R__TANA___T _O?

_R__TANA___T_ _AN _E HIRE_ TO FIN_ _E__RIT_ WEA_NE__E_,
_OTENTIA_ _ATA _EA_ _A__E_, _I__O_ER E_I_EN_E FRO_ EN_R__TE_ _E__A_E_ AN_ _ORE.

_R__TANA___T_ ARE OFTEN A__O_IATE_ WITH _O_ERN_ENT A_EN_IE_ OR _AW ENFOR_E_ENT,
HIRE_ TO EN__RE A_EN__ EN_R__TION _ETHO__ ARE __ TO _AR WITH THE __RRENT _TAN_AR__
IN ___ER_E__RIT_ AN_ EN_A_E IN THE _E_I_HERIN_ OF EN_R__TE_ _E__A_E_.
_R__TANA___T_ _O THI_ __ __R_O_EF____ E___OITIN_ WEA_NE__E_ _O FI_E_ _AN _E A___IE_.
A_ _ENTIONE_, _O_ERN_ENT OR_ANI_ATION_ OFTEN E___O_ _R__TANA___T_
TO _E_I_HER EN_R__TE_ _O___NI_ATION_ AN_ _AW ENFOR_E_ENT A_EN_IE_ WI__ HIRE
_R__TANA___T_ TO _E_O_E EN_R__TE_ _E__A_E_ WITHIN E_I_EN_E OR TE_TIF_ A_ E__ERT_ ON A _A_E.

RE_AR__E__ OF THEIR IN___TR_ OR ETHI__,
_R__TANA___T_ ___T HA_E A _TRON_ _N_ER_TAN_IN_ OF _ATHE_ATI__, _I_HER_, _O_E_,
AN_ EN_R__TION ___TE__, WITH _AI__ RE__ON_I_I_ITIE_ IN____IN_ ANA___IN_ INTE__I_EN_E INFOR_ATION,
_IA_NO_IN_ WEA_NE__E_ WITHIN _R__TO_RA_HI_ A__ORITH__, _E_E_O_IN_ NEW _R__TANA___I_ TOO__ AN_ _ORE.


O__II, _O __ _____H_I_?
__ N__ AF _W_O_W__F_. _FFT _W__N_ I__FW.
A_F.%
```

몇몇의 단어들은 완성됨

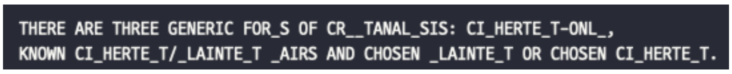
THI_ 를 THIS 로, TRIGRAM에서 HQM은 AN_ 이므로 AND로 예상 (N → S, M → D)

RE_ARD_ESS OF → regard less of, yzgg → WI__ → will, 많이 반복되는 ATTA__ERS → ATTACKERS 로 예측 (I → G, G → L, X → C, V → K)



```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher = 'KSTAWHYZQPNMIGKX'
my_candidate = 'THEORAWINFSDGLTC'    # 예상 키 후보
```

_ESSAGE 의 반복 → MESSAGE (U → M)

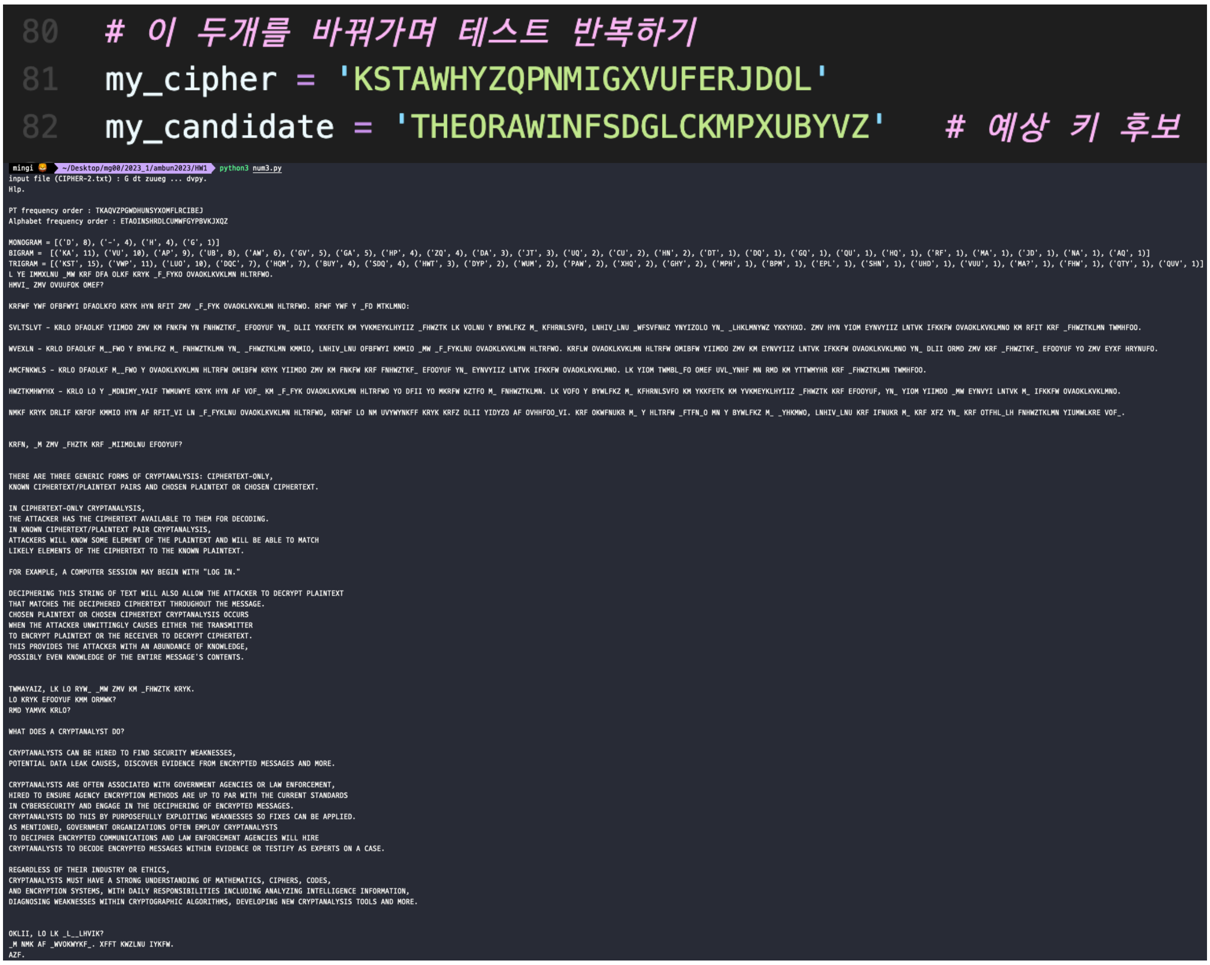


```
THERE ARE THREE GENERIC FOR_S OF CR__TANAL_SIS: CI_HERTE_T-ONL_,
KNOWN CI_HERTE_T/_LAINTE_T _AIRS AND CHOSEN _LAINTE_T OR CHOSEN CI_HERTE_T.
```

반복적인 단어 연속 출현 & 문맥상 → CIPHERTEXT, PLAINTEXT (F → P, E → X)

CIPHERTEXT THRO_GHO_T THE MESSAGE → throughout (R → U)
WILL _E A_LE TO → will be able to (J → B)
DECR_PT PLAINTEXT → DECRYPT (D → Y)
DISCO_ER E_IDENCE FROM ENCR_PTED MESSAGES AND MORE. → DISCOVER EVIDENCE (O → V)
문맥상 암호에 대한 이야기로 생각되어 치환함

최종 결과 :

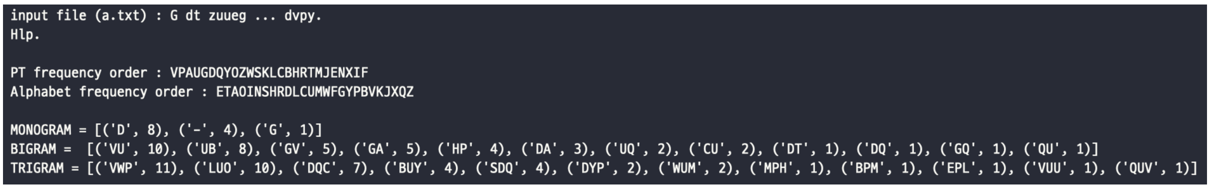


```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher = 'KSTAWHYZQPNMIGXVUFERJDOL'
my_candidate = 'THEORAWINFSDGLCKMPXUBYVZ'    # 예상 키 후보
```

```
mingi 🦁 ~/Desktop/mg00/2023_1/ambun2023/HW1 python3 num3.py
input file (CIPHER-2.txt) : G dt zuueg ... dvpy.
Hlp.

PT frequency order : TKAQVZPGWDHUNSYXOMFLRCIBEJ
Alphabet frequency order : ETAOINSHRDLCUMWFGYPBVKJXQZ

MONOGRAM = [('D', 8), ('-', 4), ('H', 4), ('G', 1)]
BIGRAM =  [('KA', 11), ('VU', 10), ('AP', 9), ('UB', 8), ('AW', 6), ('GV', 5), ('GA', 5), ('HP', 4), ('ZQ', 4), ('DA', 3), ('JT', 3), ('UQ', 2), ('CU', 2), ('HN', 2), ('DT', 1), ('DQ', 1), ('GQ', 1), ('QU', 1), ('HQ', 1), ('RF', 1), ('MA', 1), ('JD', 1), ('NA', 1), ('AQ', 1)]
TRIGRAM = [('KST', 15), ('VWP', 11), ('LUO', 10), ('DQC', 7), ('HQM', 7), ('BUY', 4), ('SDQ', 4), ('HWT', 3), ('DYP', 2), ('WUM', 2), ('PAW', 2), ('XHQ', 2), ('GHY', 2), ('MPH', 1), ('BPM', 1), ('EPL', 1), ('SHN', 1), ('UHD', 1), ('VUU', 1), ('MA?', 1), ('FHW', 1), ('QTY', 1), ('QUV', 1)]
L YE IMMXLNU _MW KRF DFA OLKF KRYK _F_FYKO OVAOKLKVKLMN HLTRFWO.
HMVI_ ZMV OVUUFOK OMEF?

KRFWF YWF OFBFWYI DFAOLKFO KRYK HYN RFIT ZMV _F_FYK OVAOKLKVKLMN HLTRFWO. RFWF YWF Y _FD MTKLMNO:

SVLTSLVT - KRLO DFAOLKF YIIMDO ZMV KM FNKFW YN FNHWZTKF_ EFOOYUF YN_ DLII YKKFETK KM YVKMEYKLHYIIZ _FHWZTK LK VOLNU Y BYWLFKZ M_ KFHRNLSVFO, LNHIV_LNU _WFSVFNHZ YNYIZOLO YN_ _LHKLMNYWZ YKKYHXO. ZMV HYN YIOM EYNVYIIZ LNTVK IFKKFW OVAOKLKVKLMNO KM RFIT KRF _FHWZTKLMN TWMHFOO.

WVEXLN - KRLO DFAOLKF M__FWO Y BYWLFKZ M_ FNHWZTKLMN YN_ _FHWZTKLMN KMMIO, LNHIV_LNU OFBFWYI KMMIO _MW _F_FYKLNU OVAOKLKVKLMN HLTRFWO. KRFLW OVAOKLKVKLMN HLTRFW OMIBFW YIIMDO ZMV KM EYNVYIIZ LNTVK IFKKFW OVAOKLKVKLMNO YN_ DLII ORMD ZMV KRF _FHWZTKF_ EFOOYUF YO ZMV EYXF HRYNUFO.

AMCFNKWLS - KRLO DFAOLKF M__FWO Y OVAOKLKVKLMN HLTRFW OMIBFW KRYK YIIMDO ZMV KM FNKFW KRF FNHWZTKF_ EFOOYUF YN_ EYNVYIIZ LNTVK IFKKFW OVAOKLKVKLMNO. LK YIOM TWMBL_FO OMEF UVL_YNHF MN RMD KM YTTWMYHR KRF _FHWZTKLMN TWMHFOO.

HWZTKMHWYHX - KRLO LO Y _MDNIMY_YAIF TWMUWYE KRYK HYN AF VOF_ KM _F_FYK OVAOKLKVKLMN HLTRFWO YO DFII YO MKRFW KZTFO M_ FNHWZTKLMN. LK VOFO Y BYWLFKZ M_ KFHRNLSVFO KM YKKFETK KM YVKMEYKLHYIIZ _FHWZTK KRF EFOOYUF, YN_ YIOM YIIMDO _MW EYNVYI LNTVK M_ IFKKFW OVAOKLKVKLMNO.

NMKF KRYK DRLIF KRFOF KMMIO HYN AF RFIT_VI LN _F_FYKLNU OVAOKLKVKLMN HLTRFWO, KRFWF LO NM UVYWYNKFF KRYK KRFZ DLII YIDYZO AF OVHHFOO_VI. KRF OKWFNUKR M_ Y HLTRFW _FTFN_O MN Y BYWLFKZ M_ _YHKMWO, LNHIV_LNU KRF IFNUKR M_ KRF XFZ YN_ KRF OTFHL_LH FNHWZTKLMN YIUMWLKRE VOF_.


KRFN, _M ZMV _FHZTK KRF _MIIMDLNU EFOOYUF?


THERE ARE THREE GENERIC FORMS OF CRYPTANALYSIS: CIPHERTEXT-ONLY,
KNOWN CIPHERTEXT/PLAINTEXT PAIRS AND CHOSEN PLAINTEXT OR CHOSEN CIPHERTEXT.

IN CIPHERTEXT-ONLY CRYPTANALYSIS,
THE ATTACKER HAS THE CIPHERTEXT AVAILABLE TO THEM FOR DECODING.
IN KNOWN CIPHERTEXT/PLAINTEXT PAIR CRYPTANALYSIS,
ATTACKERS WILL KNOW SOME ELEMENT OF THE PLAINTEXT AND WILL BE ABLE TO MATCH
LIKELY ELEMENTS OF THE CIPHERTEXT TO THE KNOWN PLAINTEXT.

FOR EXAMPLE, A COMPUTER SESSION MAY BEGIN WITH "LOG IN."

DECIPHERING THIS STRING OF TEXT WILL ALSO ALLOW THE ATTACKER TO DECRYPT PLAINTEXT
THAT MATCHES THE DECIPHERED CIPHERTEXT THROUGHOUT THE MESSAGE.
CHOSEN PLAINTEXT OR CHOSEN CIPHERTEXT CRYPTANALYSIS OCCURS
WHEN THE ATTACKER UNWITTINGLY CAUSES EITHER THE TRANSMITTER
TO ENCRYPT PLAINTEXT OR THE RECEIVER TO DECRYPT CIPHERTEXT.
THIS PROVIDES THE ATTACKER WITH AN ABUNDANCE OF KNOWLEDGE,
POSSIBLY EVEN KNOWLEDGE OF THE ENTIRE MESSAGE'S CONTENTS.


TWMAYAIZ, LK LO RYW_ _MW ZMV KM _FHWZTK KRYK.
LO KRYK EFOOYUF KMM ORMWK?
RMD YAMVK KRLO?

WHAT DOES A CRYPTANALYST DO?

CRYPTANALYSTS CAN BE HIRED TO FIND SECURITY WEAKNESSES,
POTENTIAL DATA LEAK CAUSES, DISCOVER EVIDENCE FROM ENCRYPTED MESSAGES AND MORE.

CRYPTANALYSTS ARE OFTEN ASSOCIATED WITH GOVERNMENT AGENCIES OR LAW ENFORCEMENT,
HIRED TO ENSURE AGENCY ENCRYPTION METHODS ARE UP TO PAR WITH THE CURRENT STANDARDS
IN CYBERSECURITY AND ENGAGE IN THE DECIPHERING OF ENCRYPTED MESSAGES.
CRYPTANALYSTS DO THIS BY PURPOSEFULLY EXPLOITING WEAKNESSES SO FIXES CAN BE APPLIED.
AS MENTIONED, GOVERNMENT ORGANIZATIONS OFTEN EMPLOY CRYPTANALYSTS
TO DECIPHER ENCRYPTED COMMUNICATIONS AND LAW ENFORCEMENT AGENCIES WILL HIRE
CRYPTANALYSTS TO DECODE ENCRYPTED MESSAGES WITHIN EVIDENCE OR TESTIFY AS EXPERTS ON A CASE.

REGARDLESS OF THEIR INDUSTRY OR ETHICS,
CRYPTANALYSTS MUST HAVE A STRONG UNDERSTANDING OF MATHEMATICS, CIPHERS, CODES,
AND ENCRYPTION SYSTEMS, WITH DAILY RESPONSIBILITIES INCLUDING ANALYZING INTELLIGENCE INFORMATION,
DIAGNOSING WEAKNESSES WITHIN CRYPTOGRAPHIC ALGORITHMS, DEVELOPING NEW CRYPTANALYSIS TOOLS AND MORE.


OKLII, LO LK _L__LHVIK?
_M NMK AF _WVOKWYKF_. XFFT KWZLNU IYKFW.
AZF.
```

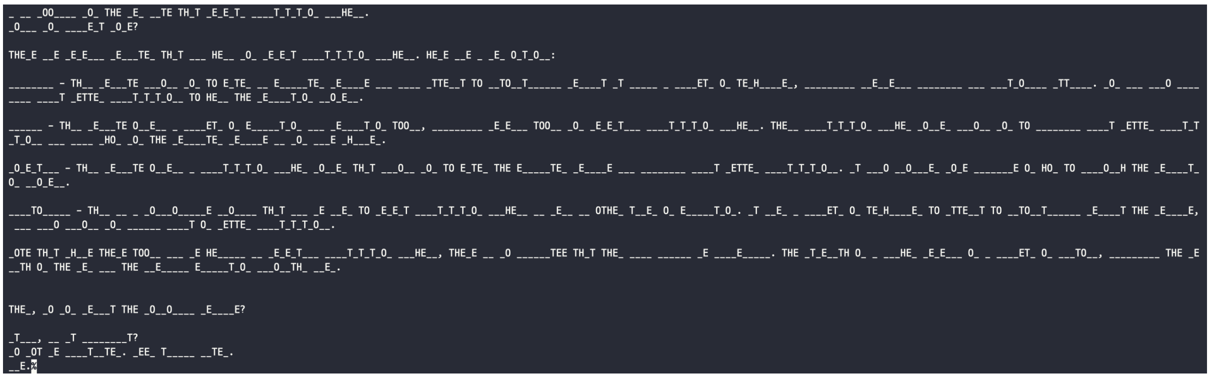
my_map을 출력해서 치환되지 않은 알파벳을 확인함.

결과를 보아 B, C 는 해독되지 않았지만, 중요 내용 앞/뒤는 해독이 안되어 그 부분만 다시 해독.



```
input file (a.txt) : G dt zuueg ... dvpy.
Hlp.

PT frequency order : VPAUGDQYOZWSKLCBHRTMJENXIF
Alphabet frequency order : ETAOINSHRDLCUMWFGYPBVKJXQZ

MONOGRAM = [('D', 8), ('-', 4), ('G', 1)]
BIGRAM =  [('VU', 10), ('UB', 8), ('GV', 5), ('GA', 5), ('HP', 4), ('DA', 3), ('UQ', 2), ('CU', 2), ('DT', 1), ('DQ', 1), ('GQ', 1), ('QU', 1)]
TRIGRAM = [('VWP', 11), ('LUO', 10), ('DQC', 7), ('BUY', 4), ('SDQ', 4), ('DYP', 2), ('WUM', 2), ('MPH', 1), ('BPM', 1), ('EPL', 1), ('VUU', 1), ('QUV', 1)]
```

VU, VWP 를 보고 겹치는 V를 T로 유추하면 THE, TO로 방향을 잡고 해독



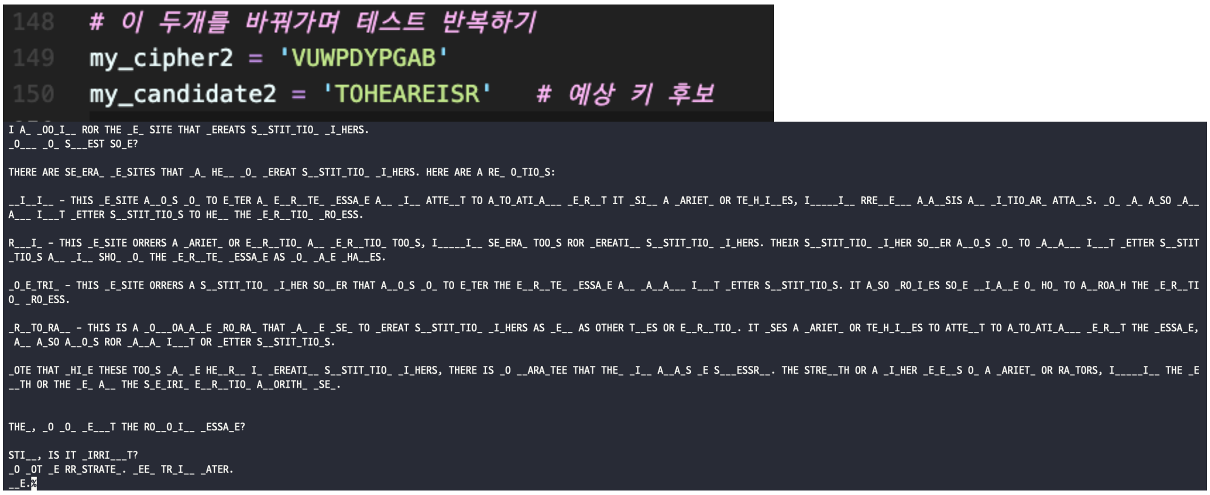
```
_ __ _OO____ _O_ THE _E_ __TE TH_T _E_E_T_ ____T_T_T_O_ ___HE__.
_O___ _O_ ____E_T _O_E?

THE_E __E _E_E___ _E___TE_ TH_T ___ HE__ _O_ _E_E_T ____T_T_T_O_ ___HE__. HE_E __E _ _E_ O_T_O__:

________ - TH__ _E___TE ___O__ _O_ TO E_TE_ __ E_____TE_ _E____E ___ ____ _TTE__T TO __TO__T______ _E____T _T _____ _ ____ET_ O_ TE_H____E_, _________ __E__E___ ________ ___ ___T_O____ _TT____. _O_ ___ ___O ____
____ ____T _ETTE_ ____T_T_T_O__ TO HE__ THE _E____T_O_ __O_E__.

______ - TH__ _E___TE O__E__ _ ____ET_ O_ E_____T_O_ ___ _E____T_O_ TOO__, _________ _E_E___ TOO__ _O_ _E_E_T___ ____T_T_T_O_ ___HE__. THE__ ____T_T_T_O_ ___HE_ _O__E_ ___O__ _O_ TO ________ ____T _ETTE_ ____T_T
_T_O__ ___ ____ _HO_ _O_ THE _E____TE_ _E____E __ _O_ ___E _H___E_.

_O_E_T___ - TH__ _E___TE O__E__ _ ____T_T_T_O_ ___HE_ _O__E_ TH_T ___O__ _O_ TO E_TE_ THE E_____TE_ _E____E ___ ________ ____T _ETTE_ ____T_T_T_O__. _T ___O __O___E_ _O_E _______E O_ HO_ TO ____O__H THE _E____T_
O_ __O_E__.

____TO_____ - TH__ __ _ _O___O_____E __O____ TH_T ___ _E __E_ TO _E_E_T ____T_T_T_O_ ___HE__ __ _E__ __ OTHE_ T__E_ O_ E_____T_O_. _T __E_ _ ____ET_ O_ TE_H____E_ TO _TTE__T TO __TO__T______ _E____T THE _E____E,
 ___ ___O ___O__ _O_ ______ ____T O_ _ETTE_ ____T_T_T_O__.

_OTE TH_T _H__E THE_E TOO__ ___ _E HE_____ __ _E_E_T___ ____T_T_T_O_ ___HE__, THE_E __ _O ______TEE TH_T THE_ ____ ______ _E ____E_____. THE _T_E__TH O_ _ ___HE_ _E_E___ O_ _ ____ET_ O_ ___TO__, _________ THE _E
__TH O_ THE _E_ ___ THE __E_____ E_____T_O_ ___O__TH_ __E_.


THE_, _O _O_ _E___T THE _O__O____ _E____E?

_T___, __ _T ________T?
_O _OT _E ____T__TE_. _EE_ T_____ __TE_.
__E.%
```

THERE 로 생각해서 해독해보기 → (Y → R), There are → (DYP → ARE)

MONOGRAM에서 많이 나오는 D는 A로 판명났고, 첫 글자로 나오는 한 글자를 I로 예상함 (G → I)

THI_ 라는 단어가 굉장히 많이보임 → (A → S)

많이 보이는 UB 를 OR로 예측 (B → R)



```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher2 = 'VUWPDYPGAB'
my_candidate2 = 'TOHEAREISR'    # 예상 키 후보
```

```
I A_ _OO_I__ ROR THE _E_ SITE THAT _EREATS S__STIT_TIO_ _I_HERS.
_O___ _O_ S___EST SO_E?

THERE ARE SE_ERA_ _E_SITES THAT _A_ HE__ _O_ _EREAT S__STIT_TIO_ _I_HERS. HERE ARE A RE_ O_TIO_S:

__I__I__ - THIS _E_SITE A__O_S _O_ TO E_TER A_ E__R__TE_ _ESSA_E A__ _I__ ATTE__T TO A_TO_ATI_A___ _E_R__T IT _SI__ A _ARIET_ OR TE_H_I__ES, I_____I__ RRE__E___ A_A__SIS A__ _I_TIO_AR_ ATTA__S. _O_ _A_ A_SO _A__
A___ I___T _ETTER S__STIT_TIO_S TO HE__ THE _E_R__TIO_ _RO_ESS.

R___I_ - THIS _E_SITE ORRERS A _ARIET_ OR E__R__TIO_ A__ _E_R__TIO_ TOO_S, I_____I__ SE_ERA_ TOO_S ROR _EREATI__ S__STIT_TIO_ _I_HERS. THEIR S__STIT_TIO_ _I_HER SO__ER A__O_S _O_ TO _A__A___ I___T _ETTER S__STIT
_TIO_S A__ _I__ SHO_ _O_ THE _E_R__TE_ _ESSA_E AS _O_ _A_E _HA__ES.

_O_E_TRI_ - THIS _E_SITE ORRERS A S__STIT_TIO_ _I_HER SO__ER THAT A__O_S _O_ TO E_TER THE E__R__TE_ _ESSA_E A__ _A__A___ I___T _ETTER S__STIT_TIO_S. IT A_SO _RO_I_ES SO_E __I_A__E O_ HO_ TO A__ROA_H THE _E_R__TI
O_ _RO_ESS.

_R__TO_RA__ - THIS IS A _O___OA_A__E _RO_RA_ THAT _A_ _E _SE_ TO _EREAT S__STIT_TIO_ _I_HERS AS _E__ AS OTHER T__ES OR E__R__TIO_. IT _SES A _ARIET_ OR TE_H_I__ES TO ATTE__T TO A_TO_ATI_A___ _E_R__T THE _ESSA_E,
 A__ A_SO A__O_S ROR _A__A_ I___T OR _ETTER S__STIT_TIO_S.

_OTE THAT _HI_E THESE TOO_S _A_ _E HE__R__ I_ _EREATI__ S__STIT_TIO_ _I_HERS, THERE IS _O __ARA_TEE THAT THE_ _I__ A__A_S _E S___ESSR__. THE STRE__TH OR A _I_HER _E_E__S O_ A _ARIET_ OR RA_TORS, I_____I__ THE _E
__TH OR THE _E_ A__ THE S_E_IRI_ E__R__TIO_ A__ORITH_ _SE_.


THE_, _O _O_ _E___T THE RO__O_I__ _ESSA_E?

STI__, IS IT _IRRI___T?
_O _OT _E RR_STRATE_. _EE_ TR_I__ _ATER.
__E.%
```

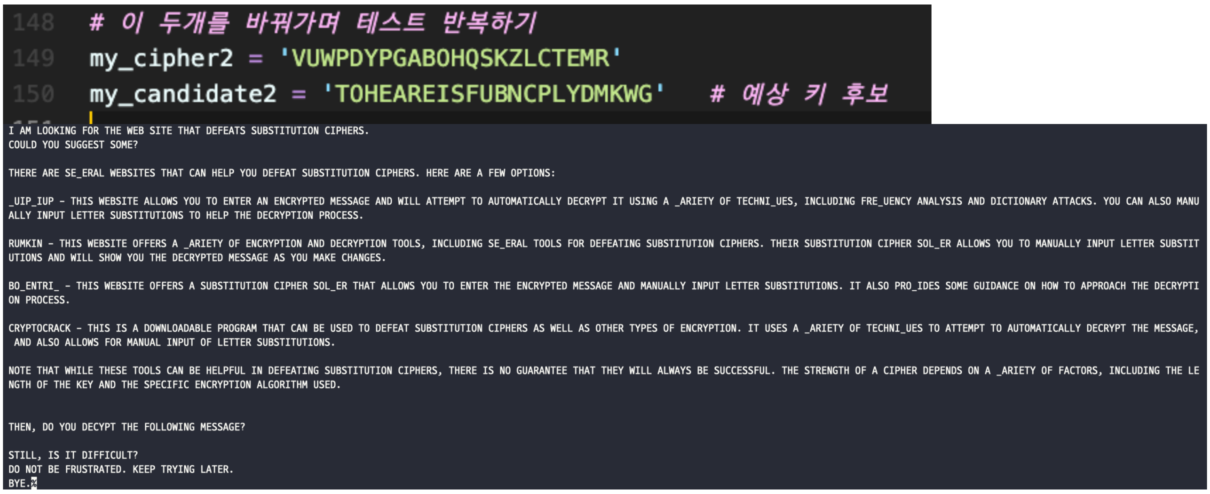
ROR 등 단어가 아닌 것들이 속출됨.

UB를 OR이 아닌 OF로 예측 (B → F)

IT _SES A → It uses a,
OFFERS A S__STIT_TIO_ _I_HER → offers a substitution cipher (ubbpya d aohavgvovguq sgkwpy)
(O → U, H → B, Q → N, S → C, K → P)

THAT CAN HE_P _OU _EFEAT SUBSTITUTION CIPHERS. → help you defeat (wpzk luo cpbpdv)
(Z → L, L → Y, C → D)

I A_ LOO_IN_ FOR THE _EB SITE → I am looking for the web site (G dt zuuegqr buy vwp mph agvp)
(T → M, E → K, M → W)
COULD YOU SU__EST SO_E? → Could you suggest some? (Suozc luo aorrpav autp?)
(R → G)

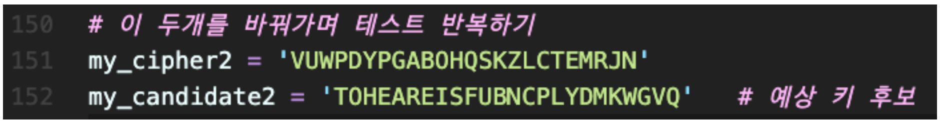


```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher2 = 'VUWPDYPGABOHQSKZLCTEMR'
my_candidate2 = 'TOHEAREISFUBNCPLYDMKWG'    # 예상 키 후보
```

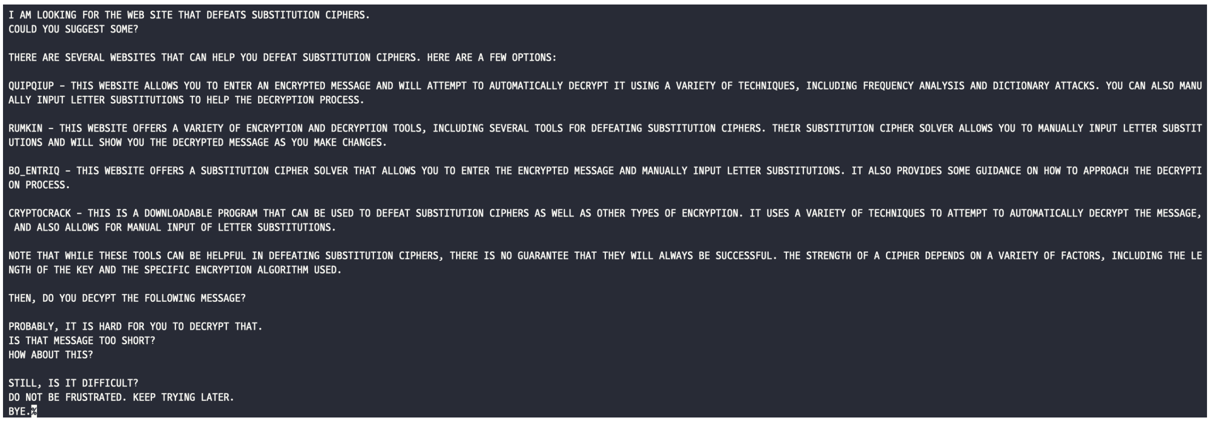
```
I AM LOOKING FOR THE WEB SITE THAT DEFEATS SUBSTITUTION CIPHERS.
COULD YOU SUGGEST SOME?

THERE ARE SE_ERAL WEBSITES THAT CAN HELP YOU DEFEAT SUBSTITUTION CIPHERS. HERE ARE A FEW OPTIONS:

_UIP_IUP - THIS WEBSITE ALLOWS YOU TO ENTER AN ENCRYPTED MESSAGE AND WILL ATTEMPT TO AUTOMATICALLY DECRYPT IT USING A _ARIETY OF TECHNI_UES, INCLUDING FRE_UENCY ANALYSIS AND DICTIONARY ATTACKS. YOU CAN ALSO MANU
ALLY INPUT LETTER SUBSTITUTIONS TO HELP THE DECRYPTION PROCESS.

RUMKIN - THIS WEBSITE OFFERS A _ARIETY OF ENCRYPTION AND DECRYPTION TOOLS, INCLUDING SE_ERAL TOOLS FOR DEFEATING SUBSTITUTION CIPHERS. THEIR SUBSTITUTION CIPHER SOL_ER ALLOWS YOU TO MANUALLY INPUT LETTER SUBSTIT
UTIONS AND WILL SHOW YOU THE DECRYPTED MESSAGE AS YOU MAKE CHANGES.

BO_ENTRI_ - THIS WEBSITE OFFERS A SUBSTITUTION CIPHER SOL_ER THAT ALLOWS YOU TO ENTER THE ENCRYPTED MESSAGE AND MANUALLY INPUT LETTER SUBSTITUTIONS. IT ALSO PRO_IDES SOME GUIDANCE ON HOW TO APPROACH THE DECRYPTI
ON PROCESS.

CRYPTOCRACK - THIS IS A DOWNLOADABLE PROGRAM THAT CAN BE USED TO DEFEAT SUBSTITUTION CIPHERS AS WELL AS OTHER TYPES OF ENCRYPTION. IT USES A _ARIETY OF TECHNI_UES TO ATTEMPT TO AUTOMATICALLY DECRYPT THE MESSAGE,
 AND ALSO ALLOWS FOR MANUAL INPUT OF LETTER SUBSTITUTIONS.

NOTE THAT WHILE THESE TOOLS CAN BE HELPFUL IN DEFEATING SUBSTITUTION CIPHERS, THERE IS NO GUARANTEE THAT THEY WILL ALWAYS BE SUCCESSFUL. THE STRENGTH OF A CIPHER DEPENDS ON A _ARIETY OF FACTORS, INCLUDING THE LE
NGTH OF THE KEY AND THE SPECIFIC ENCRYPTION ALGORITHM USED.


THEN, DO YOU DECYPT THE FOLLOWING MESSAGE?

STILL, IS IT DIFFICULT?
DO NOT BE FRUSTRATED. KEEP TRYING LATER.
BYE.%
```

_ariety → variety (jdygpvl) , TECHNI_UES → techniques (vpswqgnopa)
(J → V, N → Q)

최종 키 :



```
# 이 두개를 바꿔가며 테스트 반복하기
my_cipher2 = 'VUWPDYPGABOHQSKZLCTEMRJN'
my_candidate2 = 'TOHEAREISFUBNCPLYDMKWGVQ'   # 예상 키 후보
```



```
I AM LOOKING FOR THE WEB SITE THAT DEFEATS SUBSTITUTION CIPHERS.
COULD YOU SUGGEST SOME?

THERE ARE SEVERAL WEBSITES THAT CAN HELP YOU DEFEAT SUBSTITUTION CIPHERS. HERE ARE A FEW OPTIONS:

QUIPQIUP - THIS WEBSITE ALLOWS YOU TO ENTER AN ENCRYPTED MESSAGE AND WILL ATTEMPT TO AUTOMATICALLY DECRYPT IT USING A VARIETY OF TECHNIQUES, INCLUDING FREQUENCY ANALYSIS AND DICTIONARY ATTACKS. YOU CAN ALSO MANU
ALLY INPUT LETTER SUBSTITUTIONS TO HELP THE DECRYPTION PROCESS.

RUMKIN - THIS WEBSITE OFFERS A VARIETY OF ENCRYPTION AND DECRYPTION TOOLS, INCLUDING SEVERAL TOOLS FOR DEFEATING SUBSTITUTION CIPHERS. THEIR SUBSTITUTION CIPHER SOLVER ALLOWS YOU TO MANUALLY INPUT LETTER SUBSTIT
UTIONS AND WILL SHOW YOU THE DECRYPTED MESSAGE AS YOU MAKE CHANGES.

BO_ENTRIQ - THIS WEBSITE OFFERS A SUBSTITUTION CIPHER SOLVER THAT ALLOWS YOU TO ENTER THE ENCRYPTED MESSAGE AND MANUALLY INPUT LETTER SUBSTITUTIONS. IT ALSO PROVIDES SOME GUIDANCE ON HOW TO APPROACH THE DECRYPTI
ON PROCESS.

CRYPTOCRACK - THIS IS A DOWNLOADABLE PROGRAM THAT CAN BE USED TO DEFEAT SUBSTITUTION CIPHERS AS WELL AS OTHER TYPES OF ENCRYPTION. IT USES A VARIETY OF TECHNIQUES TO ATTEMPT TO AUTOMATICALLY DECRYPT THE MESSAGE,
 AND ALSO ALLOWS FOR MANUAL INPUT OF LETTER SUBSTITUTIONS.

NOTE THAT WHILE THESE TOOLS CAN BE HELPFUL IN DEFEATING SUBSTITUTION CIPHERS, THERE IS NO GUARANTEE THAT THEY WILL ALWAYS BE SUCCESSFUL. THE STRENGTH OF A CIPHER DEPENDS ON A VARIETY OF FACTORS, INCLUDING THE LE
NGTH OF THE KEY AND THE SPECIFIC ENCRYPTION ALGORITHM USED.

THEN, DO YOU DECYPT THE FOLLOWING MESSAGE?

PROBABLY, IT IS HARD FOR YOU TO DECRYPT THAT.
IS THAT MESSAGE TOO SHORT?
HOW ABOUT THIS?

STILL, IS IT DIFFICULT?
DO NOT BE FRUSTRATED. KEEP TRYING LATER.
BYE.%
```

해독방법 요약:

1) 알파벳 빈도분석 진행
2) 2글자, 3글자 단어 빈도분석 진행
3) 1, 2를 활용하여 하나씩 바꿔가며 분석 + 사전에 있는 단어 유추
4) 해독된 내용을 보며 문맥상 유추