LAPORAN TUGAS 1

IF4020 KRIPTOGRAFI

DISUSUN OLEH

13520023 Ahmad Alfani Handoyo

13520066 Putri Nurhaliza

TEKNIK INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

SEMESTER II 2022/2023

DAFTAR ISI

Bagian A

1. General Function

a. Program Utama

Website dibangun menggunakan bahasa pemrograman Python dengan *framework* Flask. Program utama adalah file ***app.py*** yang mengatur *logic* utama website, mencakup *route*, tampilan yang di-*render*, dan pemanfaatan fungsi algoritma *cipher*.

b. Modul Helper

Algoritma *cipher* di bawah ini dibantu dengan dua modul helper, yaitu ***stringparser.py*** dan ***matrixoperation.py***. *String parser* mencakup fungsi-fungsi yang berguna untuk melakukan *parsing* terhadap teks *alphabet*, ASCII, maupun *number*. *Matrix operation* mencakup fungsi-fungsi operasi pada matriks, seperti mendapatkan determinan dan invers.

2. Vigenere Cipher

a. *Source code program*

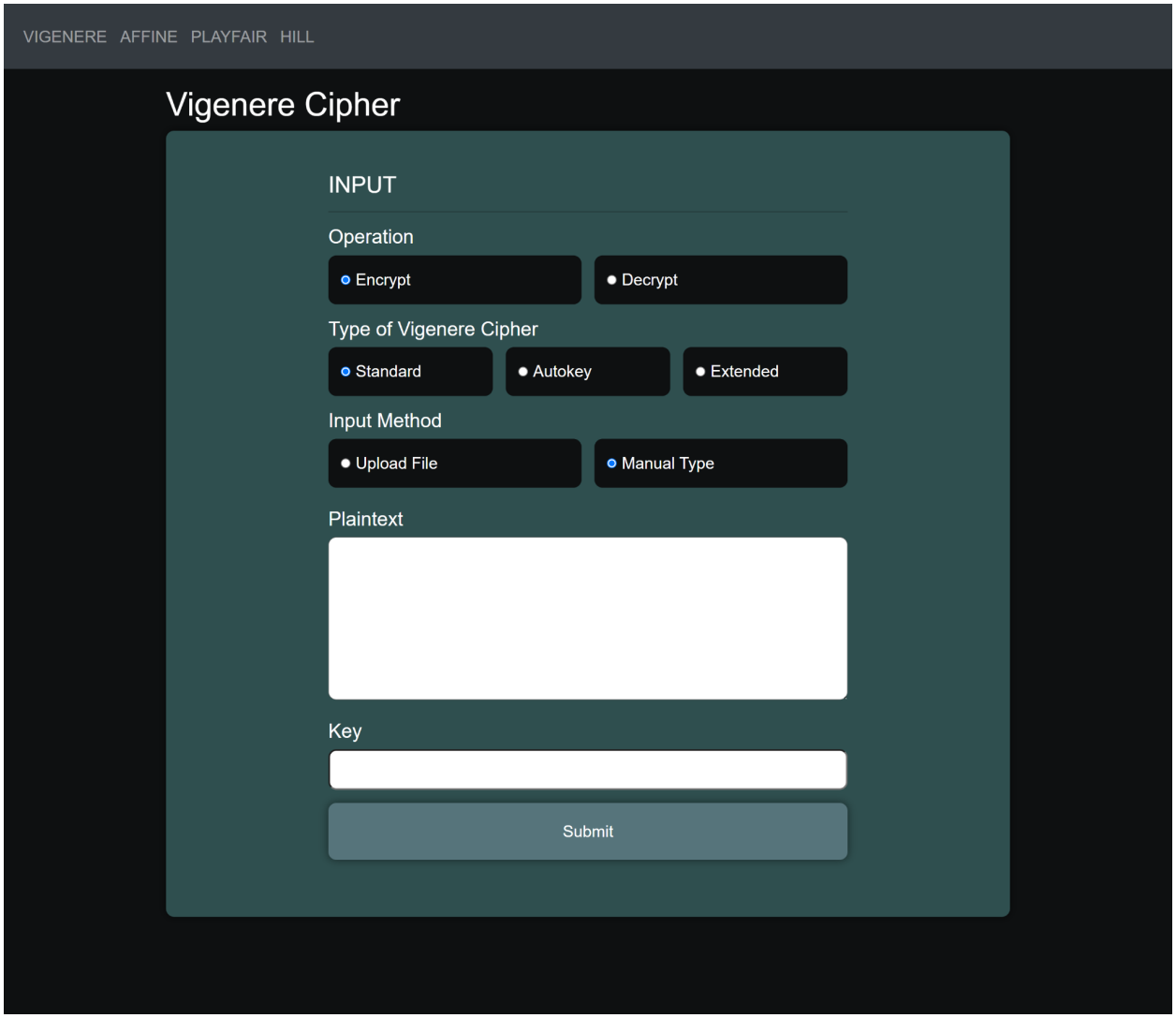
Program Vigenere cipher terdiri atas fungsi utama ***cipher*** yang menerima pesan berupa plainteks maupun cipher teks, *key* bertipe string, operation berupa *encrypt* atau *decrypt*, serta *type* untuk menentukan jenis vigenere *cipher* (standard, autokey, atau extended). Program ini dibantu dengan fungsi ***parseKey*** untuk membuat *key* sepanjang teks. Untuk type standard dan extended, *key* dikali hingga mencapai panjang pesan. Untuk type autokey, bagian awal pesan disisipkan ke akhir *key* hingga panjang *key* mencapai panjang pesan.

```
from . import stringparser as sp

STANDARD = 'standard'
AUTOKEY = 'autokey'
EXTENDED = 'extended'

ENCRYPT = 'encrypt'
DECRYPT = 'decrypt'

def parseKey(text: str, key: str, operation=ENCRYPT, type=STANDARD) ->
str:
    """Parse key to be the same length as text."""
    if type == STANDARD or type == EXTENDED:
```

```
        if len(key) < len(text):
            key = (key * (len(text) // len(key) + 1))[:len(text)]
    elif type == AUTOKEY:
        if operation == ENCRYPT:
            key = key + text[:len(text) - len(key)]
        elif operation == DECRYPT:
            textKey = text[:len(text) - len(key)]
            textKeyNum = sp.alphabetToNumber(textKey)
            for i in range(len(textKey)):
                key += sp.numberToAlphabet([(textKeyNum[i] -
sp.alphabetToNumber(key[i])[0]) % 26])
    return key

def cipher(text, key: str, operation=ENCRYPT, type=STANDARD) -> dict:
    """Encrypt/decrypt plaintext using Vigenere cipher with key.

    Returns a dictionary with the type of operation (encyrpt or
decrypt), type of vigenere cipher (standard, autokey, or extended), key,
original text, and resulting text."""

    result = ''
    if type == STANDARD or type == AUTOKEY:
        text = sp.stringToAlphabet(text)
        key = parseKey(text, sp.stringToAlphabet(key), operation, type)

        textNum = sp.alphabetToNumber(sp.stringToAlphabet(text))
        keyNum = sp.alphabetToNumber(sp.stringToAlphabet(key))
        if operation == ENCRYPT:
            result = sp.numberToAlphabet([(textNum[i] + keyNum[i]) % 26
for i in range(len(textNum))])
        elif operation == DECRYPT:
            result = (sp.numberToAlphabet([(textNum[i] - keyNum[i]) % 26
for i in range(len(textNum))])).lower()
    elif type == EXTENDED:
        key = parseKey(text, key, operation, type)

        textASCII = text
        keyASCII = sp.stringToASCII(key)
        if operation == ENCRYPT:
```

```
            result = bytes([(textASCII[i] + keyASCII[i]) % 256 for i in
range(len(textASCII))])
        elif operation == DECRYPT:
            result = bytes([(textASCII[i] - keyASCII[i]) % 256 for i in
range(len(textASCII))])

    return {'operation': operation, 'type': type, 'key': key, 'text':
text, 'result': result}
```

b. Tampilan antar muka



c. Contoh plainteks dan cipherteks

i. Standard Vigenere Cipher (26 huruf alfabet)

Key: mozart

Plainteks (**vigenere_standard_plaintext.txt**):

The serenade was completed in Vienna on 10 August 1787, around the time Mozart was working on the second act of his opera Don Giovanni. It is not known why it was composed. Wolfgang Hildesheimer, noting that most of Mozart's serenades were written on commission, suggests that this serenade, too, was a commission, whose origin and first performance were not recorded.

The traditionally used name of the work comes from the entry Mozart made for it in his personal catalog, which begins, "Eine kleine Nacht-Musik". As Zaslaw and Cowdery point out, Mozart almost certainly was not giving the piece a special title, but only entering in his records that he had completed a little serenade.

The work was not published until about 1827, long after Mozart's death, by Johann Andre in Offenbach am Main. It had been sold to this publisher in 1799 by Mozart's widow Constanze, part of a large bundle of her husband's compositions.

Today, the serenade is widely performed and recorded; indeed, both Jacobson and Hildesheimer opine that the serenade is the most popular of all Mozart's works. Of the music, Hildesheimer writes, "even if we hear it on every street corner, its high quality is undisputed, an occasional piece from a light but happy pen.

Cipherteks (**vigenere_standard_ciphertext.txt**):

FVDSVKQBZDVPMGBODIXSSEUBZJHEEGMCMALZGGSAIHGBCTYXFWLEDHLOQTNTEKNRBBZUNNKAQ
GDCFGPOBTFYTWROGXDOCOEZUCUAEGUWSIJGAHJNFPZKGYZMIORCFFBCREUPAZEGRGSVHLUXEV
DIDXDBNTZGSHGAKFAGSOWFANZRKLESQEETPSRWVKQKQIKMQBNNTHYAHSJBABRUXZQGSSKAMHS
HZLESQEETPSSOFPMGZCFFYWRSZHZKGOJXAFHGZGMBCFZKEHOEIYAFLAEVQKDRVGAHQETHDRDD
KAQHQAUBFWNNREXMTSVWZOLEFYFVDWFKWQNMVLRFNMKAQSMTIRYCYAIMYOCEWHDWSIEAUGOEI
LABZLTTFOKOXPTWBHSXSWMSVBZSJLVBZSMATAFATSZDMGYAJEMKZNUVAKCEIRBCHNKHGHLOQT
DHZLDHEHBEIMMWMLPPMGMOKZUJHNXMTSOIVVQORPVVUOKTZMXSAUKHZZXEEMQFHNXBZVHSIXO
CQDJMTOSHVAMRBODIXSSEUTXWSTCXESQEETPSSHVPAFJWRLZCSPLUXWRHVWGBSICTNCTTCHZU
ZFKXDANZRKFGCERMTPXJFAMBMAEWDSHNFYRSMBRVTOLMRBZWSHRWNSDNJHXRSOKAUGOUSEUGG
EIBZPXMFSMFSSNBPCVCFGEHZNQXBOQTFYMZZRXXNIMDCXATGEIAGGAAEWEQNMGHEWSIFGEHND
RRFVDSVKQBZDVBEKHDVEKDDRWHDADDRGPFDCFKPSCIEWQSCBFMTXZCFUECMAEWTWKDVLTSHMV
KADHNVMTOSTYXESQEETPSHSKAQANSKIADTLRKATZLCFANZRKLICQKJHRHGEDNEWBHZEPSRHVB
YSQWIBFSREMXZWEWVAQOQIKHZSUEIREHQEVMOCQNVKUHRHZZTETACBFMHSLGPWRPLMQRZNFVO
ORIFGMZOIVVQTQODTXWFHKUGHGAGIKDDN

ii. Auto-key Vigenere Cipher (26 huruf alfabet)

Key: heilhitler

Plainteks (**vigenere_autokey_plaintext.txt**):

My Fuhrer

General Koller today gave me a briefing on the basis of communications given him by Colonel General Jodl and General Christian, according to which you had referred certain decisions to me and emphasized that I, in case negotiations would become necessary, would be in an easier position

than you in Berlin. These views were so surprising and serious to me that I felt obligated to assume, in case by 2200 o'clock no answer is forthcoming, that you have lost your freedom of action. I shall then view the conditions of your decree as fulfilled and take action for the wellbeing of Nation and Fatherland. You know what I feel for you in these most difficult hours of my life and I cannot express this in words. God protect you and allow you despite everything to come here as soon as possible.

Your faithful Hermann Goring.

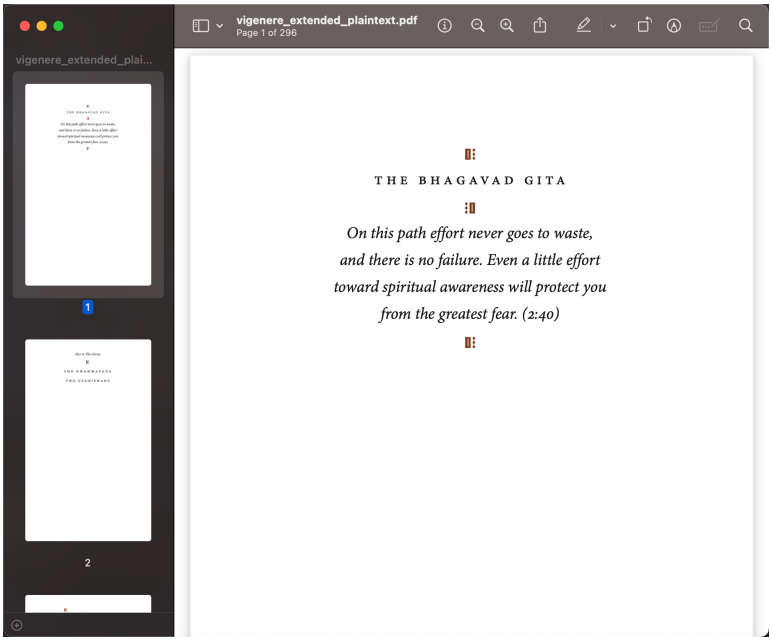
Cipherteks (**vigenere_autokey_ciphertext.txt**):

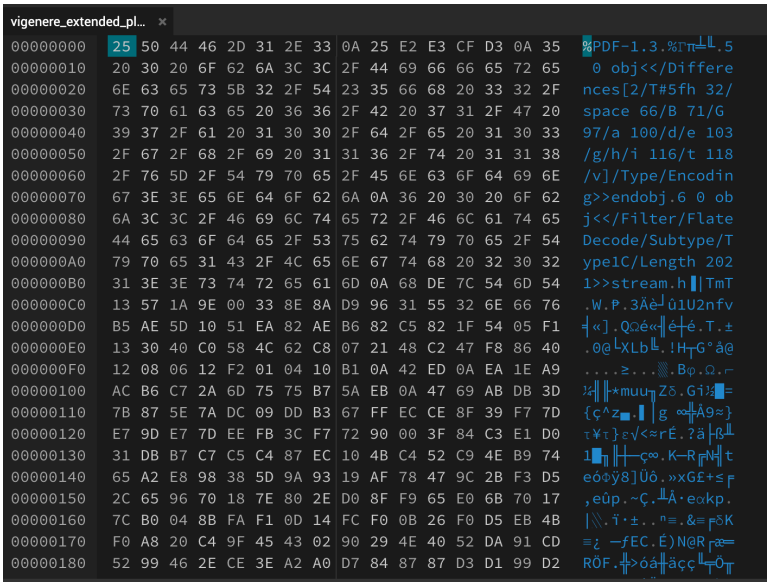
```
TCNFOZXCKVZCWUSBSCRIEXFDLIULGIDXOERGKFDRSSNUYMFFAVYCSVVQNUFQUOYKCZEAVDGNA
QAOQIWGSALTSFLGFLZWSOREAHXEYNFDWCUUOWGMRNLEJFZVBVGGOYJWTKGBAAOZYMHLPFYKCH
IXFMEUIFKWZHNAGRQGIFLSZHAOEMZRGXTPAIAVBEVXUEZWBVCTASAWCCNTDUMQBEABYNHTWCF
KABYNHTWIEYJSUDLFVXBSVXIGVXYPBQWNQBOXYLVLHBMFFZZPEFPLVWWJAYNHNMJMFUSHUHVZ
AWHYTBPWXYIHCXXZFSUSIZIYIOMCBDAAMXMQVOSWTSAGTBEKFSBLGYPFKCSCRGZYSDQFLHYTA
ACGPNBXSOLRMIBRAVPSVHKCZRHKMSQWEVFLNMPSADALWESXJSAYQXEHUWQTLRCKLSPJSJYGZL
OJKCPIDSSXEFSPLGWIBQYOBXHGPMZYGSZGNSBRLEJSVNTRKNTAMFYAAGDONRRFHWUDRWZORZB
KYYHCNRXSJGVKCMBQBMJAGGZLARCWXWHGJEPTYRFRNOYYVTXEKSZGSFGVBWFCNSJVLNWVXEKH
VFLECXPERTPNHUMIUQHSATHACJYUCLWQGKXJGFKXOMEKTGUCARHWGSSKAPZRYGJFXSQUSJSZB
VWMIGULICPRX
```

iii. Extended Vigenere Cipher (256 karakter ASCII)

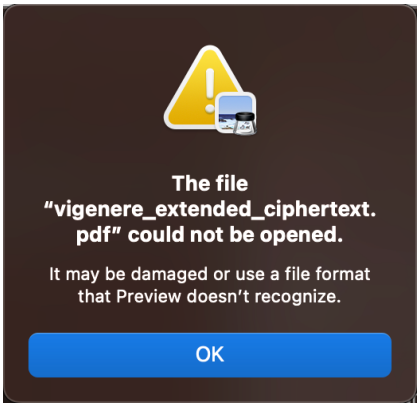
Key: `mahabharata`

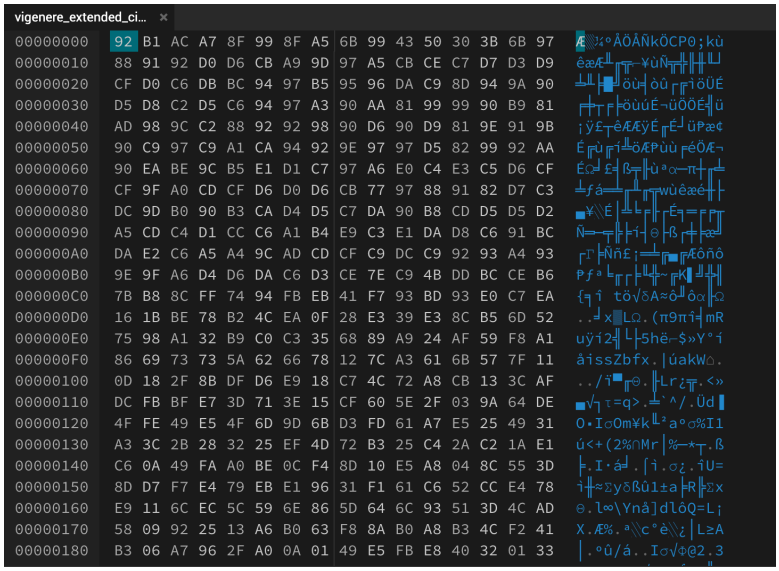
Plainteks (**vigenere_extended_plaintext.pdf**):





Cipherteks (**vigenere_extended_ciphertext.pdf**):





3. Affine Cipher

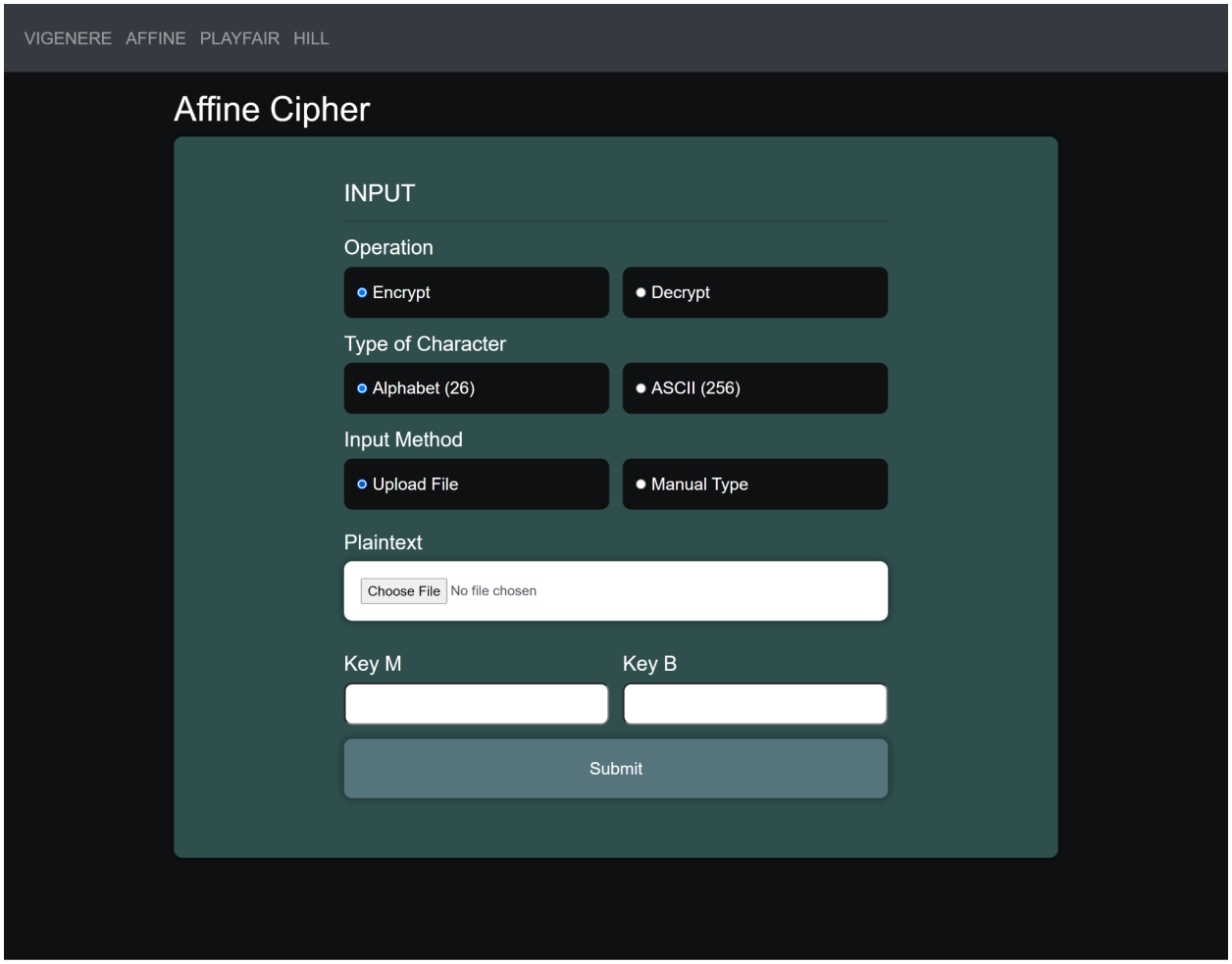
a. *Source code program*

Program Affine Cipher terdiri atas fungsi utama ***cipher*** yang menerima pesan berupa plainteks maupun cipher teks, *key* M dan B bertipe integer, operation berupa *encrypt* atau *decrypt*, serta *n* yang merepresentasikan jenis karakter alfabet 26 karakter atau ASCII 256 karakter. Program ini dibantu oleh fungsi ***validateKey*** untuk mengecek apakah *key* M relatif prima dengan *n*.

```
from . import stringparser as sp
from math import gcd

ENCRYPT = 'encrypt'
DECRYPT = 'decrypt'

ALPHABETICAL = 26
BYTELENGTH = 256

def validateKey(n: int, m: int) -> bool:
    """Validate key, m must be relatively prime with n."""
    return gcd(n, m) == 1

def cipher(text, keyM: int, keyB: int, operation=ENCRYPT,
n=ALPHABETICAL) -> dict:
    """Encrypt/decrypt plaintext using Affine cipher with key.

    Returns a dictionary with the type of operation (encyrpt or
decrypt), alphabet size, M & B key, original text, and resulting
text."""

    if not validateKey(n, keyM):
        return {'error': f'Key M is not relatively prime with alphabet
size, {n}.'}
    if not 0 < keyB < n:
        return {'error': f'Key B must be in range 0 < b < {n}.'}

    if n == ALPHABETICAL:
        text = sp.stringToAlphabet(text)
        textNumbers = sp.alphabetToNumber(text)
    elif n == BYTELENGTH:
```

```
        textNumbers = text

    if operation == ENCRYPT:
        """ENCRYPT -> C ≡ mP + b (mod n)"""
        result = [((keyM * p + keyB) % n) for p in textNumbers]
    elif operation == DECRYPT:
        """DECRYPT -> P ≡ m^-1(C - b) (mod n)"""
        mInverse = pow(keyM, -1, n)
        result = [((mInverse * (c - keyB)) % n) for c in textNumbers]

    if n == ALPHABETICAL:
        result = sp.numberToAlphabet(result)
        if operation == DECRYPT:
            result = result.lower()
    elif n == BYTELENGTH:
        result = bytes(result)

    return {'operation': operation, 'n': n, 'keyM': keyM, 'keyB': keyB,
'text': text, 'result': result}
```

b. Tampilan antar muka



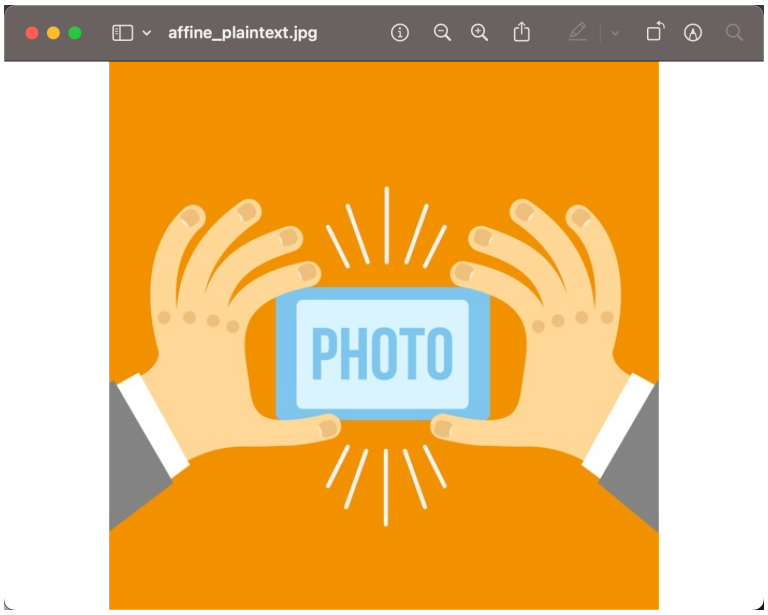
c. Contoh plainteks dan cipherteks

Type of character: ASCII (256)

Key M: `7`

Key B: `102`

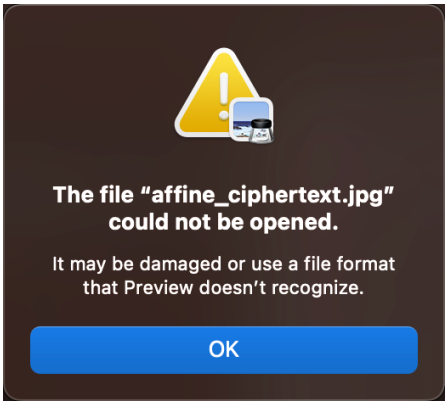
Plainteks (**affine_plaintext.jpg**):

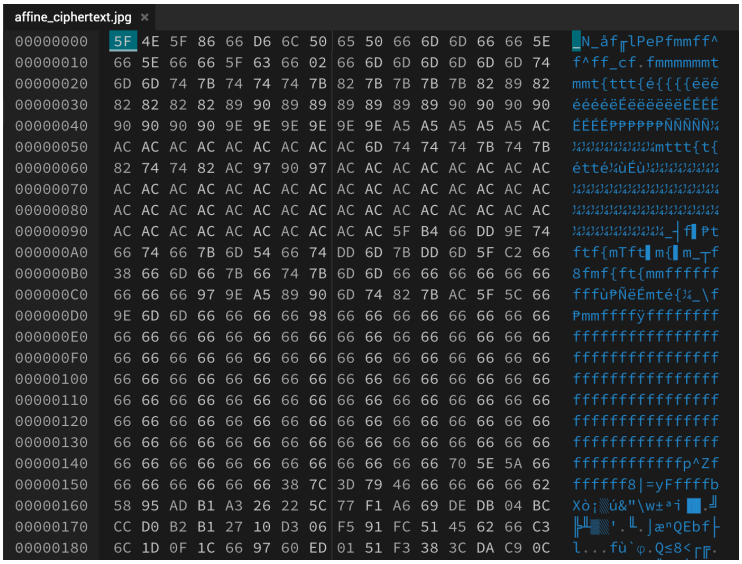


affine_plaintext.jpg

```
00000000  FF D8 FF E0 00 10 4A 46 49 46 00 01 01 00 00 48  ╪ α..JFIF.....H
00000010  00 48 00 00 FF DB 00 84 00 01 01 01 01 01 01 02  .H.. ▐.ä........
00000020  01 01 02 03 02 02 02 03 04 03 03 03 03 04 05 04  ................
00000030  04 04 04 04 05 06 05 05 05 05 05 05 06 06 06 06  ................
00000040  06 06 06 06 08 08 08 08 08 08 09 09 09 09 09 0A  ................
00000050  0A 0A 0A 0A 0A 0A 0A 0A 0A 01 02 02 02 03 02 03  ................
00000060  04 02 02 04 0A 07 06 07 0A 0A 0A 0A 0A 0A 0A 0A  ................
00000070  0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A  ................
00000080  0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A 0A  ................
00000090  0A 0A 0A 0A 0A 0A 0A 0A 0A 0A FF C2 00 11 08 02  .......... ┬····
000000A0  00 02 00 03 01 22 00 02 11 01 03 11 01 FF C4 00  ·····"····· ─·
000000B0  1E 00 01 00 03 00 02 03 01 01 00 00 00 00 00 00  ................
000000C0  00 00 00 07 08 09 05 06 01 02 04 03 0A FF DA 00  ............ ┌·
000000D0  08 01 01 00 00 00 00 BE 00 00 00 00 00 00 00 00  ·······┘........
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000140  00 00 00 00 00 00 00 00 00 00 00 00 26 48 6C 00  ............&Hl.
00000150  00 00 00 00 00 00 1E BA B1 95 20 00 00 00 00 24  .......▒▒ò ....$
00000160  FE 99 C1 9D 9B 40 64 DA 27 5D C0 25 C8 A3 F2 7A  ▪Ö┴¥¢@d┌']└%╚ú≥z
00000170  EA C6 54 9D F7 86 EB 60 39 BD 3A FD 69 24 00 7B  Ω╞T¥≈ðˋ9╜:²ï$.{
00000180  4A D1 CF 1A 00 07 B6 81 CD FD CB 1E FA EC C5 AA  J╤╧...╢ü═²╦·∞╪¬
```

Cipherteks (**affine_ciphertext.jpg**):





4. Playfair Cipher

a. *Source code program*

Program Playfair Cipher terdiri atas fungsi ***cipher*** yang menerima pesan berupa plainteks maupun cipherteks, *key* bertipe string, dan *operation* berupa encrypt atau decrypt. Program ini dibantu dengan fungsi parseKey untuk membentuk matriks *key* dengan membuang huruf duplikat, membuang huruf "J" jika ada, dan melengkapi matriks dengan sisa huruf yang tersedia. Selain itu, program ini juga dibantu dengan fungsi parseText untuk melakukan *preprocessing* pada pesan dengan cara mengganti "J" menjadi "I", membuat bigram, dan menambahkan "X" jika dibutuhkan.

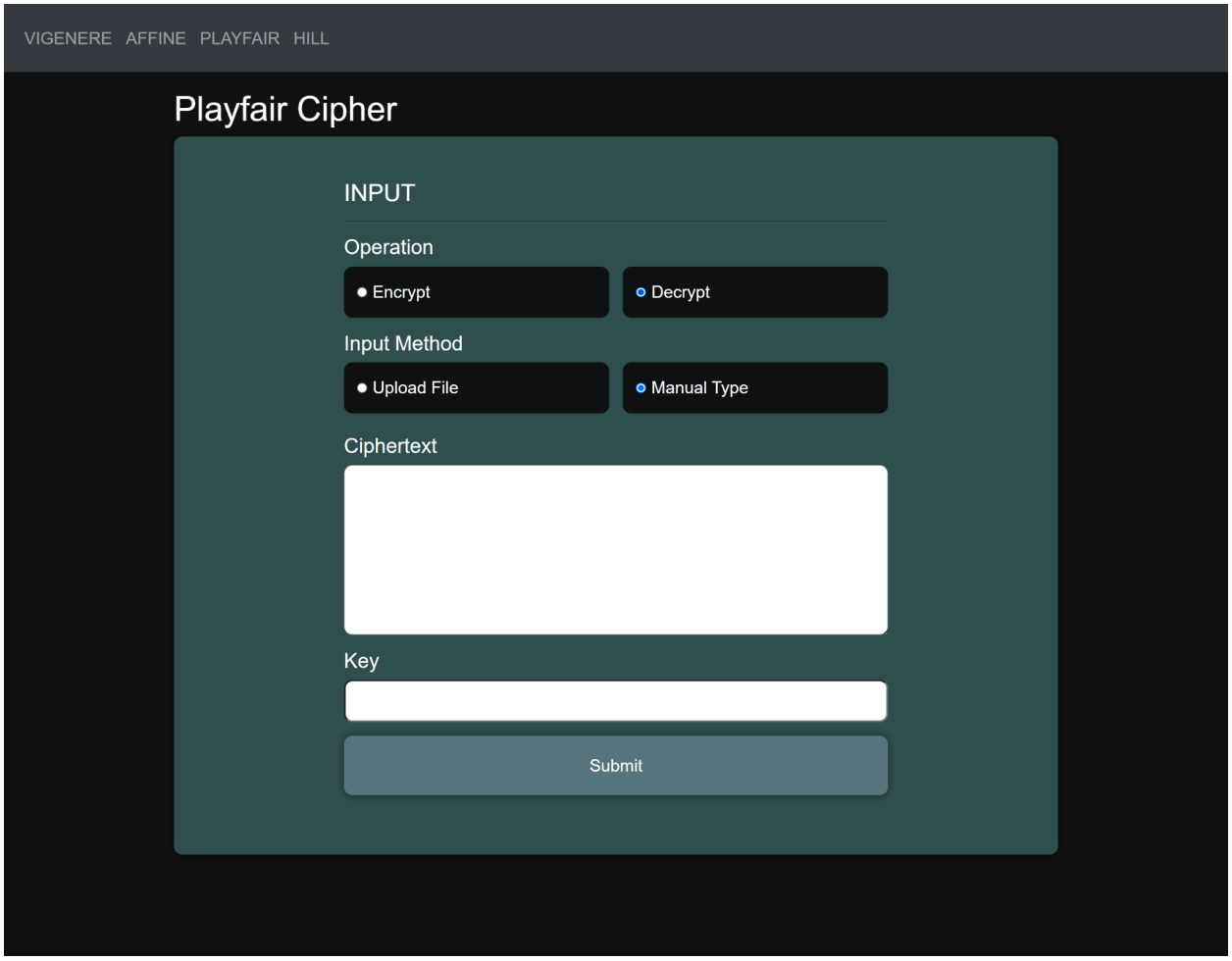
```
from . import stringparser as sp
import numpy as np

ENCRYPT = 'encrypt'
DECRYPT = 'decrypt'

def parseKey(key: str) -> list[list[int]]:
    """Parse key to be square matrix"""

    key = sp.stringToAlphabet(key)

    key = ''.join(dict.fromkeys(key))
    key = key.replace('J', '')
```

```
    for char in ('ABCDEFGHIKLMNOPQRSTUVWXYZ'):
        if char not in key:
            key += char

    matrixKey = np.array(list(key))
    matrixKey = matrixKey.reshape(5, 5)

    return matrixKey

def parseText(text: str) -> list[str]:
    """
        - Replace 'J' with 'I'
        - make bigram
        - add 'X' if there is pair of same character
        - add 'X' if the length of text is odd
    """

    text = sp.stringToAlphabet(text)
    text = text.replace('J', 'I')

    bigram = []
    i = 0
    while i < len(text):
        if i + 1 < len(text):
            if text[i] == text[i + 1]:
                bigram.append(text[i] + 'X')
                i += 1
            else:
                bigram.append(text[i] + text[i + 1])
                i += 2
        else:
            bigram.append(text[i] + 'X')
            i += 1

    return bigram


def cipher(text: str, key: str, operation=ENCRYPT) -> dict:
    """Encrypt/decrypt plaintext using Playfair cipher with key.
```

```
    Returns a dictionary with the type of operation (encyrpt or
decrypt), key, original text, original text bigram, and resulting
text."""

    text = sp.stringToAlphabet(text)
    matrixKey = parseKey(key)
    bigram = parseText(text)

    result = []
    if operation == ENCRYPT:
        for pair in bigram:
            p1 = np.where(matrixKey == pair[0])
            p2 = np.where(matrixKey == pair[1])

            if pair[0] == 'X' and pair[1] == 'X':
                result.append('XX')
            elif p1[0] == p2[0]:
                result.append(matrixKey[p1[0], (p1[1] + 1) % 5][0] +
                              matrixKey[p2[0], (p2[1] + 1) % 5][0])

            elif p1[1] == p2[1]:
                result.append(matrixKey[(p1[0] + 1) % 5, p1[1]][0] +
                             matrixKey[(p2[0] + 1) % 5, p2[1]][0])

            else:
                result.append(matrixKey[p1[0], p2[1]][0] +
                             matrixKey[p2[0], p1[1]][0])
        result = ''.join(result)
    elif operation == DECRYPT:
        for pair in bigram:
            p1 = np.where(matrixKey == pair[0])
            p2 = np.where(matrixKey == pair[1])

            if pair[0] == 'X' and pair[1] == 'X':
                result.append('XX')
            elif p1[0] == p2[0]:
                result.append(matrixKey[p1[0], (p1[1] - 1) % 5][0] +
                              matrixKey[p2[0], (p2[1] - 1) % 5][0])
```

```
            elif p1[1] == p2[1]:
                result.append(matrixKey[(p1[0] - 1) % 5, p1[1]][0] +
                              matrixKey[(p2[0] - 1) % 5, p2[1]][0])

            else:
                result.append(matrixKey[p1[0], p2[1]][0] +
                              matrixKey[p2[0], p1[1]][0])
        result = (''.join(result)).lower()


    return {'operation': operation, 'key': matrixKey, 'text': text,
'text bigram': ' '.join(bigram), 'result': result}
```

b. Tampilan antar muka



c. Contoh plainteks dan cipherteks

Key: `syracuse`

Plainteks (**playfair_plaintext.txt**):

```
The decision of Mr. Hearst to establish a metropolitan newspaper here indicates
his appreciation of the importance of this city and his conviction that it is a
growing, prosperous and progressive center.
```

Cipherteks (**playfair_ciphertext.txt**):

```
VGBFFYGROWOPUQYIDYAYVZWMUYXSFIGRKYNUWSPQQIGWYPVHTRXDNDYIBYBHPELRSXUYIKYCXAOAFYK
RWGPOQBVGBHNQWBXSQYBNUZIKYSGWRCPEIKYSPOWHSZOWMVKYWGWGYCISWRHOKMBWAMBYMBYCPEOAMI
YBATRGYHYFMVBY
```

5. Hill Cipher

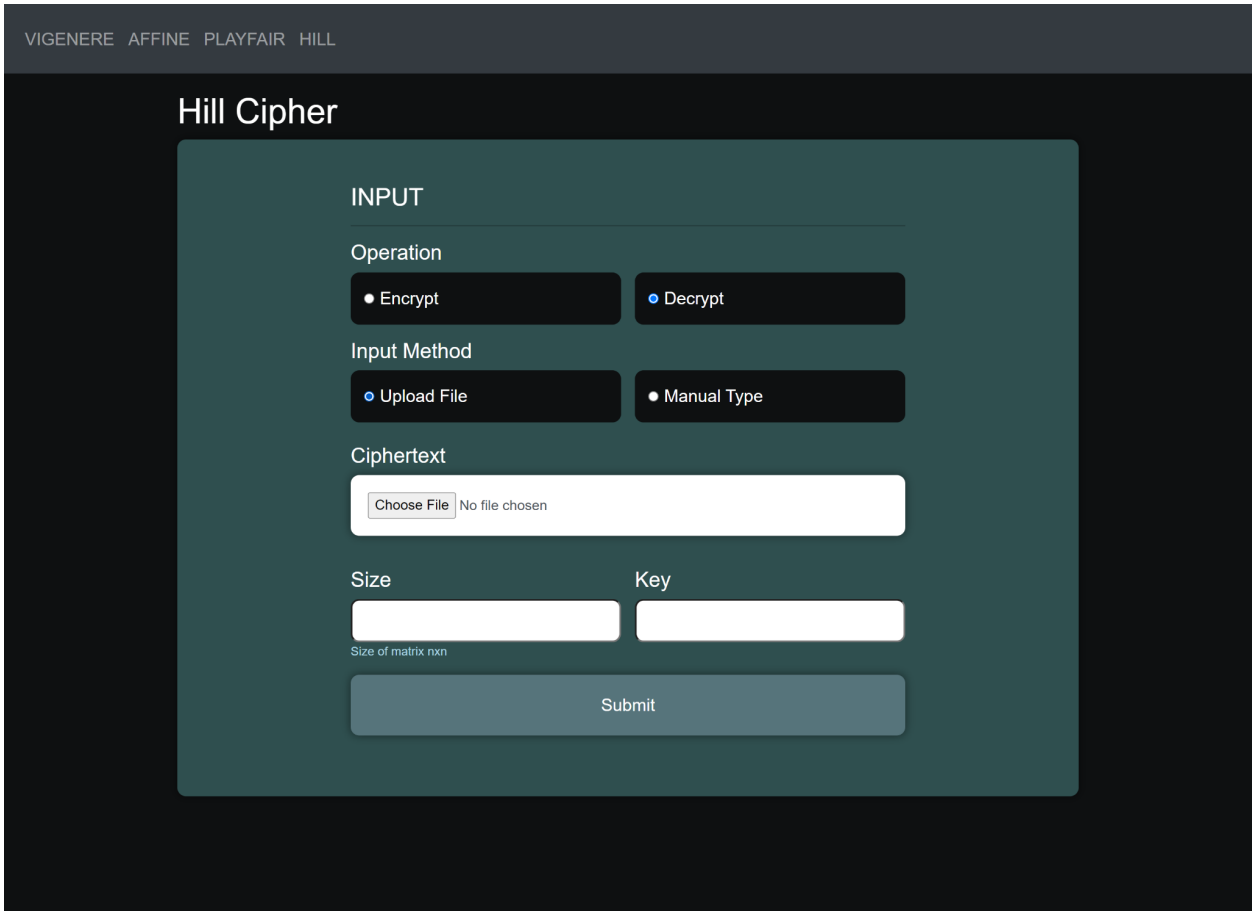
a. *Source code program*

Program Hill Cipher terdiri atas ***cipher*** yang menerima pesan berupa plainteks atau cipherteks, *key* bertipe string yang memiliki panjang *nxn* agar dapat dibentuk matriks dengan ukuran *nxn* dengan *n* adalah *size* yang harus ditetapkan. Matriks *key* harus bersifat invertible agar dapat didekripsi. Program ini juga menerima *operation* berupa *encrypt* atau *decrypt*. Pesan akan dienkripsi/didekripsi per *n* huruf. Untuk memenuhi kekurangan karakter, maka ditambahkan padding "X" secukupnya. Misal, jika ukuran matriks 3x3 dan plainteks adalah "CLASSIC" maka plainteks akan diubah menjadi "CLASSICXX" agar tepat 9 karakter untuk kemudian dikonversi ke matriks numerik.

```
from . import stringparser as sp
from . import matrixoperation as mo
import numpy as np

ENCRYPT = 'encrypt'
DECRYPT = 'decrypt'
N = 26

def cipher(text: str, key: str, size: int, operation=ENCRYPT) -> dict:
    """Encrypt/decrypt plaintext using Hill cipher with key. Adds
padding of X if text length is not a multiple of size.

    Returns a dictionary with the type of operation (encyrpt or
decrypt), key, original text, and resulting text."""

    if not sp.isAlphabet(key):
        return {'error': 'Key must only contain alphabetical
characters.'}
    if len(key) != size*size:
        return {'error': f'Key must have length {size*size}.'}

    text = sp.stringToAlphabet(text)
    lenText = len(text)
    if lenText % size != 0:
        text += 'X' * (size - (lenText % size))
```

```
    textNumber = sp.alphabetToNumber(sp.stringToAlphabet(text))
    textMatrix = np.array([textNumber[i:i+size] for i in range(0,
len(text), size)])
    textMatrix = textMatrix.transpose()

    keyNumber = sp.alphabetToNumber(sp.stringToAlphabet(key))
    keyMatrix = np.array([keyNumber[i:i+size] for i in range(0,
len(key), size)])

    if not mo.isInverseMatrix(keyMatrix,size,N):
        return {'error': 'Key matrix is not invertible.'}

    if operation == ENCRYPT:
        """C = KP mod N"""
        cipherMatrix = np.remainder(np.matmul(keyMatrix, textMatrix), N)
        result =
(sp.numberToAlphabet(cipherMatrix.transpose().flatten()))

    elif operation == DECRYPT:
        """P = K^-1C mod N"""
        keyInv = mo.getInverseMatrixModulo(keyMatrix, size, N)
        plainMatrix = np.remainder(np.matmul(keyInv, textMatrix), N)
        result =
(sp.numberToAlphabet(plainMatrix.transpose().flatten())).lower()

    return {'operation': operation, 'key': key, 'text': text, 'result':
result}
```

b. Tampilan antar muka



c. Contoh plainteks dan cipherteks

Size: 4

Key: microinstruction

Plainteks (**hill_plaintext.txt**):

Edward Joseph Snowden is an American and naturalized Russian former computer intelligence consultant who leaked highly classified information from the National Security Agency (NSA) in 2013, when he was an employee and subcontractor. His disclosures revealed numerous global surveillance programs, many run by the NSA and the Five Eyes intelligence alliance with the cooperation of telecommunication companies and European governments and prompted a cultural discussion about national security and individual privacy.

In 2013, Snowden was hired by an NSA contractor, Booz Allen Hamilton, after previous employment with Dell and the CIA. Snowden says he gradually became disillusioned with the programs with which he was involved, and that he tried to raise his ethical concerns through internal channels but was ignored. On May 20, 2013, Snowden flew to Hong Kong after leaving his job at an NSA facility in Hawaii, and in early June he revealed thousands of classified NSA documents to journalists Glenn Greenwald, Laura Poitras, Barton Gellman, and Ewen MacAskill. Snowden came to international attention after stories based on the material

appeared in The Guardian, The Washington Post, and other publications. Snowden made a number of claims about the Government Communications Security Bureau (GCSB) of New Zealand. He accused the agency of conducting surveillance on New Zealand citizens and engaging in espionage during the time period of 2008 - 2016, when John Key served as the Prime Minister of New Zealand.

Cipherteks (**hill_ciphertext.txt**):

```
MCVSQHKFHHWZUYDSWXLLIFEEITCEYPMMYLMLGXBFCRVZYICFHEKDUVVDKCRGDGLRFKFZBPVOJEWJMAS
UHENIFXJKPQHHGYYICYKRUOYLGKHTMQPSDBVEQUPYVSXKMGMLTKOSQOREQZJLDOYVKETQIJEQMYXGZE
VFALDSOWYUZQNSWAZHVTELWTEWBVRZGVAWKUOXOMLJWCPBPEFWQQTOBRZKJGWZYWQCMTZXHGNWTEZKK
VFBYZXSWULQNKAJJEBBXHPWGEHQRRHDCBFBYEXTNSWHBPVOJEWJJYYFBKHACWQOZTQUSMCCMVRJVSXK
CJLAQWHJHEATTCQZINEEITQAOYFDWHDQJKRXUVKYJUJJNSLWVURYMLEZGJNQQMHHPOEEWLDAGUGOJEE
RMEZWFKWKADAEGWBTNEJRBNUBEJHMMDLLRRBZMETIIJEAZKVEOEJUFQFDOFNKUZXAFQCRIWEDBTFWSJ
QAHIICKIZPNUGYQVFUKBQFIQXJHIEJCOPHSXTEBTXZCBPGZHQECUKWUYDSKVFLJGCPANYYTKDWEPVZM
WAYMQXJUUAFQXIEFOFUGXGTEMITOQBXRRMHGKZOCEMLROYJPRPCHCXJUZAVROASPSZOKBDJDSGBZAEB
WGXRHODSZVEJVVHHROMDUPHCBUUYPGBDWFZRMLDDCSKWGPBZOTHNHKOPCPGQAVOZROVZMMDMYOJMPIM
EBSHUTENPCBQGYBJZKAWFSGVTSNTTGVTQAKWKMBLQJALGGRFHKNVNIRNZRMNBCGUPHHKRIXIEGKHTMQ
PSUQOXYULPFJWNDUBBLFKBUWTSZKDEUVXYXKDIZLUNTSTIYEFEUYKDFFHKOIRMKIMXZPTALYKJSMIWF
KSBURXPXUDRMWAYFOFAVZPUQOREWNZLLCKKVSXKQVFUAXXFKCDBMIXLDPVAKAZVONFHFUJXHCXSXCBR
EOAFNJYHDZIJEARFPWXDFCPHBOLMKFXQJEWSJJRETCQZUPKEUYDSMRTLGYBCTWXQLWFFOAHWTSQVNJK
DCSLPTBBGFJWNASUGEELYQOREOILTQHGUIZXVEGPRLOQFQJVUEONYBNHOUKXJCASIKTIVRWANRYIXFZ
WHOLEMISVBWEWBZIGYTIWTHOZCSRKWIMQNUZRVBOHOONHLZWCRWZYWSAFCCULTCVZNXFPCEILCXODFK
VKUGTTFLQSICSZTPZMBOOHWBUSSWKFJGZQGPIZRQJVUEONYBNHO
```

6. Link Github Kode Program

https://github.com/blueguy42/Classic-Ciphers

Bagian B

1. Teknik Analisis Frekuensi pada Cipher Abjad-Tunggal

a. Berkas cipherteks

```
CZWKWFKWUFKNXHLCZWXKNWLFLCXQZWKWCZWCWKEUNSNJPXKNPNJFCWYXJWVXXSLCXCZWBWENJNJWGKW
BNIUNSEWFJNJPNJVWCXKOFRQZNVWXCZWKLAVFNECZWZNLCXKNAJXKQWPNFJLWCCVWEWJCXBUNSWJNLQ
ZWKWCZWJFEWYWKNUWLZWJAWUNSNJPLQWKWCZWXKNPNJFVYQWVVWKLXBUNSWJFVCWKJFCNUWVRKWAXPJ
NLWYWCREXVXPNLCLLHAZFLFJFCXVRVNOWKEFJGXNJCCXCZWXVYJXKLWQXKYUNSFEWFJNJPLWFENVWCZ
WLGFAWVWBCOWCQWWJCQXKXQNJPOXFCLNJAXJUXRQZNVWXCZWKLKWBWKCXCZWCZAWJCHKRFJPVXLFIXJ
GXWEQNYLNCZQZNAZKWBWKLCXLAFJYNJFUNFJGNKFCWLFLQNANJPLKWPFKYVWLLPNUWJCZWLAFJYNJFU
NFJLYXENJFJAWXBCZWLWFYHKNJPCZNLWFKVRGWKNXYNCQFLJCVXJPHJCNVAXJCKFLCNJPJFEWLQWKWO
WNJPXBBWKWYHGORUFKNXHLXCZWKAHVCHKWLFAKXLLCZWGVFJWCCZWFKFOLLVFULFJYORDFJCNJWLBXK
WIFEGVWSJWQXBCZWLWKFNYWKLFLKHLXKKZXLKWVFCNJPCXKXQNJPQZNVWCZWPWKEFJLVFOWVVWYCZWE
FLFLAXEFJJNFLZEWJFVVHYNJPCXCZWNKFLZQXXYOXFCLXCZWKJFCNXJLLHAZFLCZWWJPVNLZFJYAWVC
LLWCCVWYEWKWVRXJYFJWLZWFCZWJLXKGFPFJLQZNVLCCZWNKNLZKWBWKKWYCXCZWEFLYHOPFNVFJYBN
JJPFNVYFKSFJYBFNKBXKWNPJWKLXKTHNCWLHNCFOVRJXKCZEWJPNUWJCZWAXEEXJAHVCHKFVGKFACNA
WXBCXKEWJCNJPAXFLCFVLWCCVWEWJCLFJYEXJFLCWKNWLNCQFLJCVXJPHJCNVCZWUNSNJPLBWFKLXEW
KWGHCFCNXJLGKWFYCXFVEXLCFVVAXKJWKLXBWHKXGWFJYEWLXGXCFENFCZWKWNLWUWJWUNYWJAWCZFC
CZWUNSNJPLKWFAZWYOFPZYFYCZWAWJCKWXBCZWNLVFENAWEGNKWFCCZWCNEWCZWUNSNJPFPWFLAXEEX
JVRKWBWKKWYCXVFLCWYBKXECZWWFKVRLCXCZWJXKEFJAXJTHWLCXBWJPVFJYNJCZKXHPZXHCCZNLGWK
NXYCZWUNSNJPLHLWYCZWJXKCZWKJFJYOFVCNALWFLCXCWKKXKNLWJWNPZOXHKNJPSNJPYXELWICWJYN
JPCZWNKNJBVHWJAWCZKXHPZAXEOFCFJYAHVCHKWHJCNVWUWJCHFVVRUNSNJPLAXHVYJXVXJPWKOWEWK
WVRYWLAKNOWYFLAXFLCFVKFNYWKLAXJLNYWKCZWBFACLCQXUNSNJPSNJPLLQWRJBXKSOWFKYFJYAJHC
```

```
CZWPKWFCQXHVYFLAWJYCZWWJPVNLZCZKXJWVWNBWKNSLXJFJWFKVRNAWVFJYWKQXHVYLWCCVWLZXKCN
UWYAXVXJNWLNJJXKCZFEWKNAFLAFJYNJFUNFJLQXHVYWUWJLWKUWFLEWKAWJFKNWLBXKCZWORDFJCNJ
WWEGNKWNJLZXKCCZWLWQWKWJXEWKWGNKFCWLOHCCZWBXKWBFCZWKLXBFGFCAZQXKSTHNVCAHVCHKWCZ
WEXCNUFCNXJLBXKLHAZWIGFJLNXJFKWLHOMWACCXYWOFCWBXKEXYWKJZNLCXKNFJLCZXHPZCZWKWFKW
AVWFKNJAWJCNUWLFLCXQZRCZWGXGHVFCNXJXBLAFJYNJFUNFENPZCZFUWFACWYNJCZWQFRCZFCCZWRY
NYYHKNJPCZNLRWFKGWKNXYXJWKWVFCNUWVRFGGFKWJCKWFLXJNLFLAFKANCRXBKWLXHKAWLCZHLBXKA
NJPCZWUNSNJPLCXVXXSBHKCZWKFBNWVYWUWJKXOONJPFJYSNVVNJPAVFLLWLXBGWXGVWOVWLLWYQNCZ
FEXKWOXHJCNBHVZXEWVFJYFJXCZWKGXLLNOVWLCNEHVHLNLCZWKHVWXBAZFKVWEFPJWFJYCZWKWVNPN
XHLGWKLWAHCNXJCZFCQWJCZFJYNJZFJYQNCZNCQNCZAZKNLCNFJNJBVHWJAWLWWGNJPWUWKBHKCZWKN
JCXYWJEFKSLQWYWJFJYJXKQFRNCEFSWLVXPNAFVLWJLWCZFCCZWUNSNJPLQWKWVXXSNJPCXGKXCWACC
ZWNKGFPFJOWVNWBLRLCWEKWLNLCMHYWXAZKNLCNFJUFVHWLFJYWUWJCFSWKWUWJPWBXKCZXLWLWCCVW
EWJCLFVKWFYRVXLCCXFEXJXCZWNLCNAYWUXCNXJCZNLNLJXCLGWAHVFCNXJCZWNJCKXYHACNXJXBAZK
NLCNFJNCRQXHVYAXEWCXYNUNYWJXKQFRBXKFVEXLCZFVBFAWJCHKRAFHLNJPHJCXVYOVXXYLZWYFJYA
HVCHKFVCKFJLBXKEFCNXJNCLZXHVYFVLXOWJXCWYCZFCYHKNJPCZWUNSNJPFPWLAFJYNJFUNFLAVXLW
LCJWNPZOXHKLQWKWWIGWKNWJANJPUFKRNJPVWUWVLXBNJJWKCHKEXNVCZHLPKFJCNJPCZWUNSNJPLFJ
FYUFJCFPWQZWJWIGVXNCNJPCZWLWVFJYLBXKQWFVCZLVFUWLXKCWKKNCXKRCZWLWFKXHCWLHLWYORCZ
WUNSNJPLQWKWFVEXLCWJCNKWVRBKWWXBXGGXLNCNXJVWFUNJPCZWKFNYWKLHJNEGWYWYFLCZWRCKFUW
VVWYBKXEXJWYWLCNJFCNXJXBGVHJYWKCXCZWJWICCZNLOKWFSYXQJNJQZFCZFYXJAWOWWJFGKXBNCFO
VWJWCQXKSXBCKFYWKXHCWLBXKWHKXGWFJSNJPYXELAFJOWZWKFVYWYOFASFLBFKFLCZWAXVVFGLWXBC
ZWKXEFJWEGNKWNJCZWCZAWJCHKRFJYVFCWKCXCZWKFGNYCZAWJCHKRWIGFJLNXJXBNLVFENAGZNVXLX
GZRCZWWJYXBCZWUNSNJPFPWAFJOWGNJJWYYXQJCXFJHEOWKXBBFACXKLBNKLCXBFVVCZWBFVVXHCCZF
CXAAHKKWYBXVVXQNJPCZWAZKNLCNFJNLFCNXJXBLAFJYNJFUNFQXHVYZFUWHJCXVYWBBWACLXJCZWKW
PNXJLYXEWLCNAFJYBXKWNPJGXVNARORCZWCZAWJCHKRYWJEFKSJXKQFRFJYLQWYWJQWKWWBBWACNUWV
RAXJCKXVVWYORYNXAWLWLVWPNCNENLWYORCZWAFCZXVNAAZHKAZFJYZFYBNKEVRWLCFOVNLZWYCZWEL
WVUWLFLLWGFKFCWSNJPYXELCZNLEWFJCFJWJXKEXHLAHVCHKFVLZNBCNJCZWGKNXKNCNWLXBLAFJYNJ
FUNFLVWFYWKLZNGNJCZFCLWJLWCZWUNSNJPLQWKWJXCYWBWFCWYOHCFKPHFOVREFYWCXOWZFUWNJFEF
JJWKCZFCBNCCZWANUNVNCRXBCZWNKTHNASVRCKFJLBXKENJPZXEWVFJYLBXKWIFEGVWCZWEWYNWUFVA
ZHKAZEFYWNCBXKONYYWJCXCFSWBWVVXQAZKNLCNFJLFLLVFUWLPNUWJCZWBFACCZFCLVFUWCKFYNJPQ
FLCZWJHEOWKXJWLXHKAWXBGKXBNCBXKCZWUNSNJPLCZNLKWEXUWYFPKWFCYWFVXBCZWWAXJXENANJAW
JCNUWCXCKFUWVFJYKFNYXUWKLWFLCZWJWQVWFYWKLZNGFVLXAZXLWCXKWBXAHLCZWNKENVNCFKRFCCW
JCNXJBKXECZWSNJPYXELXBCZWQWLCFJYNJLCWFYGFKCFSWNJLHAZAFEGFNPJLFLCZWOFVCNAQFKLFJY
CZWFCCWEGCWYAXJTHWLCXBMWKHLFVWEBKXEZWKWXJXHCNCLWWEWYCZWUNSNJPLQWKWJXVXJPWKFKWAX
PJNLWYBXKAWNJCZWQXKVYCZXHPZCZWNKOKHCFVNCROKFUWKRFJYLCKWJPCZQXHVYVXJPOWKWEWEOWKW
YORCZXLWQZXZFYXJAWBWVCCZWLZFKGWYPWXBCZWNKOFCCVWFIW
```

b. Langkah-langkah dekripsi

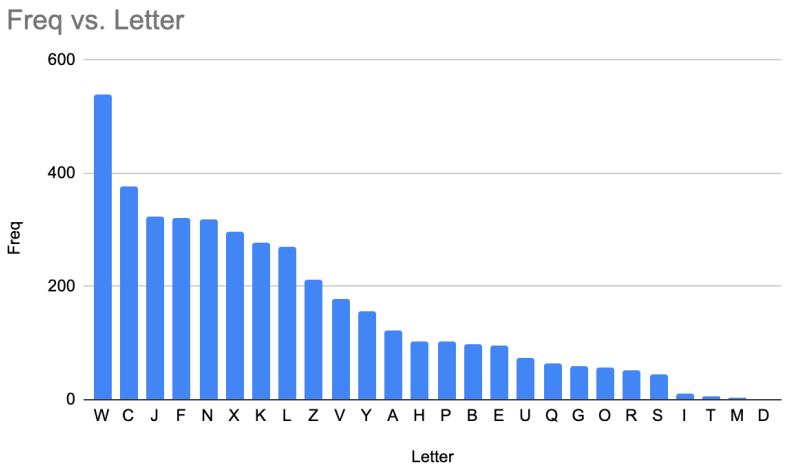
Pengubahan dari cipherteks ke plainteks dibantu menggunakan fitur *search and replace* pada Visual Studio Code yang mempunyai kapabilitas pencarian *match case* sehingga cipherteks direpresentasikan dengan huruf kapital dan plainteks dengan huruf kecil.

Pertama-tama dibuat tabel frekuensi kemunculan huruf dengan sebuah fungsi Python bernama ***substringFreq*** yang dapat dilihat pada *file* **script.py**:

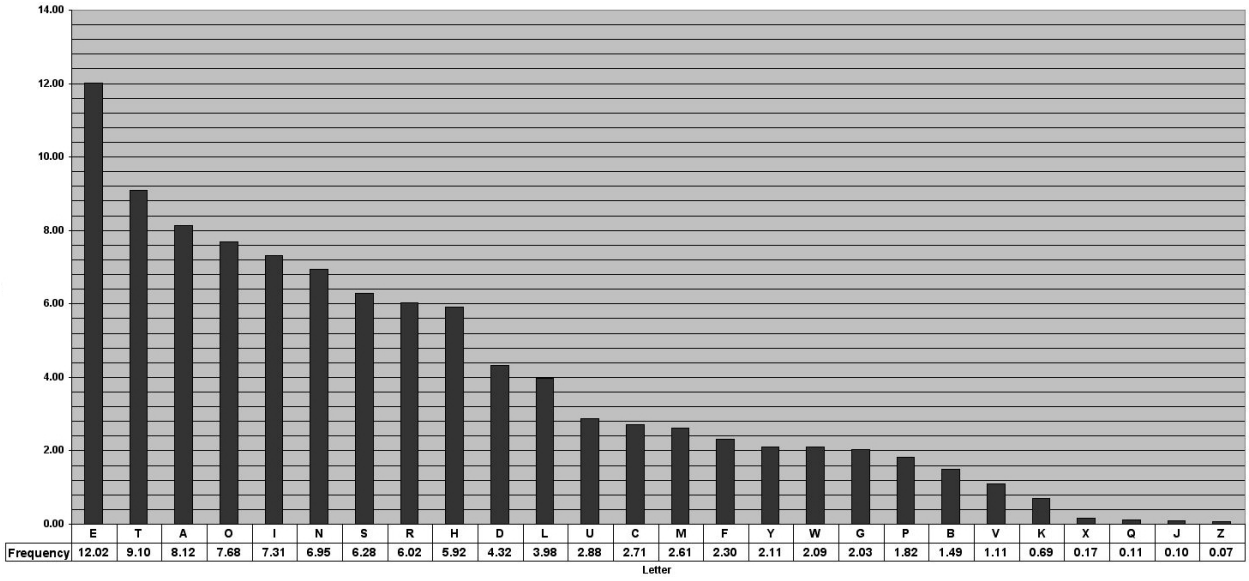
```python
def substringFreq(string: str, n: int, step: int, printAll: bool) -> dict:
    """Returns a dictionary of frequencies of substring length n of a string, sorted by frequency.
    First removes all non-alphabetic characters and converts them to uppercase. Goes through string with steps."""
    string = ''.join(filter(str.isalpha, string)).upper()

    freq = {}
    for i in range(0, len(string)-n+1, step):
        if string[i:i+n] in freq:
            freq[string[i:i+n]] += 1
        else:
            freq[string[i:i+n]] = 1
    freq = dict(OrderedDict(sorted(freq.items(), key=lambda i: i[1], reverse=True)))

    i=0
    for x in freq:
        if printAll:
            i += 1
            print(f"{i}\t{x}\t{freq[x]}")
        else:
            if freq[x] > 1:
                i += 1
                print(f"{i}\t{x}\t{freq[x]}")
    return freq
```

Fungsi tersebut membuat tabel frekuensi n-gram berupa struktur data OrderedDict, yaitu sebuah *dictionary*/*map* dengan pasangan *key-value* berupa substring n-gram dan frekuensi n-gram yang diurutkan menurun berdasarkan frekuensi n-gram. Hasil kemudian dicetak dengan pengkondisian apakah mencetak semua atau hanya n-gram dengan frekuensi lebih dari 1. *Step* yang dimaksud adalah berapa banyak loncatan indeks yang diambil setiap iterasi. Di sini ingin ditemukan frekuensi huruf sehingga n=1 dengan step=1 (dipanggil *substringFreq(string, 1, 1, True)* dengan string yaitu cipherteks). Kemudian hasil tabel frekuensi dicetak sehingga menghasilkan tabel frekuensi dan diproses menjadi grafik batang:

1	W	539
2	C	376
3	J	323
4	F	320
5	N	318
6	X	298
7	K	277
8	L	269
9	Z	211
10	V	178
11	Y	156
12	A	123
13	H	104
14	P	102
15	B	97
16	E	96
17	U	73
18	Q	63
19	G	60
20	O	56
21	R	53
22	S	45
23	I	11
24	T	5
25	M	3
26	D	2



Tabel frekuensi yang dihasilkan dapat dicocokkan dengan tabel frekuensi huruf pada Bahasa Inggris seperti grafik frekuensi huruf pada referensi Cornell Department of Mathematics, 2004:



	E	T	A	O	I	N	S	R	H	D	L	U	C	M	F	Y	W	G	P	B	V	K	X	Q	J	Z
Frequency	12.02	9.10	8.12	7.68	7.31	6.95	6.28	6.02	5.92	4.32	3.98	2.88	2.71	2.61	2.30	2.11	2.09	2.03	1.82	1.49	1.11	0.69	0.17	0.11	0.10	0.07

Karena frekuensi E dan T cukup lebih besar dari frekuensi huruf-huruf selanjutnya, diterka bahwa huruf cipherteks W → e dan C → t. Dari terkaan ini, tersisa banyak pola ‘tZe’ sebanyak 99 kali yang diterka sebagai trigram *‘the’* yang merupakan trigram paling umum di Bahasa Inggris. Sehingga, diterka bahwa huruf Z → h. Karena antara huruf a, o, i, n, s, dan selanjutnya mempunyai frekuensi yang relatif mirip satu sama lain, akan sulit menentukan substitusi huruf murni dari frekuensinya. Sebagai contoh, ketika subtitusi K → a, kombinasinya dengan huruf-huruf e, t, dan h menghasilkan kata-kata yang tidak masuk akal secara semantik dan sintaks di Bahasa Inggris.

Oleh karena itu, dilakukan terkaan melalui semantik dan arti dari kata-kata yang berhasil dibentuk dari huruf yang sudah didekripsi. Dicoba bahwa K → r sehingga kata awal cipherteks menjadi *‘there’*.

```
thereFreUFrNXHLtheXrNeLFLtXQheretheterEUNSNJPXrNPNJFteYXJeV
XXSLtXtheBeENJNJeGreBNIUNSEeFJNJPNJVetXrOFRQhNVeXtherLAVFNE
thehNLtXrNAJXrQePNFJLettVeEeJtXBUNSeJNLQheretheJFEeYerNUeLh
eJAeUNSNJPLQeretheXrNPNJFVYQeVVerLXBUNSeJFVterJFtNUeVRreAXP
JNLeYetREXVXPNLtLLHAhFLFJFtXVRVNOerEFJGXNJttXtheXVYJXrLeQXr
YUNSFEeFJNJPLeFENVetheLGFAeVeBtOetQeeJtQXrXQNJPOXFtLNJAXJUX
RQhNVeXtherLreBertXthethAeJtHrRFJPVXLFIXJGXeEQNYLNthQhNAhre
BerLtXLAFJYNJFUNFJGNrFteLFLQNANJPLrePFrYVeLLPNUeJtheLAFJYNJ
FUNFJLYXENJFJAeXBtheLeFYHrNJPthNLeFrVRGerNXYNtQFLJtVXJPHJtN
VAXJtrFLtNJPJFEeLQereOeNJPXBBereYHGORUFrNXHLXtherAHVtHreLFA
rXLLtheGVFJettheFrFOLLVFULFJYORDFJtNJeLBXreIFEGVeSJeQXBtheL
erFNYerLFLrHLXrrhXLreVFtNJPtXrXQNJPQhNVethePerEFJLVFOeVVeYt
heEFLFLAXEFJJNFLhEeJFVVHYNJPtXtheNrFLhQXXYOXFtLXtherJFtNXJL
```

Metode penerkaan dengan melihat kata-kata Bahasa Inggris umum yang mungkin dibentuk ini diulang hingga didapatkan mayoritas substitusi huruf dengan pengecualian huruf-huruf dengan frekuensi terkecil yaitu I, T, M, dan D atau huruf yang belum terenkripsi berupa x, q, j, dan z. Selama metode penerkaan ini, mulai dipahami konteks dari teks yang berhubungan dengan sejarah dan Viking sekaligus membantu dekripsi melalui kata-kata seperti *period*, *historic*, *overseas*, *nations*, *viking*, *norde*, *campaign*, *kingdom*, *war*, *baltic*, dll.

```
therearevarioustheoriesastowherethetermvikingoriginatedonel
ookstothefemininePrefiIvikmeaninginletorbaywhileothersclaim
thehistoricnorwegiansettlementofvikeniswherethenamederivesh
encevikingsweretheoriginaldwellersofvikenalternativelyrecog
nisedetymologistssuchasanatolylibermanpointtotheoldnorsewor
dvikameaningseamilethespaceleftbetweentworowingboatsinconvo
ywhileothersrefertothethcenturyanglosaIonpoemwidsithwhichre
ferstoscandinavianpiratesaswicingsregardlessgiventhescandin
aviansdominanceoftheseaduringthisearlyperioditwasntlongunti
lcontrastingnameswerebeingofferedupbyvariousotherculturesac
rosstheplanetthearabsslavsandbyDantinesforeIampleknewofthes
eraidersasrusorrhosrelatingtorowingwhilethegermanslabelledt
hemasascomanniashmenalludingtotheirashwoodboatsothernations
suchastheenglishandceltssettledmerelyondanesheathensorpagan
swhilsttheirishreferredtothemasdubgailandfinngaildarkandfai
```

Dekripsi huruf-huruf I, T, M, dan D dilakukan dengan menerka kata-kata istilah yang mungkin berhubungan dengan konteks teks. Untuk I, ditemukan pola ‘anglosaIon’ yang berkemungkinan berupa kata ‘*anglo-saxon*’, yang pada saat itu menduduki daerah Inggris berseberangan dengan para Viking. Sehingga I → x. Untuk T, ditemukan pola ‘thenormanconTuest’ yang dapat berarti ‘*the norman conquest’*, sehingga T → q. Untuk M, ditemukan pola ‘Mudeochristian’ dan ‘Merusalem’ yang dapat berarti ‘*Judeo-Christian’* dan

'Jerusalem'. Dua kata tersebut mempunyai unsur religius sejarah dan berhubungan dengan konteks sejarah teks. Sehingga M → j. Tersisa D → z yang konsisten dengan semua penggunaannya di teks untuk kata *'Byzantine'*.

Dari langkah-langkah sebelumnya dihasilkan pemetaan huruf:

Letter	Frequency	Plain letter
W	539	e
C	376	t
J	323	n
F	320	a
N	318	i
X	298	o
K	277	r
L	269	s
Z	211	h
V	178	l
Y	156	d
A	123	c
H	104	u

Letter	Frequency	Plain letter
P	102	g
B	97	f
E	96	m
U	73	v
Q	63	w
G	60	p
O	56	b
R	53	y
S	45	k
I	11	x
T	5	q
M	3	j
D	2	z

c. Plainteks hasil deskripsi

Dekripsi menghasilkan plainteks:

```
therearevarioustheoriesastowherethetermvikingoriginatedonelookstothefemininepre
fixvikmeaninginletorbaywhileothersclaimthehistoricnorwegiansettlementofvikenisw
herethenamederiveshencevikingswereTheoriginaldwellersofvikenalternativelyrecogn
isedetymologistssuchasanatolylibermanpointtotheoldnorsewordvikameaningseamileth
espaceleftbetweentworowingboatsinconvoywhileothersrefertothethcenturyanglosaxon
poemwidsithwhichreferstoscandinavianpiratesaswicingsregardlessgiventhescandinav
iansdominanceoftheseaduringthisearlyperioditwasntlonguntilcontrastingnameswereb
eingofferedupbyvariousotherculturesacrosstheplanetthearabsslavsandbyzantinesfor
exampleknewoftheseraidersasrusorrhosrelatingtorowingwhilethegermanslabelledthem
asascomanniashmenalludingtotheirashwoodboatsothernationssuchastheenglishandcelt
ssettledmerelyondanesheathensorpaganswhilsttheirishreferredtothemasdubgailandfi
nngaildarkandfairforeignersorquitesuitablynorthmengiventhecommonculturalpractic
eoftormentingcoastalsettlementsandmonasteriesitwasntlonguntilthevikingsfearsome
reputationspreadtoalmostallcornersofeuropeandmesopotamiathereisevenevidencethat
thevikingsreachedbaghdadthecentreoftheislamicempireatthetimethevikingageascommo
nlyreferredtolastedfromtheearlystothenormanconquestofenglandinthroughoutthisper
iodthevikingsusedthenorthernandbalticseastoterroriseneighbouringkingdomsextendi
ngtheirinfluencethroughcombatandcultureuntileventuallyvikingscouldnolongerbemer
elydescribedascoastalraidersconsiderthefactstwovikingkingssweynforkbeardandcnut
thegreatwouldascendtheenglishthroneleiferiksonanearlyicelanderwouldsettleshorti
```

vedcoloniesinnorthamericascandinavianswouldevenserveasmercenariesforthebyzantin
eempireinshortthesewerenomerepiratesbuttheforefathersofapatchworkquiltcultureth
emotivationsforsuchexpansionaresubjecttodebateformodernhistoriansthoughthereare
clearincentivesastowhythepopulationofscandinaviamighthaveactedinthewaythattheyd
idduringthisyearperiodonerelativelyapparentreasonisascarcityofresourcesthusforc
ingthevikingstolookfurtherafieldevenrobbingandkillingclassesofpeopleblessedwith
amorebountifulhomelandanotherpossiblestimulusistheruleofcharlemagneandthereligi
ouspersecutionthatwenthandinhandwithitwithchristianinfluenceseepingeverfurtheri
ntodenmarkswedenandnorwayitmakeslogicalsensethatthevikingswerelookingtoprotectt
heirpaganbeliefsystemresistjudeochristianvaluesandeventakerevengeforthosesettle
mentsalreadylosttoamonotheisticdevotionthisisnotspeculationtheintroductionofchr
istianitywouldcometodividenorwayforalmosthalfacenturycausinguntoldbloodshedandc
ulturaltransformationitshouldalsobenotedthatduringthevikingagescandinaviasclose
stneighbourswereexperiencingvaryinglevelsofinnerturmoilthusgrantingthevikingsan
advantagewhenexploitingtheselandsforwealthslavesorterritorythesearoutesusedbyth
evikingswerealmostentirelyfreeofoppositionleavingtheraidersunimpededastheytrave
lledfromonedestinationofplundertothenextthisbreakdowninwhathadoncebeenaprofitab
lenetworkoftraderoutesforeuropeankingdomscanbeheraldedbackasfarasthecollapseoft
heromanempireinthethcenturyandlatertotherapidthcenturyexpansionofislamicphiloso
phytheendofthevikingagecanbepinneddowntoanumberoffactorsfirstofallthefallouttha
toccurredfollowingthechristianisationofscandinaviawouldhaveuntoldeffectsonthere
gionsdomesticandforeignpolicybythethcenturydenmarknorwayandswedenwereeffectivel
ycontrolledbydioceseslegitimisedbythecatholicchurchandhadfirmlyestablishedthems
elvesasseparatekingdomsthismeantanenormousculturalshiftintheprioritiesofscandin
aviasleadershipinthatsensethevikingswerenotdefeatedbutarguablymadetobehaveinama
nnerthatfitthecivilityoftheirquicklytransforminghomelandsforexamplethemedievalc
hurchmadeitforbiddentotakefellowchristiansasslavesgiventhefactthatslavetradingw
asthenumberonesourceofprofitforthevikingsthisremovedagreatdealoftheeconomicince
ntivetotravelandraidoverseasthenewleadershipalsochosetorefocustheirmilitaryatte
ntionfromthekingdomsofthewestandinsteadpartakeinsuchcampaignsasthebalticwarsand
theattemptedconquestofjerusalemfromhereonoutitseemedthevikingswerenolongerareco
gnisedforceintheworldthoughtheirbrutalitybraveryandstrengthwouldlongberemembere
dbythosewhohadoncefeltthesharpedgeoftheirbattleaxe

Pencarian plainteks di Google mengarahkan ke artikel yang membicarakan mengenai sejarah Viking pada link:

https://guidetoiceland.is/history-culture/vikings-and-norse-gods-in-iceland

Mengutip dari artikel tersebut sekaligus hasil dekripsi dengan tanda baca:

> There are various theories as to where the term "*Viking*" originated; one looks to the feminine prefix 'vík', meaning 'inlet' or 'bay', while others claim the historic Norwegian settlement of Viken is where the name derives (hence, Vikings were the original "dwellers of Viken").
>
> Alternatively, recognised etymologists such as Anatoly Liberman point to the Old Norse word 'vika', meaning 'sea mile', the space left between two rowing boats in convoy, while others refer to the 9th Century Anglo-Saxon poem, *Widsith*, which refers to Scandinavian pirates as "Wicings".
>
> Regardless, given the Scandinavians' dominance of the sea during this early period, it wasn't long until contrasting names were being offered up by various other cultures across the planet. The Arabs, Slavs and Byzantines, for example, knew of these raiders as 'Rus'' or 'Rhōs' (relating to 'rowing'), while the Germans labelled them as *Ascomanni* ("Ashmen"), alluding to their ash wood boats.
>
> Other nations such as the English and Celts settled merely on Danes, Heathens or Pagans, whilst the Irish referred to them as 'Dubgail' and 'Finngail' ('dark' and 'fair foreigners') or, quite suitably, 'Northmen'.

Given the common cultural practice of tormenting coastal settlements and monasteries, it wasn't long until the Viking's fearsome reputation spread to almost all corners of Europe and Mesopotamia—there is even evidence that the Vikings reached Baghdad, the centre of the Islamic Empire at the time.

The Viking Age, as commonly referred to, lasted from the early 790s to the Norman Conquest of England in 1066. Throughout this period, the Vikings used the Northern and Baltic seas to terrorise neighbouring kingdoms, extending their influence through combat and culture until, eventually, Vikings could no longer be merely described as coastal raiders.

Consider the facts; two Viking kings, Sweyn Forkbeard and Cnut the Great, would ascend the English throne. Leif Erikson (an early Icelander) would settle short-lived colonies in North America. Scandinavians would even serve as mercenaries for the Byzantine Empire. In short, these were no mere pirates, but the forefathers of a patchwork-quilt culture.

The motivations for such expansion are subject to debate for modern historians, though there are clear incentives as to why the population of Scandinavia might have acted in the way that they did during this 200 year period. One relatively apparent reason is a scarcity of resources, thus forcing the Vikings to look further afield, even robbing and killing classes of people blessed with a more bountiful homeland.

Another possible stimulus is the rule of Charlemagne and the religious persecution that went hand-in-hand with it. With Christian influence seeping ever further into Denmark, Sweden and Norway, it makes logical sense that the Vikings were looking to protect their pagan belief system, resist Judeo-Christian values and even take revenge for those settlements already lost to a monotheistic devotion. This is not speculation; the introduction of Christianity would come to divide Norway for almost half a century, causing untold bloodshed and cultural transformation.

It should also be noted that during the Viking Age, Scandinavia's closest neighbours were experiencing varying levels of inner turmoil, thus granting the Vikings an advantage when exploiting these lands for wealth, slaves or territory. The sea routes used by the Vikings were almost entirely free of opposition, leaving the raiders unimpeded as they travelled from one destination of plunder to the next.

This breakdown in what had once been a profitable network of trade routes for European kingdoms can be heralded back as far as the collapse of the Roman Empire in the 5th Century, and later, to the rapid 7th Century expansion of Islamic philosophy.

The end of the Viking Age can be pinned down to a number of factors. First of all, the fallout that occurred following the Christianisation of Scandinavia would have untold effects on the region's domestic and foreign policy.

By the 12th Century, Denmark, Norway and Sweden were effectively controlled by dioceses legitimised by the Catholic Church and had firmly established themselves as separate Kingdoms. This meant an enormous cultural shift in the priorities of Scandinavia's leadership; in that sense, the Vikings were not defeated, but arguably, made to behave in a manner that fit the civility of their quickly transforming homelands.

For example, the medieval church made it forbidden to take fellow Christians as slaves. Given the fact that slave-trading was the number one source of profit for the Vikings, this removed a great deal of the economic incentive to travel and raid overseas. The new leadership also chose to refocus their military attention from the kingdoms of the west and, instead, partake in such campaigns as the Baltic Wars and the attempted conquest of Jerusalem.

From here on out, it seemed, the Vikings were no longer a recognised force in the world, though their brutality, bravery and strength would long be remembered by those who had once felt the sharp edge of their battleaxe.

2. Metode Kasiski

a. Berkas cipherteks

```
FSIKTSZDRCZEUGPFPOJWXRKCXVPVOQGSNESTECHYYEGKPCNOZCQMJTSFEVYSZEPXEDCCBGAGAHYHQCX
RUSOKSTJCAUUSZURCEYTMJXDKWHZFEZRLETHHSSLMEQWZMCYCLJNOAZSPLHNGFXESIHSSXCVWOUQSTB
LMEQWZMCYHNYGAERPPPROQPYOYIRNIXGBYOGWKSOZPREZOXRZKTRBFWREYPWYMAIKLXVPZGPTIOZPOV
SYGAWKAXVPOYRNWEGEBOWYYISHIEBTQRYXIETXVPAOBQPAZLSCSOQNREYPOYRIYYPAJWOXCYGEMOREB
OHNCZEFUVWEMUDGLAVSDFZGRVSJGVCFBJRBFWREYPWYZNXWQXFTPKGGMOKWHTAGRRHPNEHECHYYEGKA
ODTUPZIZJYFTBMYAITVPCDWULBJWHSIEMKYEWWMSKSWIFVWWTIFFDZGBROATSCJUJPEJUWIASXTBPYG
RCEVGRVWIUYBEHUZNAETHPWCCLISHIEBTQGQULWYWDCSGBGSDGPTEVKCNVPNJFZAIFVRWZSGZIZFNJN
OGOPJKLDYEZIGFFVPVWETKPPQGSFIEZXICBYMHXPNIGAFKYQSBZLSOIYRGSXKVSNCXBRHQVXCEVKLBV
PNTCWSZFRINATHTCTMPGQXVSOTUPBRACISVOTBGLAJYGEPAPFXNKEQSSJIVPKSIHPFYYOSRKWSLZKTR
PPNISGWJCAGALSIYRGJFSNKMBQCXARWPNIBZHOMAXDGXHSSLMEGAUJHSSKPHTPOSBLBJGGWKIIOYKGT
RWYUYZOOTLVLEREHPZODRMJGXZLBZGFXDOWWYQOBRRPIEIDSJKNWOJIOEVLMYPKCIRMMZFRITZMBNHO
MASBYSAPGVCPMAYEQNCXBVRCZSRYOKTVHATGSEVOQRVQVXWZBGJFSONVOYYZFRRQSFSCCLNRSLRIHZO
HMHXKLXVPHURNPDAQOYDUNHPWZMCYCLRUIAGVHSOZRUEPZMAPOHMHXIOPZTCTNRSLRIOQHKPGLAKVIA
HOMAEYGPRPFGUNWBUVAPRCFVGDZLSYTOJYIZCMHSKGRRVWTHPPQGKRADGXWDBUUXRKCRODHUZNPWQII
AKGPQTNKWGFFKZLXDKQORAGRUEPNEGYCZWRXYUQSZIZANYOKWHSSKKRVCKRQPCLQNQKYMFTGRYAHPNI
FPWYYYWKLSZVZUPREXUYHECHYYEGKMGDOOBUIOGMRLHOKRADKRHSSXCJEOGJOCAKPAEIKHHZPGUUSSK
RHQWYFVRCZSHSSXGIINZSUPHLGFLPUIOEHUZNKAZWOMWMYAHXKEIEWLSYJEYLPFHNCVWOAVDCWYCQXD
GXHSSLGFLYGRHLZQYCTWXIBEZERUIBOWVTGZFRMJIEFYOZGBRKLEDCWTARWOCLCHOYAHVOKHTZFBGBP
WZMBRHNCEYHKWCQHNCXMJMHCXOYYGLWTOMZILMELWBMBRFKJREOKHVPFLPBQPNIQFFYCGLAVVWYQKQF
AWYQOCFERBFWNSKPJKPGLAXIWDCTCCVKSMGPHNYGLWYFSPBGEEIAJYDZBZFRCONSIWRTMGXARPOYMUL
RXDGXHSSVPVRYKWGTGGDVWDLVCXHNCZENXMORSCYFFKXROMCELNQAJWOXCYGEWWSSGTFMPRAETXCLJK
PLLWTHGZAKYAHOZVCYUHMLFQZXVPFKYEIDGFWEGZFNXWSENPSBCECKTIVPORUNCOLISWGNSAKNEEBOB
KTRVOGXWDTOCQEHRXVPTUMQVWZMCYGGPREHCEMDRKTBYNKHKTHNMHXPNIFPGZSAXERSBPRGWFEIUWWC
OYQVKJKHHZRKJVZAXJCZRLMELEYJOEVKPVRPNITTSRBOYPZLSQCUBAIRKVQLAKRBFWGPGZOVNESWILS
OGGKBWEXEBOOYIRHSNIFPHNCSSKJJCCVOKOYPYEAZGOPNHIOXHPRZFNXPNITZCJGFEHXIOOMKYGIJZS
PLKGQIINEEBRFEYAHQTOBZKOLTPUHVSLYYFVWLXSATGKZLWWEMBRGULBJWLMGSGGKBWEXMAXSJGNXAR
CQZAVJNMJKHHZVOQZSPNIFTTNCPEHRIRLGULBJWLMGSHNCCVETGSDGCYFHEYEDACOLGIZHIQLIYCUIN
NYGMOTBUEOHVCVSTRUILXSATGKQUIYXMSOORMGEJJXCWRYYZSOOVHZFALGSPNIVTUNFVPHYYROSTJLZ
AXCVPOBWEEETGOXSJMJRSOXVLHKPEMXRIZTUNRAMJMXVPKGRRVKBIFQZUURHPUHFZKTRUIATXWCSBGY
PWMIHSSVSQHHKXICBKBVRPUEZLYKRUEPOWBZKIYYPAJXCMORYXIPNIBEVKGFPWTHKSSXCFEIUWWCGNC
YXAXMGNORJRHOGQCDWXGFPWTHHSOZQGLANMGECXWBJPUFOWOQCGLWZWGZITGDYAXMUSHODLSQBMGTHZ
MOEHGOSJCAANRBKIZEVKABSHGXAZGVFRVAUJHSSRYXIWIGCXDGLVIZHCPPOARVJQRZWPKYMSWWSSGTF
OQYEJJ
```

b. Langkah-langkah dekripsi

Diketahui bahwa teks dienkripsi dengan *Vigenere cipher* dan pesan ditulis dengan Bahasa Inggris. Pertama-tama, ingin ditentukan panjang kunci *Vigenere cipher*. Untuk mencari panjang kunci ini, dicari kriptogram yang berulang pada cipherteks. Dicoba dicari kriptogram berupa trigram karena pada Bahasa Inggris trigram yang paling sering muncul adalah kata *'the'*. Digunakan *script* yang sama pada bagian sebelumnya dengan pemanggilan fungsi yaitu *substringFreq(string, 3, 1, False)* dengan string yaitu cipherteks. Ini artinya kita mencari substring dengan panjang 3 dan iterasi melangkah dengan step sebanyak 1. Dihasilkan tabel frekuensi trigram seperti berikut:

```
1   HSS 11
2   PNI 11
3   XVP 8
4   HNC 7
5   GLA 6
6   LME 5
7   WZM 5
8   EVK 5
9   ZFR 5
10  YAH 5
11  HYY 4
12  ZMC 4
```

Di sini diambil sampel untuk metode Kasiski dengan trigram ‘HSS’, ‘PNI’, dan ‘XVP’. Selanjutnya, ingin dicari jarak antara setiap trigram yang mengulang ini. Oleh karena itu, dibentuk suatu script untuk membantu pekerjaan ini pada *file* **script.py**.

```python
def allIndexSubstring(string: str, substring: str) -> list[int]:
    """Returns a list of all indexes of a substring in a string."""
    indexes = []
    for m in re.finditer(substring, string):
        indexes.append(m.start())
    return indexes

def differenceArray(array: list[int]) -> list[int]:
    """Returns a list of differences between adjacent elements in an array."""
    diff = []
    for i in range(len(array)-1):
        diff.append(array[i+1]-array[i])
    return diff

def GCDArray(array: list[int]) -> int:
    """Returns the greatest common divisor of all elements in an array."""
    return math.gcd(*array)
```

Fungsi allIndexSubstring mengembalikan semua indeks suatu substring ditemukan pada suatu string. Fungsi differenceArray mengembalikan perbedaan/pengurangan antara satu indeks dengan indeks selanjutnya pada suatu *array*. Fungsi GCDArray mengembalikan *greatest common divisor* untuk semua elemen pada suatu *array*. Ketiga trigram ‘HSS’, ‘PNI’, dan ‘XVP’ diproses melalui fungsi-fungsi ini untuk menemukan *greatest common divisor* untuk jarak masing-masing trigram.

```
index1 = allIndexSubstring(string, "HSS")
index2 = allIndexSubstring(string, "PNI")
index3 = allIndexSubstring(string, "XVP")

diff1 = differenceArray(index1)
diff2 = differenceArray(index2)
diff3 = differenceArray(index3)

gcd1 = GCDArray(diff1)
gcd2 = GCDArray(diff2)
gcd3 = GCDArray(diff3)

print(f'HSS\n{index1}\n{diff1}\n{gcd1}')
print(f'PNI\n{index2}\n{diff2}\n{gcd2}')
print(f'XVP\n{index3}\n{diff3}\n{gcd3}')
```

```
HSS
[115, 145, 755, 765, 1155, 1235, 1275, 1345, 1585, 2295, 2485]
[30, 610, 10, 390, 80, 40, 70, 240, 710, 190]
10
PNI
[592, 712, 742, 1182, 1482, 1792, 1852, 1952, 2072, 2192, 2342]
[120, 30, 440, 300, 310, 60, 100, 120, 120, 150]
10
XVP
[24, 224, 244, 274, 954, 1684, 1754, 2254]
[200, 20, 30, 680, 730, 70, 500]
10
```

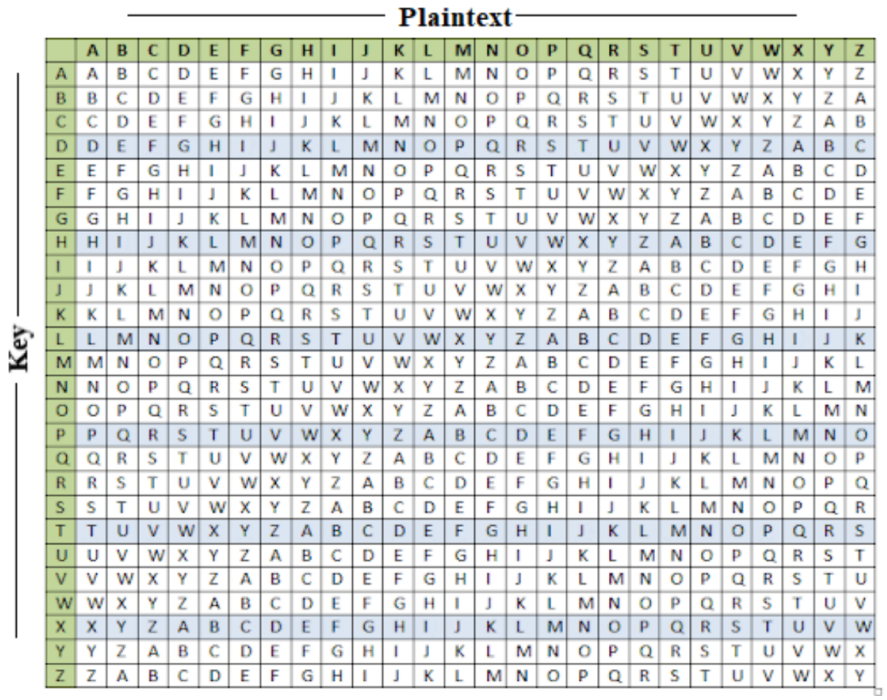
Terlihat bahwa untuk ketiga trigram *greatest common divisor* masing-masing trigram adalah 10 sehingga kemungkinan besar panjang kunci berukuran 10 karakter pula. Selanjutnya, cipherteks dikelompokkan sehingga semua indeks modulo 10 pada kelompok yang sama. Hal ini karena seharusnya semua indeks dengan hasil modulo 10 yang sama dienkripsi dengan suatu huruf kunci yang sama. Sebagai contoh, huruf pada indeks 3 akan dienkripsi dengan kunci yang sama dengan huruf pada indeks 13. Dari 10 kelompok ini ditemukan huruf dengan frekuensi terbesar. Untuk perhitungan huruf paling sering muncul digunakan fungsi mostFrequentLetter pada **script.py**.

```
def mostFrequentLetter(string: str) -> str:
    """Returns the most frequent letter in a string."""
    return max(set(string), key = string.count)
```

```
arr = ["" for i in range(10)]
for i in range(len(string)):
    arr[i%10] = arr[i%10] + string[i]

for i in range(10):
    print(f'{i} : {mostFrequentLetter(arr[i])}')
```

```
0 : R
1 : E
2 : W
3 : K
4 : I
5 : H
6 : P
7 : S
8 : K
9 : Y
```

Dari hasil di atas, huruf yang paling sering muncul pada indeks 0 adalah R, indeks 1 E, indeks 2 W, dan seterusnya. Huruf-huruf ini berpotensi berasal dari huruf ‘e’ sebelum dienkripsi karena ‘e’ adalah huruf yang paling sering muncul pada Bahasa Inggris.

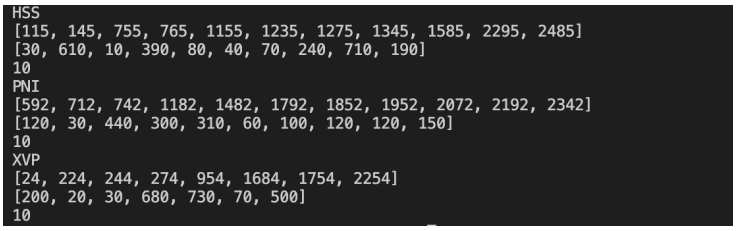


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Perhatikan tabel di atas. Untuk indeks 0, agar ‘e’ dienkripsi menjadi R maka dibutuhkan kunci dengan huruf N. Untuk indeks 1, agar ‘e’ dienkripsi menjadi E maka dibutuhkan kunci dengan huruf A. Untuk indeks 2, agar ‘e’ dienkripsi menjadi W maka dibutuhkan kunci dengan huruf S. Untuk indeks 3, agar ‘e’ dienkripsi menjadi K maka dibutuhkan kunci dengan huruf G. Untuk indeks 4, agar ‘e’ dienkripsi menjadi I maka dibutuhkan kunci dengan huruf E. Untuk indeks 5, agar ‘e’ dienkripsi menjadi H maka dibutuhkan kunci dengan huruf D. Untuk indeks 6, agar ‘e’ dienkripsi menjadi P maka dibutuhkan kunci dengan huruf L. Untuk indeks 7, agar ‘e’ dienkripsi menjadi S maka dibutuhkan kunci dengan huruf O. Untuk indeks 8, agar ‘e’ dienkripsi

menjadi K maka dibutuhkan kunci dengan huruf G. Untuk indeks 9, agar ‘e’ dienkripsi menjadi Y maka dibutuhkan kunci dengan huruf U. Sehingga, dihasilkan kunci dengan panjang 10 huruf berupa ‘NASGEDLOGU’.

Menjalankan program dekripsi *Vigenere cipher* yang sudah dibuat dengan kunci ‘NASGEDLOGU’ menghasilkan plainteks di atas. Dapat terlihat bahwa mayoritas plainteks di atas belum menghasilkan kata-kata yang bermakna dalam Bahasa Inggris. Oleh karena itu, dilakukan perbaikan pada kunci yang didapatkan dengan menganalisis trigram ‘HSS’, ‘PNI’, dan ‘XVP’ dan terkaan bahwa mereka merepresentasikan kata *‘the’*, menimbang indeks mulai mereka.



Perhatikan kembali hasil indeks masing-masing trigram yang dihasilkan sebelumnya. ‘HSS’ selalu mulai di indeks yang kongruen dengan 5 (mod 10). Dengan melihat tabel enkripsi sebelumnya, diterka bahwa di indeks 5 t → H dengan kunci O. Pada indeks 6, h → S dengan kunci L. Pada indeks 7, e → S dengan kunci O. Dengan perbaikan ini kunci menjadi ‘NASGEOLOGU’.

Selanjutnya, PNI selalu mulai di indeks yang kongruen dengan 2 (mod 10). Dengan melihat tabel enkripsi sebelumnya, diterka bahwa di indeks 2 t → P dengan kunci W. Pada indeks 3, h → N dengan kunci G. Pada indeks 4, e → I dengan kunci E. Dengan perbaikan ini kunci menjadi ‘NAWGEOLOGU’.

Terakhir, XVP selalu mulai di indeks yang kongruen dengan 4 (mod 10). Dengan melihat tabel enkripsi sebelumnya, diterka bahwa di indeks 4 t → X dengan kunci E. Pada indeks 5, h → V dengan kunci O. Pada indeks 6, e → P dengan kunci L. Di sini kunci tetap 'NAWGEOLOGU'.

Dijalankan kembali program dekripsi *Vigenere cipher* yang sudah dibuat dengan kunci 'NAWGEOLOGU' yang menghasilkan plainteks:

```
ssmepeoplimeyalreadckrowthehiwtsryoftobelekelocatidmnnorthsymetraprovmngebutforxhsseofyouahsdonotknswxhestoryfelindthefsrqationofpaoetob
athmsximetheriiwsomeinfsrqationthetaillbediwcyssedcurmoysaswhatveeditdownxofalakeissniofthelavgistlakesmnwoutheasxawiaandisevslcanicleki
inthemihdpethereiwarislandcelpedsamosmrmslandthimejorityojtlepopulaxisnaroundxofalakeisfaxaktribemtmsestimaxehthattobelekewasfovmiddurin
genixplosiorojaboutyeerwagowhicliwaneruptmorsupervopcenosuperzopcanothaxiwmounttofaaindblowrvslcanicawhlasspreahtshalftheiavthfromclirat
osoutlajricaeverqyitesurpviwingbecaysiitturnssuxthespreedsfthedusxtsberecorhehuptotherovthpoletleiruptionscgurredfovoreweekanhtledustbuv
sxreachedoipometersebsvesealezeptheevidingefoundapssreinforgewthenotisnxhatthefsrgeoftheevuttionandmtwoceanwazewcouldanrililatelijemnatl
antmsxhisincihertcausedqawsdeathfslpowedbytleixtinctisnsfsomespicmesaccorhirgtodnaezihencethiwevuptionapssshranktlerumberoftespletoabsux
ofthetoxaphumanpotupationofxhiearthatxhettimeabsuxmilliontespleaftevtleeruptisnecalderaaawformedwlighthenfiplidwithwaxevandbecaqeahatisn
oakrownastofapakeupwavdtressurefyxhemagmaxhethasnotcexcomeoutgaysestheeqevgenceofwaqosirislenhthereiselwofolkloveebouttobelekeissaihhisa
idatiqeahenthериwesafarmevnemedtobaahswentfislirgtothermvirtogetfmsltoeattofaketsabigenhbeautifyljishbuthiiwsurprisidxhatthefmslcantalke
ptarentlyxhifishistlemncarnatmorofapringewswhowasguvsedforvmopatingthirylesofthikmngdomasetlankyoufsrlavingrepeesedherfvoqthecursitlepri
ncewsaasmarryxofahowevevtlereisonipvomisethetlasbeenakriedupontlecshouldnstxellanyorexhatthepvircessisajiwhfromthimerriagewesfornaboyraq
edsamosmrwamosirgveaintoavevylandsomeenhstrongbsyfutthereerihabitstlaxamazeevirconehealaacsfeelshynkryandnezevsatisfiidellthefosdvations
aveelwaysdezoyredwithsuxtherestynxilonedacsemosiraswiknedtodepizerfoodfsrlisfathevirthefielhbytthefoohnivercamexofaalsoaptrsachedsaqowir
andasoehwherethifsodforhiqbytsamosivahmittedtlaxthefoodmselreadyeetintobawavviryangryenhunknowirgpybreaksliwpromisefywayingsorojafishsaq
owirimmedmaxelycomppamnedtohiwmstherifhicelledasorojafishthipvincessweshisappoirtidbecausihirhusbanhhesbrokenxhipromisewhicriedalstendto
ldsemssirtorurtsthehighliplsuddenpyzeryheavcreincamedswrwithatevrmblelighxnmngthewaxevoverfloaehtodrownxhientirevmlpagethepydhleturnehir
toalakexhetisnowcelpedtobalekithenthemspandwherisemosirshilxeriscalpehsamosirmspandthatwtlehistorcojtobalakitlatssounmqyerightijysuvisit
tsbelakeyougarfeelthegoslatmospleveofthelekiaccompariidbybeauxijulviewssfwamosiriwlend
```

Melihat ke percobaan plainteks di atas, beberapa kata-kata Bahasa Inggris mulai bermakna seperti *north*, *you*, *human,* dll.

Namun, beberapa kata masih mengandung huruf yang tidak jelas. Yang menjadi perhatian khusus yaitu kata-kata yang masih mengandung huruf acak namun secara keseluruhan dapat dipahami kata yang dimaksud. Kata '*alreadc*' yang bermulai pada indeks 13 dapat diterka sebagai kata *'already'* dengan 'c' pada indeks 19 merupakan kunci yang salah untuk indeks yang kongruen dengan 9 (mod 10). Sehingga, kita dapat memperbaiki kunci dengan mengganti indeks ke-9 agar y → W dengan suatu huruf kunci. Melihat ke tabel di atas, huruf yang menjadi kunci adalah Y. Dengan perbaikan ini kunci menjadi 'NAWGEOLOGY'.

Selanjutnya, kata 'ssme' yang bermulai pada indeks 0 dapat diterka sebagai kata *'some'* dengan 's' pada indeks 1 merupakan kunci yang salah untuk indeks yang kongruen dengan 1 (mod 10). Sehingga, kita dapat memperbaiki kunci dengan mengganti indeks ke-1 agar o → S dengan suatu huruf kunci. Melihat ke tabel di atas, huruf yang menjadi kunci adalah E. Pada akhirnya, didapatkan kunci akhir untuk *Vigenere cipher* yaitu 'NEWGEOLOGY'.

c. Plainteks hasil deskripsi

Dekripsi menghasilkan plainteks:

```
somepeoplemayalreadyknowthehistoryoftobalakelocatedinnorthsumatraprovincebutfor
thoseofyouwhodonotknowthestorybehindtheformationoflaketobathistimethereissomein
formationthatwillbediscussedcuriousaswhatreaditdowntobalakeisoneofthelargestlak
esinsoutheastasiaandisavolcaniclakeinthemiddlethereisanislandcalledsamosirislan
dthemajorityofthepopulationaroundtobalakeisbataktribeitisestimatedthattobalakew
asformedduringanexplosionofaboutyearsagowhichisaneruptionsupervolcanosupervolca
```

nothatismounttobawindblownvolcanicashhasspreadtohalftheearthfromchinatosouthafr
icaevenquitesurprisingbecauseitturnsoutthespreadofthedusttoberecordeduptothenor
thpoletheeruptionoccurredforoneweekandthedustburstreachedkilometersabovesealeve
ltheevidencefoundalsoreinforcesthenotionthattheforceoftheeruptionanditsoceanwav
escouldannihilatelifeinatlantisthisincidentcausedmassdeathfollowedbytheextincti
onofsomespeciesaccordingtodnaevidencethiseruptionalsoshrankthenumberofpeopletoa
boutofthetotalhumanpopulationoftheearthatthattimeaboutmillionpeopleaftertheerup
tionacalderawasformedwhichthenfilledwithwaterandbecamewhatisnowknownastobalakeu
pwardpressurebythemagmathathasnotyetcomeoutcausestheemergenceofsamosirislandthe
reisalsofolkloreabouttobalakeissaidhesaidatimewhentherewasafarmernamedtobawhowe
ntfishingtotherivertogetfishtoeattobagetsabigandbeautifulfishbutheissurprisedth
atthefishcantalkapparentlythefishistheincarnationofaprincesswhowascursedforviol
atingtherulesofthekingdomasathankyouforhavingreleasedherfromthecursetheprincess
wasmarrytobahoweverthereisonepromisethathasbeenagreeduponthеyshouldnottellanyon
ethattheprincessisafishfromthemarriagewasbornaboynamedsamosirsamosirgrewintoave
ryhandsomeandstrongboybuttherearehabitsthatamazeeveryonehealwaysfeelshungryandn
eversatisfiedallthefoodrationsarealwaysdevouredwithouttherestuntilonedaysamosir
assignedtodeliverfoodforhisfatherinthefieldbutthefoodnevercametobaalsoapproache
dsamosirandaskedwherethefoodforhimbutsamosiradmittedthatthefoodisalreadyeatento
bawasveryangryandunknowinglybreakshispromisebysayingsonofafishsamosirimmediatel
ycomplainedtohismotherifhecalledasonofafishtheprincesswasdisappointedbecauseher
husbandhasbrokenthepromiseshecriedalotandtoldsamosirtoruntothehighhillsuddenlyv
eryheavyraincamedownwithaterriblelightningthewateroverflowedtodrowntheentirevil
lagethepuddleturnedintoalakethatisnowcalledtobalakethentheislandwheresamosirshe
lteriscalledsamosirislandthatsthehistoryoftobalakethatssouniquerightifyouvisitt
obalakeyoucanfeelthecoolatmosphereofthelakeaccompaniedbybeautifulviewsofsamosir
island

Bila dicari di Google, plainteks mengarahkan ke artikel yang membicarakan mengenai asal-usul Danau Toba pada link:

https://pradiptadh.wordpress.com/2020/06/25/history-of-lake-toba

Mengutip dari artikel tersebut sekaligus hasil dekripsi dengan tanda baca:

> Some people may already know the history of Toba Lake located in North Sumatra Province. But for those of you who do not know the story behind the formation of Lake Toba, this time there is some information that will be discussed. Curious as what? Read it down!
>
> Toba Lake is one of the largest lakes in Southeast Asia, and is a volcanic lake in the middle there is an island called Samosir Island. The majority of the population around Toba Lake is Batak tribe.
>
> It is estimated that Toba Lake was formed during an explosion of about 73,000-75,000 years ago which is an eruption Supervolcano (super volcano) that is Mount Toba. Wind-blown volcanic ash has spread to half the earth, from China to South Africa. Even quite surprising because it turns out the spread of the dust to be recorded up to the North Pole. The eruption occurred for one week and the dust burst reached 10 kilometers above sea level. The evidence found also reinforces the notion that the force of the eruption and its ocean waves could annihilate life in Atlantis.
>
> This incident caused mass death followed by the extinction of some species. According to DNA evidence, this eruption also shrank the number of people to about 60% of the total human population of the earth at that time, about 60 million people.
>
> After the eruption, a caldera was formed which then filled with water and became what is now known as Toba Lake. Upward pressure by the magma that has not yet come out causes the emergence of Samosir Island.

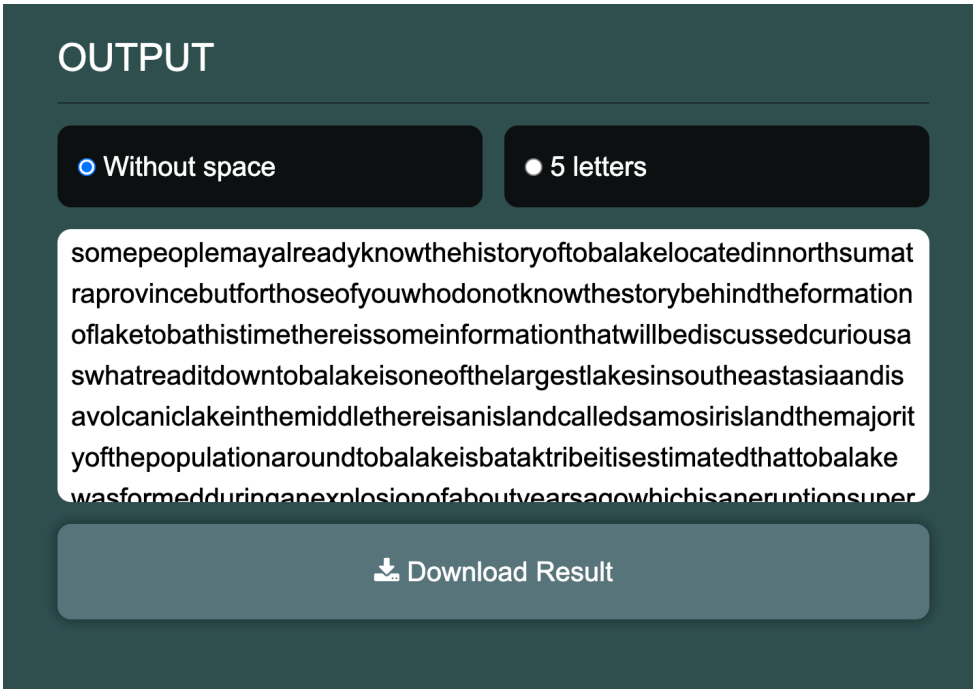
There is also folklore about Toba Lake is, said he said a time when there was a farmer named Toba who went fishing to the river to get fish to eat. Toba gets a big and beautiful fish, but he is surprised that the fish can talk. Apparently the fish is the incarnation of a princess who was cursed for violating the rules of the kingdom. As a thank you for having released her from the curse, the princess was marry Toba. However, there is one promise that has been agreed upon, they should not tell anyone that the princess is a fish.

From the marriage was born a boy named Samosir. Samosir grew into a very handsome and strong boy, but there are habits that amaze everyone. He always feels hungry and never satisfied, all the food rations are always devoured without the rest. Until one day Samosir assigned to deliver food for his father in the field, but the food never came. Toba also approached Samosir and asked where the food for him, but Samosir admitted that the food is already eaten. Toba was very angry and unknowingly breaks his promise by saying "Son of a fish!"

Samosir immediately complained to his mother if he called a Son of a fish, the princess was disappointed because her husband has broken the promise. She cried a lot and told Samosir to run to the high hill. Suddenly very heavy rain came down with a terrible lightning, the water overflowed to drown the entire village. The puddle turned into a lake that is now called Toba Lake, then the island where Samosir shelter is called Samosir Island.

That's the history of Toba Lake, that's so unique right? If you visit Toba Lake you can feel the cool atmosphere of the lake accompanied by beautiful views of Samosir Island.

Berikut dekripsi cipherteks pada program yang dibuat, dengan plainteks terpotong:



3. Kriptanalisis *Playfair Cipher*

a. Berkas cipherteks

```
QUKAROQULALPKHBUSHPLIWIDCSCYGRBAUXSHBUSHAGCFHZQCQBWUZCBKECIVDGFQDGFAEALASHBPKNP
OBLHZFXFMBCFBMEALALXDUGWUZHXDFQFTLUSHKNLVCSANSHXDUGWUVCMOCLCSENMLKFHEQUVFUGZDGD
MBZSCZEMZHXDFQFTIDPWPCGRDQRUQCBLCZGROWVCRVBLHZUQZOSHXKDKFAILKBKGFQKBXDBLBLFBKZC
HHAFTLUIBKZCHUPQMQCTHPWWOEAIVDTQPBUSHQBWUFTLUSHBKIDPWPCCHXKABNVROQUBLCZLGBAQBWU
FTHOSHBLWCHLRVUMSHBPAHCYWCDIBLLAGLCLCKLGDIEMZDLRACPZQBWUEMBKLCZEDMWOFTLCZEMLKFE
MBLCZPWWOQCBLCZGROWYCTKSAMPQUCEBANULEBMSHLELCDGRVAMCHCTHLBAUXDSVCMEOZLGBAEMQBWU
```

FTLCPBCHEMTHPWWOFTILKBLEPKVCMEZEMLKFEMHEQUVFUGZSCZEMBLKBAEPUAKLMHAIDLRAMHZUQXYZ
DLRACUGZDFBBLAKLGDIVCZEPUBUSHONKZFBIGCHCEBATKZFKTLEIOEMZHLUSHIPFQUMPCUMLGOMAHEC
UQBLKBXDEAZSCZEMETACRUGKTDUWVLBTRUXKWCLCUGLENDLBVFUGZSAKWCDIUQUTACNULEALFNQUKZA
HZHZSWCDIOBKXEMZSKBGREHCTNVZSHSCLCVQUHCNKTDDMPCGRIYHDEMMEUGZDFBZSHZUMWOGRKNQUUM
KGALUGDMPCCHLASHBPAHKGRGALUGMEGIDMPCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPM
LUGHPBLAEKLBKMBQCLMMASHDMPCGRIYHDEMMEBQZCBKLUDSCWONKZFBKTRVBLAEKLBKMBQCLMMASHBQ
SHVCPZMERLQEHKGCPUZSAFBFVULERVBLAHPWPCGRIYHDEMPZMQPCABSHUNRUSERUQBWUZDLRCZEMINW
UGRDNMKUGINCZOPBKFTLOPUHEACRUGKTDFTOUSHBQSHVCPZZHZAFNACBPMDHOSHVCMEZEACRUGKTDEM
BLCHFVFTLOPUHEACRUGKTDBLFTBLFSBCFBSHBPAHECUGQUKAZDFBBLFSBCFBEMFAILKBDMPCGRIYHDE
MMHPWPCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLAEKLBKMBQCLMDGALBQZCBK
LUDSTCNUECPKKBBLFTLMDVDSKTHSKBAHCLNYBCFBTRAVPUHEACRUGKTDMBGDDGPZQBWUZDLRACPHZCF
BBLFBBLFSBCFBVCPZZSWDFALCUGURNBCHZFIVDMVCUGINKZFBXDBLFBWZKNPOBLLADSRNZDFBAZKBZS
AHPWPCCHLAQBWUZDLRHSKBSHKTBLACZAIGBGKBTNACMBZSHSLACHBLFHPKHMPOCDLEUGFBWZFTIOKPH
CINCZLGHLKBFTILGHSHKPBGKBSHKTAMPIACZCCHMPBLLAZSHSCLUQSKCKCHFVPURGHLBMSHKCIVHALC
DBBUMOFTFTHOKLLUCFABSHEDGDLCVCXGBUMUSHCQBKMBDXGDGTMDQUHFBILTHSKBGRQVPHHLRAGDDLK
BFTHUKPFQSATEKFSHBIACNUEMLAPCFBBLHSRBBMVLUQEHZFLCUGUMPCSHTKVCZNRUZDFBSHLEIWIUCV
BGHPFRGKACUGVCMEUSRUUMXPKBKAQBWUZDLRHZGRUQKABUSHKTBMSHEHLFBUWUKZKSFTHOKLLCLIACB
IRBBMVLTGACZASAQVDGEADXGDITRBCVFVGRUMBLCZGDGCPUHZALUGBFZAUKPOHSPOACLFGRFTLCPZZS
CZEMMPEHCTRLCNMASHDBBUMOFTLEIOLRWQBGKBFTHOKLIURBCVFVBLFBWQROPWPUEDGDLUSHXDDIEHE
MBMXDIVHMPWQULEZAHCWMRNCHWQRUDSNDLBSHFTGWABLRZHASCHEMGKEMUMBFLEHUKZFBUPIVHAGCUP
SLHPSHKTBMGRKALRVCQBMDQUHFNBKZCHCNGAPULGVAPCGDDLKBFTLCMEWQRBHNMCKPBORVBLFBKCSAN
RRYRGFQNZSHMBETEHIGALUGDCUMRULRZSACNUFTLUPWPCLRUMBLFSBCFBEMXKPWQCBLLABLAKLGDIVC
OHACLUSHDWPCLELUPMLMRVBLHPFTLUSHXDKFCHONKZFBLAKHALUGBLWCHLBMSHLEHCLAFBBLHSACNUQ
CQBWUZDLRHERUUQVUSHQPPUEDGDOUEMLMMLDMBFGRBLFHBKLACQBKMBFTHOMUKBKPKGCHBLLAZSAHPW
PCCHLAAZKBVGACCQEAZANXUNKZACUGIGGUMUFRWUZDLAUMOWBLFBZSHEFHFTUMNRTFUGTKUQZABPLEK
XMBQUHZFTLUIBWCHLBLPUBQFTLUSHXDDIEHEMBMTKRQEMBLKBTRULGISHNBSDKTOMSHTKTFMHQULFZS
KBEAABUWTDIHWCBUGDLRVCMEMVPMBAZARGFQBLFBZSHZCVLMLRAMAKMUALHFFTOUFBRLBUPDRVUMBKM
BSHBPAHEAZANXBLGRHGBUSHDWRVALHFVCPZMOLMHTRUBFLAKBFTODHAFTKBBLFTKCBTABMDLUSHBKVC
MEALTHCSUYLGEDVCMEZDLRAKMWKBFTHOAZFBDGRVAMKSMLBAMEUGQUACEDMILAACDGRVAMHZQPQUOPB
KMWKBBLKBCZKBHZAZFBDGRVAMAFRGZAMEUGCQKIMEUGZHZATGLRAMASNDMELFGRMBBLCZLMHMUMWOZH
ZATGLRAMHECHPZPHHCNZPHHCFTODMWKBCHXDBLQBWUZDLRAKWCBUKBMKBFMHLRAMHZUQXYZDLRCZEMM
PDBFQNXFTLULGBPNVBLLAZSACBAMPSAZAHFALTHHZFTHUBKCLKNPOACEDMILAACUGIUFTFCIUPQQCXD
BFWCUMEACKLSNDCQBPSHIGGUMUXDZSUMALFALMGAUPOPBFQUGVBLFBEMZSCZEMMPRLBKHOSHMLGISHB
PAHCGWUUQUQBFQCBLAHLRAMHECHZERUUQBFQCBLASOBLRCHSHUPBFVCMBPWMDQULFUQBLKBUMPMDSNU
TRALAMEMBMSHCQRBLULERVBLHZAZFBBLQUCZEMKPHLALUGMPZSKBASKLBFIGRGBMKLLCXKFVKBFTOUF
BRVUMMHKZKSZDFBLRVCMSRDBALCKIBLCSYUKBMPANSHDWRVALHFKCSATEKFBLFZZCBKZHZAUGVCNKOZ
DSOCLFUGHCMTCHGRBLASWCBUKLBQCQUPBKBLFZDGRVBLKHBPAZFBKCUGHAMEUGEMLRVCQBWUDGHLUVL
RLGBUSHDWRVALHFBLFZMEVULEBMPOCSBFLEHUKZFBBLKBAEPUAZKBVNLGFQVCQBMUGRBLHZLVCSUIKB
GRZDDKLBSHZGCLHAANLRBLAEPKMBMEGIZDSDEMEHFBPHRVRLFQQUQVEDKLNUSHZHDWUGZDSDEMEHFBA
CRLFQQCAQXQMLBABLABLGUIZDSDEMEHFBALIPFQMPSAQCQVTNACLUSHCQRNBLZDSDEMEHFBACRLFQQV
ZAHFALTHHZBLAEGKBLZDSDEMEHFBBOGRLQNGPUARSHPHVRDZDSLEZEKZFBDCRVRLFQXDBLQVFRGKABS
HZHZABUDZDSLEZEKZFBIUGRIPFQWCUMAQVQNDBLFBBLAEPKMBDMPCCHUPRBLCUGMEVULERVBLKBCZEM
LMLRAMHSMDCSBGHPEHLCUGSHMEGIZDSDEMEHFBHFRVRLFQGRUMQVEHLUSHMUSHBPKCSAROFTHCCKDEL
MHAOWRUMPSAUSGWLEZEKZFBGVGRHGTQZNCHUMSURUBLHZAZFBBLZDFBSHDMPCCHLALGZECHMEVDLRAM
HZUQXYZDLRCZDSVCMHXGFQEMHAKSBLKBKHTFUGSHKCIVHALUSHMUSHBPZDWDLVKBRBRGFQROFTLUSHW
FKPCHWCUVLRLEMBQUHPLSFBALUGTNWCHLRVBLKHBPAZFBDGRVAMAKFTIDHZFTIDABBLAHGHLBECIVDM
TGLRAMHZUQXYZDLRCSIZSHLTFBMPIZSHLTFBOEKPCHBLFZZDLALMMWAHWFLGDIFTLUSHZXKBHZQDMLL
ULERVBLFZIGGUMUVCFASHNRSRRUHABLKBMHKZKSQUGRBLHECHFTLUSHZHZABULIVCNKMHKSUVLRIZLG
OEPOMKRGQUMPBFDSRNXDBLACEDFTHOQDMUBLUPNDLBSHRGHLUVSHRGUVEMOPNBGRHDLRAMHZUQXYZDL
RACUWFAFTOUEMKNGHLBFBCHZDFBZSHZCVBLHZAZFBOUKTEQTRRVBLFZZCBKKNHKUGGVFTLCPECHSHUX
LEBLKBTFSAVCMONFLVKHPZQBWUZDLRHZSHFTOZKBCHDSZDLTFZWCDWSAUMWCBIWCZHMEGIBLCHVCNKM
BSHBQSHUMDIBLASBLLASHBPBAQOMUSHBICLXDZSCHUMLEZASHKIGDHAHURUBLLABLHSRBBMVLBGCLMQ
KTCHSHTIGKACUGBLLAZSHSCLNRFGPUBLCZDSHALCWNBUGDLAMLMBZSHSCLCQRBLUSHPKOUAHDGFQBLC
HVCNKPZMEGIGKWQCUGDMACFAKKTCSCQRNDSBOAKPWPCVLFABLHECHOZEMSZCZFTICRGALUGGKWQCUGD
IAKZKSAZKBVNLGFQBFLAFTODHAFTWQCDFTMBFVXDBLBOFTGWWCZSLMDVFTNAPUUQBLGRQNHZMEGIQBW
UZDLRCZLRLEIVMVZGACNUFTHOSHMBFVCHXDBLBLASZSAFKSRVBLHSWCZHGRPUHCNKPUBLASGRBLASPU
RGFQMBSHZXFBRVUMBLASWCBUKLBQFTIDPWPCCHCQUKPQSKTKUGDQDIGRBLKZAZFBGRHQBLFZKCSATEK

FFTLUSHBUSHPKOBXRSKBICLUMEHBKCLVNSHHGTIVCMEDMBFBLCZDSHALCZQMUSHDQWOOUKTEQVCNBCH
SHTKUGMEGIEHVCBKQCWQRNMBKSOPBLKBZSCZGDHMPWQUFRWUBLLAWQTCBKSHBKEHOBBKUMHAUBPWQUA
KPOKHBTRUBLFSBCFBEHDGAZGRLNLEBMSHLEHCLAFBQBWUZDLRHZSHKTUAWCDIUQUTRUBLGRARLEBMSH
VCMELFGRBLAEPKMBFTLOPMUTACRUGKTDQCLMMLUGZSCZFBRVUMSHTIPWPCGRIYHDEMMEUGMEGIDMPCG
RIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLAEKLBKMBQCLMMLUGBLFHMLPZMEBQZC
BKOWGSBCFBBLWCKTNAKLBKMBQCLMDGZHHERUMWKBBLHSGDHMZDKBABSHZHZAUGVCNKOHZCIVHMUQXYZ
DLRKHPZMBGDMLDGZAFTOUAHMLUGUQBFHPMPECPKEMZSABSHBQSHVCMEMBWCUGCHCQBPSHFRCZBLLABL
AHPWPCGRIYHDEMQBAZKBMQPCAELMZHGVFTHOSHFRCZBLLABLHSRBBMVLBGCLEHUNFVCHSHTKUGBLLAD
GRVAMHZUQXYZDLRCZEMMBGDMLDGZAFTHOPMSHBLWCHLALUGBLWCHLALLFGRDSZOSHPLHLRAGDDLKBCQ
BPMDQULFPZZSCZEMUQRVBLAEKLBKMBGRBLCZDSHAMLUGFBWZHABLKBLEZAUQBKMBFTOUSHBQSHLELCA
MEMRVBLWCHLUMEQPOABLGFQUMOWZSKSKLBUCHSHNKCKACUGIUHZZHILKBZHGADGFAFTMDIOCHHAUXPO
FTFTGUPWQUAKWCDILEZAFRWUBGKBGRBLHPIGQHRDZHZSCZFBUMZANUSHZHZATQWCBUKLBQUMBLHZAZF
BOUKTEQFTICUQKFCHLABLCHPWPUFTODKPCHXKABNVBLGRHQUMZHIVMTKBWFSHKMZANXEDACMILRAMHZ
UQXYZDLRAHPWPCCHWCUMANSHXDUGWUFTODLMHAOWRUDQWOLCVQNQPWWOUWVLUYLEBLLTFZWCUMZHIVD
HPWWOBLGRHQXKABNVBLGRHQZSACBQZCBKHOALVGCKHZQCLMDAMDWCBPFTHOSHORIVHAOWRUQUCZLGED
VCZETKGICHKNPOZFIVDMXUCHFTHUDTHZGDIPVLVGABBLCZPUBLWQDIUWVLRGBUDSNDLBQBWUZDLRACU
GZSCBBTMDBALUSHOWPUFTHUWCHLRVBLKSBKRVNVMLKAOELGDIMEGIBLCSDIUWVLUYLEALKNGHLBWQTD
PWPCDWSADXGDIVMLKAWQROUPSKTINGPUQUKAQBWUZDLRHSCLUQOBMQDKDPBTRUMBPWWOEHCQBKSHTKU
GHABLKBZHGAEHMLKAOULRLBSHBFVDCKHZTRRVBLCSDIUWVLTGCKCHMPONDKAIVFUGMPRLHLAMVNLEBM
UQXYZDLRAHPMBLKBTNACBLFTGCAHDIWUTFPHCGACGUWULKVASHOPMBEHCTRLCNHMKLLUSHONKZFBUMS
HBPAHECUGTKTFVCNFMUDMFQCEBAUXKTHOGRBLKZAZFBGRLNSHZHZAUGVCNKOELVHSPOHERUDSZODSKF
CHBLFZZCBKZDFBBLFZMEVUSHPKHCKTDGRVAMHZUQXYZDLRAHXGFQQUBLFHUPRBLCUGBLLAZSFBKHBLK
BMBPKBKGUPUOPZALCUGZHASCHUMEHHCCLBLFZDGANCHSHNRMKUGEMBLFZMEVULEBMSHVCMHCKCHUMMU
GHLBGVBLFZDCRVBLAHCKHZBLFBZSHEFHFTUMTNACBLACDGRVAMACUGCEBATKZDGDAKLVABMDGKACLFG
RZDFBBLCHVCNKZSACUIZDLALEILKMSKBFLUSHZQKLLUSHMDIOCHHAUXPOFTVCQBPWQUKZAHZHBLFTBL
CZDKFAGOBCFBALFAKCBKFTIDABUQQUAKPOKHUYSHUYACBKUQUVLRGZWCTRRVBLCZDKFAOUPOFTZDFBZ
SHSCLBKCKSHILPOCZFBRLFGUPBUQCBLFHMLPZMEUGEMFAIDPWPCGRIYHDEMMHPWPCGRIYHDEMMPBUSH
VCIVDVDSGRBLHPMLUGHPBLAEKLBKMBQCLMMLUGLRFTOZKBCHEMEHCQBKSDONKZFBBLWCKTNAKLBKMBQ
CLMDGZHHERUMWKBBLHSGDHMZDKBABSHZHZAUGVCNKOHZCIVHMUQXYZDLRKHPZMBGDMLDGZAFTOUAHML
UGUQBFHPMPECPKEMZSCZSHBQSHSHKTLULEALIVDLKBTHPWWONRZSCHUMSHBIACNUXDBLEAKTCQBPSHM
EXOMLGRGVBLLADGRVAMHZUQXYZDLRCZEMFLKLTFDGZATRUBWUZSHZKLIGXDIVMALGRFQCMPSABLGRLN
LEBMLEIVIMRUFTFBLUQWWCFTHUVNSHSHIMQCXDUADETKANZDDKSZSHRBHCBPUMWOZSASCLACQPHPQUW
COEPOTUSHBQSHIGQHRDZHILKBZHGAFTLUPWPCBLHZLESKQCFTMUSHUPDIUWVLBQPMSHZCBUMWKBBLHZ
AZFBOPRBALGRMBMUSHZHZAUGVCNKPEUQKFCHLABLCHPWPUFTODKPCHDQWOBLGRHQUMZHIVDASHKMEDA
CMILRAMHZUQXYZDLRAHPWPCCHWCALUGMEGIDQCVFVDKFTUQAMABFTWQBFDWSAGRHPROQPZHWQCDFTDM
PCMEGIBLCSDIUWVLTFUGORIVHALUSHQPHPQUWCOEPOUSRUFTILAHIGURXPRMHAEMCHBLFHPKHMWUAHM
ALEBMSHHABLKBZHGAEHEHDNGDCHFTOWSKBFLUSHOWPUZDFBBLFZLELOCLACTENIKLBUSHMDOUPOFTME
GIUQXDXDIVDAPONZWCXKPQKBGVCQUPUFKSPWPUDGRVAMHZUQXYZDLRHSCLUQOBMQDKDPTFUGHARVBLC
SDIUWVLUGMCPZZSKSHAEMCHTRBLKTIDZGCLZSKSRUBLAKPORHBGKBLEPKBLFTBLKSPDMPRGRGRVUMPC
AEEAAUFTLUSHHGTIEAIVDIWUBQFBZHHAPZQZWCMKTKDQUQENACRUZQKLLUSHXDKFCHUWVLFNWCKTCHQ
UAEPUUQVCUGZSCZFBALVCZNRUCQNURBLAAHXGUVEMLMOPMBAZFBGRDYSHBUSHZHZAUGVCNKOELVHSPO
CZSHBUSHZQCVQBWUZDLRAHXGFQEMGKHCCLROQUBLFHUPRBLUSHVFUMUFHZBOSKAUCHBLHZBAQOMUSHT
KUGBLFZDMPCCHFTGCWCUGBLKSPDMPBFODPOEZKCUKAHZGCLBLFZALFARGUMRUZDFBQBWUZDLRAKLVAB
SDKBZHGAFTLUMDLUSHOVLEBLCLLEXRSKBFLUSHBUSHZXKTBFILKBQUKAOPBKUMEHROQUSHNITCUIFTL
UPWPQFBBLCHPWPUUMUQQUABSHONKZFBLADSSAZCBUGRKNQUUMANSHHDEMMEUGMEGIDMPCGRIYHDEMMH
PWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLAEKLBKMBQCLMMASHRGALBQZCBKLCZEAEPUCSGSB
CFBBLWCKTNAKLBKMBQCLMDGZHHERUMWKBBLHSGDHMZDKBABSHZHZAUGVCNKOHZCIVHMUQXYZDLRKHPZ
MBGDMLDGZAFTOUAHMLUGUQBFHPMPECPKEMZSCZSHBQSHSHKTLUSHHDEMPZMQACARDBPZZSABBKSTHAL
CUGZSPWPCXDBLTKHFQBWUZDLRHZLEIVDIHKZSAKKPCHAZFBGKLRDWMBMOASVGGKABSHBKROQUZSCZFB
RLBUMCONLRHZAKBKAMQUAHXNPWPOZDKBFBPWQUKZAZKBKCSAFTLUSHBKZSASCLACZANXQPHPQUWCMEX
RMICSRUPHHCLRDMPCCHXKABNVZDLRCZLRLEBKODSHAFMPBLLAAZKBWQBFZDPMCVLRDMFQCHCQKPUTRU
ZDSCZATKBAKMHKKAQCLROTMBOBBKGVIGCZSHBUSHKMMICZEMBKCLZQSHMKGRBAILKBECKAFTIWIUHZZ
HILKBZHGAROEMCKWCBUNXUWVLTFUGMPZSCZFBUMZANUSHZHZATQWCBUKLBQUMBLHZAZFBOUKTEQZSAF
UQKFCHLABLCHPWPUQBWUZDLRKSRUSHBIACOWRUQCBLCZGROWVCUGMEGIDKFTUQAMABFTWQBFGRBLHZA
ZFBOUKTEQLEZACQNTGIHCTQKHRLMEIVMASHMESAUMSAFTOZKBCHBLCZPOFTHPLEIVHMPWQUHFUNGIQC
QVKMMIHZBLKBKHXDIVDHLXFZWCQUFBPMKLHOUQXYZDLRKHLCBKUQRVALFAFTVNLGFQKTFZWCCETKGIQ
CQPHPQUMEGIBLCSDIUWVLTGPWPCDXGDDARUBLACXRMIKHBUUWXPAKHZWQBCLABLKBCHEDKZAFFTIGXD

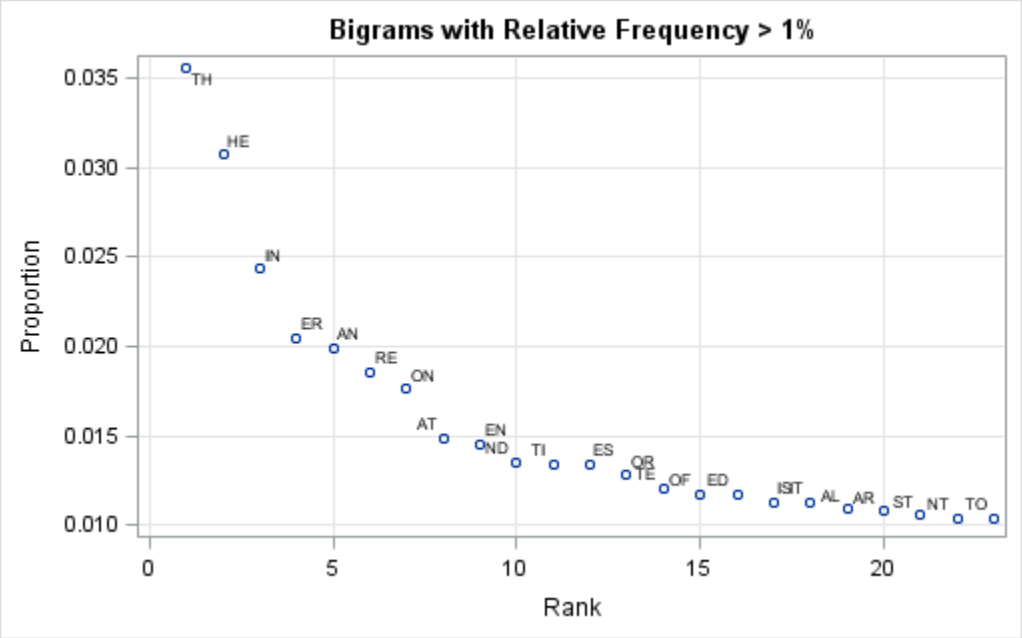
```
IVHALABLCZLGBABLACXRMICZEMMPDCRYRGFQGVVLHCBLLAQUGVBLKBCHEDKZAFVCMQPDMPBFHOUQXYZ
DLRAHQUHFGCPUBLAEGRACXRMIACUGZDFBZSHZCVBLLABLCZPOFTLAKSKTUMKGBMSHDWTDIUHZHPUBMD
QUHFTKUGMBBKUASHOWRUSHBIFTLCUGUMPCBLKSPDMPUQBOLEGATRBLKTIDZGCLZSACRHUMKGRLBGKBO
PRULBLEBQSHEAIVDIWUUGACLUSHBUSHONKZFBDMPCCHLASHUXLRLEIUACGCTDDMPCFTIDCTHLCHLMWC
LCUGMEGIZDLRACPZQBWUBKLCZEDMWOTHCKFCZHUSFNUWWOBLHPRLSABLCHVCNKOEFTUQUVCFFZWCROF
LKLTFUGZDFBZSACPECHQCBLAHPWPCGRIYHDEMMEBLPOAHPWPCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVC
IVDVDSGRBLHPMLUGHPBLAEKLBKMBQCLMDGALBQZCBKLCAMEMUMGSBCFBGRBLHPMLUGBLWCKTNAKLBKM
BQCLMMASHBGKBFBXLWCZSACNULEIUHZBMQCKTEMFTFBXLWCZSACNUKCBGLTKBHZRVBLCHVCNKOZSHBU
SHWFLVHSPOKHBUSHAZFBGRQGWCUGQBWUZDLRAHXGFQROQUBLFHUPRBHOSHTNACBLCHUQDMFQKBFTOUE
MHCCLBLFZDGANCHSHNRMIPWPCCHUMZHCZSHBLKBBLFZDWTDGCGRLCFNBLGRIQPDMPUQBORBMLKAILKB
DWSTCHSHBIKLUXEMSHILKBXDBLVCBATKUGXDBFTRRLUVEMLMDMGFWCZHBLKSPWPUEDGDOUEMHCCLFTI
UASKLBFIWHCCLBLFZMLGISHNRQPTFRHKBFTLCIVHMAZFBQCBLASMEUNWCUGLRFTOUKSNAPUSHTKUGZC
MRBLBKCHFVMHQULNSHBUSHZXKBFHPDFQUMTRNXSHNTRUZSHZRLIVIVDMPCCHEMGKZSCZKBAHLXGRLFU
GMBGDDLCLSHKXBKRVNVBKODSHAFMBSHZQKLOUAKWCDIUQUTRNZGKBGRBLCHKTFIUPRBLCUGBLFZLELC
UNFTMQKTFBUAQCKGUQGQMLPZMOCLHZMULEBMSHDWTDHUHZKZFBKNPOLMHMGIHZFTLUSHVGKLILKBGRL
RFTOUUPBASHNBLVCBQPRGRLFQMDHCTGABBABPFTLULEBMSHVCMEIPFQOHCTHLBANUSHBUSHXQRUBLAK
QCKGUQRUROQUBLASWCBUKLTFUGQUCSANSHVLDVFVPZMBFVCHNZLRFTOULAEDCHLRFTHUPKHOKCSAUMM
CUGZCMRCQBPUQXYZDLRAEPKMBFTWUMASHTFTKZATFUGMLMBCLMWACUGUQZOUQXYZDLRAHFVLMQUHDQU
LNLPKHBUSHDWKYKGTFUGZSCHGIUQUALEFQHERUDMPCCHEMGKZSCZKBACMHKZKSCQBPSHVCMEOZLGBAE
MQBWUEMBKLCZEDMWOFTILKBLEPKVCMEZEMLKFEMHEQUXGBLKMSKBFILWUAZKBBLLACFGRHQMPUFLVKH
BUMUSHCQBKMBFTOUFBRVUMBLCHVCNKZSWCZHUMMQFBLUSHRGHLBLHZCVBLAKQCKGUQBUSHOPRBALGRF
TLUSHEHCTRLCNHMUQXYZDLRCZLRLGRGALUGBKCLZDLAVCOZKPRVBABRQPRGRLFQMDHCTGABBABPBLFB
SHMEGIUMBLCHVCNKMHABSALEZABLAKQCKGRGXDIVDHLXFZWCZDLAAZKBWQCUFTNAPULRTRRVBLCHVCN
KMEBQZCBKOUCZGDGTMUMKNUXDBLLRCQTKIVMASHDQDIGRBLCZPUDIBLFBSHMEGIHAAVHSLTKHALMEHG
ANCQKPKCRYUQAMLXCZLRDSRUZHKHFQQBWUZDLRKHXDIVDLQUWCTKUGXKHXHSKBEMQVHCKTHZRMPMZHP
ZPHQUEMSHMQPCKHBULGOZFVBLFHPWWOOUKTEQUMPCXPNVROQULGVLUGLFZALGVASHDWKYKGTFUGUQVU
SHIPFQPZMPBGCLLRKCKRKPCHCVFVNZLGPZZHTXFTBMQUBLKHBPDSTDHCBPFTIGBLKMSKBFLULERVBLF
ZMBTOTHCHMWKBLABKHZUROQFTOULRLBSHZSWDARSHQPHPQUWCMQHKKAQCKMMICZLGEDQBWUZDLRHSCL
RHRVBAUQKYEKLVCSRUQCSHNUIBMCALUGEHCQBKDMFQZSCSSKBFILKBFZHZDGANCHROBLAHGIQCBLAKQ
CKGBQLAROFTOUEMQUKAOPBKLMLXCSIZSHLTFBOZSHBKLVHPSHKUHKLUSHIPFQPZMPFGTDDMKGQWMEGI
WQTCBKXDBLSAFTLUMDILKBZDLALEILKMSKBFLCUGMEGIGDMWFZWCOPBKBLFTAZKBVNLGFQGRBLCZPUD
IDWSAXDBLSAUMQVECBLKBMQLMCKFZWCZSLMHTASZXGKACUGQBWUZDLRCZEMXDIVDGFQFTOUFBUVLRIZ
LGVLUGBLKHUXCHIGFQVCZSAHOULRLHBKLAZSWUFTHOMIFBOWRNTRBMUQXYZDLRHZXDKFCHMBKSOPBLK
BVCMEHMSUGIHCBUMUSHEAEMUVSHBQSHLELCKRTKZFILKBZHGAGREHCTRLCNDADMBLHZZSCZFBUTAEPU
ABSHDMPCGRIYHDEMMEUGMEGIDMPCGRIYHDEMMHPWPCGRIYHDEMMPBUSHVCIVDVDSGRBLHPMLUGHPBLA
EKLBKMBQCLMMASHHDEMMEBQZCBKOWGSBCFBQCLMDLKBABSHECPKHZALNUBLWCTRRVBLFZWCFQONKZFB
HPECPKKBNZECTKPHUNWUBLFBBLCZDKFAOUPOFTRUBABKLCDCBPACUGVCPZMPXUABEDCHMPRUBATIZXB
KUASHLULEBMSHFRCZUQUVLERVUMOWLAKGBPBMSHUWTDGUMUDQUMBLCZCHIGFQLALMHTRUZSHSCLUQSK
CKACUGOTMBDQUMZHABSHWQRBQYBCFBFTOUSHBQSHZCBUGRZSAFBFZOUQXYZDLRACUGZSHZUMWOMBGDD
VLRIBFLACUGEAKTFTODWCDIUQBMRLNTRUPKQUMHPXSKBPLELCITACGWEHFBORURQPBUSHKGBKFTLUSH
ZXKBHEUPNDLBGRXDBLUMFQMEUGZHUTAEPUHSKBBLFBZSCZEMCQUKCHUMORUMBUSHBKILMUZSSCMEUGL
CUFCBBUGDZSCHUPXRSKIWOWYUHCCLNZINLPPLCKSUFTOUGDSHMV
```

b. Langkah-langkah dekripsi

Diberi informasi bahwa cipher teks ini dapat dipecahkan dengan menggunakan analisis frekuensi kemunculan bigram dalam Bahasa Inggris. Pertama-tama, dibuat *script* program untuk mengetahui frekuensi kemunculan setiap bigram pada cipher teks per blok. Di dapatkan hasil sebagai berikut.

1	BL	296
2	SH	267
3	FT	141
4	UG	139
5	KB	125
6	FB	122
7	HZ	117
8	GR	116
9	CH	116
10	LA	111
11	EM	105
12	LR	102
13	ZD	101
14	LU	99
15	BK	95
16	US	94
17	UM	94
18	LC	92
19	CZ	92
20	ZS	91
21	QU	88
22	MB	85
23	LF	84
24	ME	82
25	UQ	82

Tabel frekuensi yang dihasilkan dapat dicocokkan dengan tabel frekuensi huruf pada Bahasa Inggris oleh Peter Norvig yang menggunakan *library* digital Google, yaitu sebagai berikut.

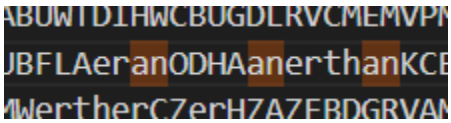


Dengan perbandingan frekuensi bigram di atas, dapat dikatakan bahwa bigram “BL” kemungkinan besar berkorespondensi dengan “th” dan bigram “SH” berkorespondensi dengan “he”. Selain itu, *playfair* cipher menjamin bahwa pasangan huruf pada bigram jika dibalik akan menghasilkan enkripsi dengan huruf-huruf yang sama yang dibalik. Misal, jika “ab” dienkripsi menjadi “XY”, maka “ba” akan dienkripsi menjadi “YX”. Oleh karena itu, diterka bahwa pasangan bigram “KB” dan “BK” berkorespondensi dengan bigram “er” dan “re” yang termasuk bigram dengan frekuensi yang tinggi pada Bahasa Inggris. Kemudian, Dengan asumsi di atas, salah satu konfigurasi matriks *key* yang mungkin adalah sebagai berikut dengan alasan:

- “he” dienkripsi menjadi “SH”, artinya E-H-S berada di kolom yang sama atau di baris yang sama.
- “th” dienkripsi menjadi “BL”, artinya T berada di baris yang sama dengan B, dan L berada di baris yang sama dengan H. Dengan mempertimbangkan alasan pertama, dapat dianggap bahwa T dan L berada di kolom yang sama, sehingga E-H-S juga berada di kolom yang sama.
- “er” dienkripsi menjadi “KB”, artinya E berada di baris yang sama dengan K dan B berada di baris yang sama dengan R.

	R		B	T
	K		E	
			H	L
			S	

Penelusuran lebih lanjut dilakukan pada bigram lain yang memiliki frekuensi tinggi dengan cara mencocokkan frekuensi bigram pada cipherteks dengan statistik. Bigram “FT” pada cipherteks kemungkinan berkorespondensi dengan “in” atau “an” karena frekuensinya cukup tinggi. Setelah percobaan “FT” didekripsi menjadi “in” dan “an”, ditemukan bahwa “an” memiliki kemungkinan yang lebih tinggi karena banyak potongan kata yang lebih masuk akal. Salah satunya adalah sebagai berikut.



Potongan kata “eranODHAanerthan” memberikan pola seperti “er anO DHAner than” dimana terdapat dua kata yang digunakan untuk perbandingan. Kata yang mungkin untuk “DHAner” adalah “cleaner”.

```
/^[A-Z]{3}ANER$/
    CLEANER
    GLEANER
```

Sehingga, didapatkan petunjuk bahwa “OD” berkorespondensi dengan “dc” dan “HA” berkorespondensi dengan “le”. Matriks *key* diperbaharui dengan ketentuan sebelumnya sehingga menghasilkan matriks berikut.

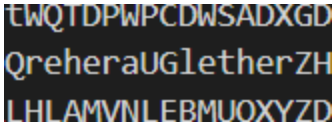
	R		B	T
C	K		E	A
D			H	L
O			S	

Walaupun masih terdapat kemungkinan bahwa setiap baris atau kolom di atas tidak terdapat di posisi yang tepat (bisa di sebelahnya), namun aturan *playfair* tetap berlaku untuk huruf-huruf yang berada di baris/kolom yang sama atau berbeda. Dengan mempertimbangkan posisi antar huruf yang sudah pasti, didapatkan informasi tambahan sebagai berikut.

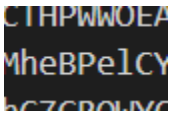
- “ta” dienkripsi menjadi “AL”
- “be” dienkripsi menjadi “EH”
- “ba” dienkripsi menjadi “TE”
- “el” dienkripsi menjadi “AH”
- “ra” dienkripsi menjadi “TK”

Pasangan bigram di atas juga berlaku pada urutan huruf yang dibalik. Setelah beberapa percobaan untuk mengganti bigram-bigram pada cipherteks dengan plainteks, didapatkan potongan-potongan kata yang memberikan petunjuk karena menghasilkan kata yang masuk akal ketika diganti. Beberapa diantaranya adalah sebagai berikut.

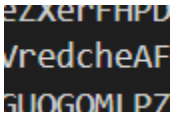
- “aUG” kemungkinan merepresentasikan “and” (“nd” dienkripsi menjadi “UG”)



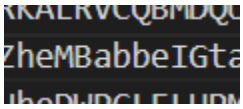
- “heBPelC” kemungkinan merepresentasikan “herself” (“rs” dienkripsi menjadi “BP”)



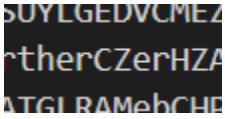
- “redcheAF” kemungkinan merepresentasikan “redcheek” (“ek” dienkripsi menjadi “AF”)



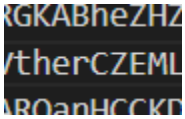
- “MBabbeIGt” kemungkinan merepresentasikan “stabbed it” (“st” dienkripsi menjadi “MB” dan “di” dienkripsi menjadi “IG”)



- “therCZerH” kemungkinan merepresentasikan “there were” (“ew” dienkripsi menjadi “CZ”)



- “therCZEM” kemungkinan mereprentasikan “there was” (“as” dienkripsi menjadi “EM")



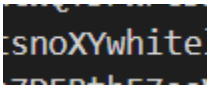
Setelah itu, dengan beberapa percobaan untuk mendekripsi bigram pada cipherteks dengan kunci di atas, didapatkan tabel frekuensi yang baru. Beberapa bigram dengan frekuensi tinggi yang belum didekripsi adalah “FB”, “CH”, “GR”, dan “LR” yang secara berurutan berkorespondensi dengan “en”, “ed”, “in”, dan “it”. Matriks *key* diperbaharui dengan ketentuan sebelumnya sehingga menghasilkan matriks berikut.

W			Z	
U	R	N	B	T

C	K	F	E	A
D	I	G	H	L
O	P		S	M

Konfigurasi huruf pada matriks *key* di atas memberikan informasi tambahan untuk pasangan bigram enkripsi-dekripsi sesuai posisi baris dan kolomnya. Kemudian dilakukan penggantian bigram kembali seperti metode sebelumnya. Metode yang terus dilakukan berulang kali menyisakan potongan kata yang masih terdapat huruf yang belum diketahui posisinya pada matriks, yaitu Q, V, X, dan Y. Salah satu potongan kata yang menarik adalah berikut ini.

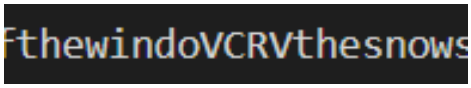
Kata yang cocok dengan pola di atas adalah “once upon a time” karena tidak ada bigram lain yang mungkin, terlebih lagi potongan kata tersebut berada di awal cerita. Artinya, “QU” didekripsi menjadi “on”, dan berlaku untuk “UQ” didekripsi menjadi “no”. Perubahan ini memunculkan potongan kata baru dengan pola yang baik seperti di bawah ini.

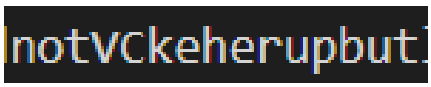


Pola kata di atas cocok dengan kata “snow white”. Perlu diperhatikan bahwa *playfair cipher* mengharuskan jika ada dua huruf yang sama berurutan, maka disipkan “x” diantaranya. Artinya, “XY” dapat didekripsi menjadi “wx”. Dengan demikian, didapat matriks *key* di bawah ini.

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

Kotak terakhir yang kosong diisi oleh V, karena V adalah abjad yang tersisa selain J. Jika kita coba menempatkan V di posisi tersebut, maka dapat dilihat hasil plainteks yang masuk akal dalam Bahasa Inggris. Beberapa contohnya adalah sebagai berikut.





Pola kata-kata di atas secara beurutan sesuai dengan "the window at(x) the snow", "and went into it(x) to rest herself", dan "not wake her up but". Sehingga, didapatkan matriks *key* lengkap seperti di bawah ini.

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

Berdasarkan algoritma *playfair* cipher, matriks akan dilengkapi dengan sisa abjad setelah *key* asli disanitasi (penghapusan huruf duplikat). Pengubahan urutan baris dan kolom secara siklik tidak akan merusak kunci. Oleh karena itu, matriks di atas dapat ditransformasi menjadi dibawah ini dan didapatkan *key* "TURNBACKFELDIGHMOPQSVWXYZ".

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

c. Plainteks hasil deskripsi

Dekripsi menghasilkan plainteks:

```
onceuponatimeinthemidxdleofwinterwhentheflakesofsnowwerefalxlinglikefeathersfro
mtheskyaqueensatatawindowsewingandtheframeofthewindowwasmadeofblackebonyandwhil
stshewassewingandloxokingoutofthewindowatxthesnowsheprickedherfingerwiththenexe
dleandthrexedropsofbloxodfelxluponthesnowandtheredloxokedprettyuponthewhitesnow
```

andshethoughtxtoherselfwouldthatihadachildaswhiteasxsnowasredasbloodandasblacka
sthewoxodofthewindowframesoonafterthatshehadalitxtledaughterwhowasaswhiteassnow
andasredasbloxodandherhairwasasblackasebonyandshewasthereforecalledlittlesnowxw
hiteandwhenthechildwasbornthequexendiedafterayearhadpassedthekingtooktohimselfa
notherwifeshewasabeautifulwomanbutproudandhaughtyandshecouldnotbearthatanyonexe
lseshouldsurpassherinbeautyshehadawonderfullookingxglassandwhenshestoodinfronto
fitandlookedatherselfinitandsaidlookingxglassloxokingxglassonthewalxlwhointhisl
andisthefairestofallthelookingxglassansweredthouoquexenartxthefairestofallthens
hewasxsatisfiedforsheknewthatxtheloxokingxglassxspokethetruthbutsnowwhitewasgro
wingupandgrewmoreandmorebeautifulandwhenshewasxsevenyearsoldshewasasbeautifulas
thedayandmorebeautifulthanthequeenherselfandoncewhenthequeenaskedherlookingxgla
ssloxokingxglassloxokingxglassonthewalxlwhointhislandisthefairestofallitanswere
dthouartfairerthanallwhoareheredyqueenbutmorebeautifulstillisxsnowwhiteasiwee
nthenthequeenwasxshockedandturnedyelxlowandgrexenwithenvyfromthathourwheneversh
eloxokedatsnowwhiteherheartheavedinherbreastshehatedthegirlsomuchandenvyandprid
egrewhigherandhigherinherheartlikeaweedsothatshehadnopeacedayornightshecalxleda
huntsmanandsaidtakethechildawayintotheforestiwillnolongerhaveherinmysightkillhe
randbringmebackherheartasatokenthehuntsmanobeyedandtookherawaybutwhenhehadxdraw
nhisknifeandwasabouttopiercesnowwhitesinnocentheartshebegantowexepandsaidahdear
huntsmanleavememylifeiwillrunawayintothewildforestandnevercomehomeagainandasxsh
ewassobeautifulthehuntsmanhadpityonherandsaidrunawaythenyoupoxorchildthewildbea
stswilxlsoxonhavedevouredyouthoughtheandyetitseemedasifastonehadbexenrolxledfro
mhisheartsinceitwasnolongernexedfulforhimtokillherandasayoungboariustxthencamer
unxningbyhestabbeditandcutoutitsheartandtoxokittothequeenasproxofthatthechildwa
sdeadthecookhadtosaltxthisandthewickedquexenateitandthoughtshehadeatenthehearto
fsnowwhitebutnowthepoorchildwasallaloneinthegreatforestandsoterrifiedthatshelox
okedateveryleafofeverytrexeanddidnotknowwhattodothenshebegantorunandranovershar
pstonesandthroughthornsandthewildbeastsranpastherbutdidhernoharmsheranaslongash
erfeetwouldgountilitwasalmosteveningthenshesawalittlecottageandwentintoitxtores
therselfeverythinginthecotxtagewasxsmallbutneaterandcleanerthancanbetoldtherewa
satableonwhichwasawhitecoverandsevenlitxtleplatesandoneachplatealitxtlespoonmor
eovertherewereresevenlitxtleknivesandforksandsevenlittlemugsagainstthewallstoodse
venlittlebedsxsidebysideandcoveredwithsnowwhitecounterpaneslittlesnowxwhitewass
ohungryandthirstythatsheatesomevegetablesandbreadfromeachplateanddrankadropofwi
neoutofeachmugforshedidnotwishtotakeallfromoneonlythenasshewassotiredshelaidher
selfdownononeofthelittlebedsbutnoneofthemsuitedheronewastoxolonganothertooshort
butatlastshefoundthatxtheseventhonewasrightandsosheremainedinitsaidaprayerandwe
ntxtoslexepwhenitwasquitedarktheownersofthecotxtagecamebacktheyweresevendwarfsw
hoduganddelvedinthemountainsfororetheylitxtheirsevencandlesandasitwasnowlightwi
thinthecotxtagetheysawthatsomeonehadbexenthereforeverythingwasnotinthesameorder
inwhichtheyhadleftitthefirstsaidwhohasbeensitxtingonmychairthesecondwhohasbeene
atingoffmyplatethethirdwhohasbeentakingsomeofmybreadthefourthwhohasbeeneatingmy
vegetablesthefifthwhohasbeenusingmyforkthesixthwhohasbexencutxtingwithmyknifeth
eseventhwhohasbexendrinkingoutofmymugthenthefirstlookedroundandsawthatxtherewas
alittleholeonhisbedandhesaidwhohasbeengetxtingintomybedtheotherscameupandeachca
lledoutsomebodyhasbexenlyinginmybedtoobuttheseventhwhenhelookedathisbedsawlittl
esnowxwhitewhowaslyingasleepthereinandhecalxledtheotherswhocamerunningupandthey
criedoutwithastonishmentandbroughtxtheirsevenlitxtlecandlesandletthelightfalxlo
nlittlesnowxwhiteohxheavensohxheavenscriedtheywhatalovelychildandtheyweresoglad
thatxtheydidnotwakeherupbutletherslexeponinthebedandtheseventhdwarfsleptwithxhi
scompanionsonehourwitheachandsogotthroughthenightwhenitwasmorninglittlesnowxwhi
teawokeandwasfrightenedwhenshesawthesevendwarfsbutxtheywerefriendlyandaskedherw
hathernamewasmynameisxsnowwhitesheansweredhowhaveyoucometoourhousesaidthedwarfs
thenshetoldthemthatherstepmotherhadwishedtohaveherkilledbutthatthehuntsmanhadsp
aredherlifeandthatshehadrunforthewholedayuntilatlastshehadfoundtheirdwellingthe
dwarfsxsaidifyouwilltakecareofourhousecoxokmakethebedswashsewandknitandifyouwil
lkexepeverythingneatandcleanyoucanstaywithusandyoushallwantfornothingyessaidsno

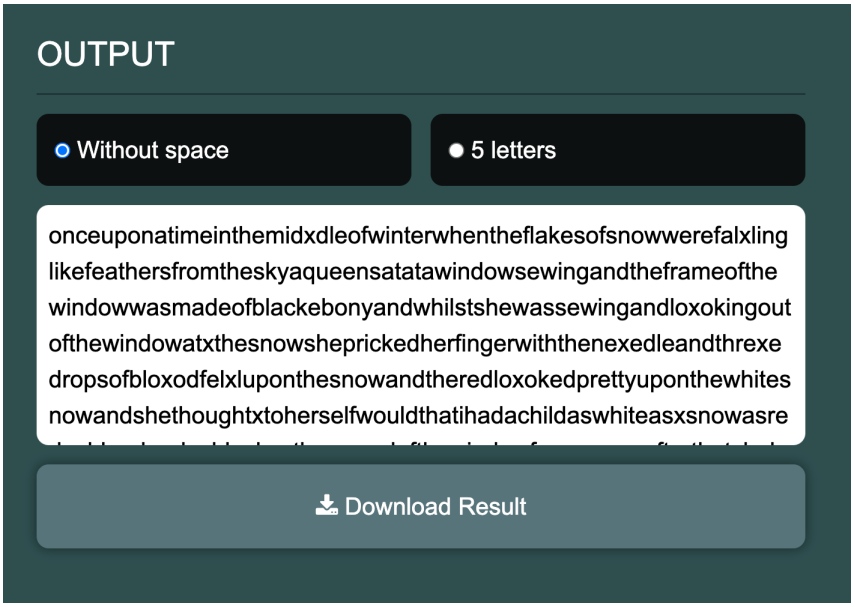
wwhitewithalxlmyheartandshestayedwiththemshekeptxthehouseinorderforthemin themor
ningstheywentxtothemountainsandloxokedforcopperandgoldinthexeveningstheycamebac
kandthentheirsupxperhadtobereadythegirlwasalonethewholedaysothegooddwarfswarned
herandsaidbewareofyourstepmothershewillsoxonknowthatyouareherebesuretoletnoxone
comeinbutthequeenbelievingthatshehadeatensnowwhitesheartcouldnotbutthinkthatshe
wasagainthefirstandmostbeautifulofallandshewentxtoherloxokingxglassandsaidlooki
ngxglassloxokingxglassonthewalxlwhointhislandisthefairestofallandtheglasxsanswe
redohqueenthouartfairestofalliseebutoverthehillswherethesevendwarfsdwelxlsnowxw
hiteisxstillaliveandwellandnoneissofairasshethenshewasastoundedforsheknewthatth
eloxokingxglassneverspokefalselyandsheknewthatthehuntsmanhadbetrayedherandthatl
itxtlesnowxwhitewasstillaliveandsoshethoughtandthoughtagainhowshemightkillherfo
rsolongasxshewasnotxthefairestinthewholelandenvyletherhavenorestandwhenshehadat
lastxthoughtofsomethingtodoshepaintedherfaceanddressedherselflikeanoldpedlerwom
anandnoxonecouldhaveknownherinthisdisguiseshewentoverthesevenmountainstotheseve
ndwarfsandknockedatthedoxorandcriedprettythingstoselxlverycheapverycheaplittles
nowxwhiteloxokedoutofthewindowandcalledoutgooddaymygoxodwomanwhathaveyoutoselxl
goxodthingsprettythingssheansweredstaylacesofallcoloursandshepulxledoutonewhich
wasbraidedfromyelxlowredandbluesilkimayletthe worthyoldwomaninthoughtsnowwhitean
dsheunboltedthedoorandboughtxthepretxtylaceschildsaidtheoldwomanwhatafrightyoul
oxokcomeiwillxlaceyouproperlyforoncesnowwhitehadnosuspicionbutstoxodbeforeheran
dletherselfbelacedwiththenewlacesbutxtheoldwomanlacedsoquicklyandsotightlythats
nowxwhitelostherbreathandfelldownasifdeadnowiamthemostbeautifulsaidthequexentoh
erselfandranawaynotlongafterwardsinthexeveningthesevendwarfscamehomebuthowshock
edtheywerewhentheysawtheirdearlitxtlesnowxwhitelyingonthegroundandthatsheneithe
rstirrednormovedandseemedtobedeadtheyliftedherupandastheysawthatshewaslacedtoot
ightlytheycutxthelacesthenshebegantobreathealitxtleandafterawhilecametolifeagai
nwhenthedwarfsheardwhathadhappenedtheysaidtheoldpedlerwomanwasnoxonexelsethanth
ewickedqueentakecareandletnoonecomeinwhenwearenotwithyoubutxthewickedwomanwhens
hehadreachedhomewentinfrontoftheglasxsandaskedloxokingxglassloxokingxglassonthe
walxlwhointhislandisthefairestofallanditansweredasbeforeohquexenthouartfairesto
falliseebutoverthehillswherethesevendwarfsdwelxlsnowxwhiteisxstillaliveandwella
ndnoneissofairasshewhensheheardthatalxlherbloxodrushedtoherheartwithfearforshes
awplainlythatlitxtlesnowxwhitewasagainalivebutnowshesaidiwilxlthinkofsomethingt
hatshalxlputanendtoyouandbythehelpofwitchcraftwhichsheunderstoodshemadeapoisono
uscombthenshedisguisedherselfandtoxoktheshapeofanotheroldwomansoshewentoverthes
evenmountainstothesevendwarfsknockedatthedoxorandcriedgoodthingstoselxlcheapche
aplittlesnowxwhiteloxokedoutandsaidgoawayicannotletanyonecomeinisupposeyoucanlo
oksaidtheoldwomanandpulxledthepoisonouscomboutandhelditupitpleasedthegirlsowell
thatsheletherselfbebeguiledandopenedthedoorwhentheyhadmadeabargaintheoldwomansa
idnowiwilxlcombyouproperlyforoncepoxorlitxtlesnowxwhitehadnosuspicionandletxthe
oldwomandoasxshepleasedbuthardlyhadsheputthecombinherhairthanthepoisoninitxtook
effectandthegirlfelxldownsenselesxsyouparagonofbeautysaidthewickedwomanyouaredo
nefornowandshewentawaybutfortunatelyitwasalmosteveningwhenthesevendwarfscamehom
ewhentheysawsnowwhitelyingasifdeaduponthegroundtheyatoncesuspectedthestepmother
andtheylookedandfoundthepoisonedcombscarcelyhadtheytakenitoutwhensnowwhitecamet
oherselfandtoldthemwhathadhapxpenedthentheywarnedheroncemoretobeuponherguardand
toxopenthedoxortonoonethequexenathomewentinfrontoftheglassandsaidlookingxglassl
oxokingxglassonthewalxlwhointhislandisthefairestofallthenitansweredasbeforeohqu
eenthouartfairestofalliseebutoverthehillswherethesevendwarfsdwelxlsnowxwhiteisx
stillaliveandwellandnoneissofairasshewhensheheardtheglassxspeakthusxshetrembled
andshoxokwithragesnowwhiteshalxldieshecriedevenifitcostsmemylifethereuponshewen
tintoaquitesecretlonelyroxomwherenoxonexevercameandthereshemadeaverypoisonousap
xpleoutsideitlookedprettywhitewitharedcheeksothateveryonewhosawitlongedforitbut
whoeverateapieceofitmustsurelydiewhentheapplewasreadyshepaintedherfaceandxdress
edherselfupasacountrywomanandsoshewentoverthesevenmountainstothesevendwarfsshek
nockedatthedoxorsnowwhiteputherheadoutofthewindowandsaidicannotletanyoneinthese
vendwarfshaveforbiddenmeitisalxlthesametomeansweredthewomanishalxlsoxongetridof

myapplesthereiwilxlgiveyouonenosaidsnowxwhiteidarenotxtakeanythingareyouafraido
fpoisonsaidtheoldwomanloxokiwillcuttheapxpleintwopiecesyoueattheredchexekandiwi
lxleatthewhitetheapxplewassocunxninglymadethatonlytheredchexekwaspoisonedsnowxw
hitelongedforthefineapxpleandwhenshesawthatthewomanatepartofitshecouldresistnol
ongerandstretchedoutherhandandtookthepoisonoushalfbuthardlyhadsheabitofitinherm
ouththanshefelxldowndeadthenthequexenlookedatherwithadreadfullookandlaughedalou
dandsaidwhiteasxsnowredasbloodblackasebonywoodthistimethedwarfscannotwakeyouupa
gainandwhensheaskedoftheloxokingxglassathomeloxokingxglassloxokingxglassonthewa
lxlwhointhislandisthefairestofallitansweredatlastohqueeninthislandthouartfaires
tofallthenherenviousheartheadrestsofarasanenviousheartcanhaverestxthedwarfswhent
heycamehomeintheeveningfoundsnowwhitelyinguponthegroundshebreathednolongerandwa
sdeadtheyliftedheruploxokedtoseewhethertheycouldfindanythingpoisonousunlacedher
combedherhairwashedherwithwaterandwinebutitwasallofnousethepoxorchildwasdeadand
remainedxdeadtheylaidheruponabierandalxlsevenofthemsatrounditandweptforherandwe
ptthreedayslongthentheyweregoingtoburyherbutshestilxlxlookedasifshewerelivingan
dstillhadherpretxtyredcheekstheysaidwecouldnotburyherinthedarkgroundandtheyhada
transparentcoffinofglasxsmadesothatshecouldbesexenfromallsidesandtheylaidherini
tandwrotehernameuponitingoldenlettersandthatshewasakingsdaughterthentheyputthec
offinoutuponthemountainandoneofthemalwaysxstayedbyitandwatcheditandbirdscametoo
andweptforsnowxwhitefirstanowlthenaravenandlastadoveandnowsnowxwhitelayalonglon
gtimeinthecofxfinandshedidnotchangebutlookedasifshewereaslexepforshewasaswhitea
ssnowasredasbloodandherhairwasasblackasebonyithappenedhoweverthatakingssoncamei
ntotheforestandwentxtothedwarfshousetospendthenighthesawthecoffinonthemountaina
ndthebeautifulsnowxwhitewithinitandreadwhatwaswritxtenuponitingoldenlettersthen
hesaidtothedwarfsletmehavethecoffiniwilxlgiveyouwhateveryouwantforitbutxthedwar
fsansweredwewillnotpartwithitforalxlthegoldintheworldthenhesaidletmehaveitasagi
ftforicanxnotlivewithoutseeingsnowwhiteiwilxlhonourandprizeherasmydearestposses
xsionashespokeinthiswaythegoxoddwarfstookpityuponhimandgavehimthecofxfinandnowt
hekingsxsonhaditcarxriedawaybyhisxservantsontheirshouldersandithappenedthatxthe
ystumbledoveratreestumpandwiththeshockthepoisonouspieceofapplewhichsnowwhitehad
bitxtenofxfcameoutofherthroatandbeforelongsheopenedhereyesliftedupthelidofthec
offinsatupandwasoncemorealiveohxheavenswhereamishecriedthekingsxsonfullofioysaid
youarewithmeandtoldherwhathadhappenedandsaidiloveyoumorethaneverythingintheworl
dcomewithmetomyfatherspalaceyoushallbemywifeandsnowwhitewaswilxlingandwentwithx
himandtheirweddingwasheldwithgreatshowandsplendourbutsnowxwhiteswickedstepmothe
rwasalsobiddentothefeastwhenshehadarxrayedherselfinbeautifulclothesshewentbefor
ethelookingxglassandsaidlookingxglassloxokingxglassonthewalxlwhointhislandisthe
fairestofalltheglassansweredohqueenofallherethefairestartthoubutxtheyoungquexen
isfairerbyfarasitrowthenthewickedwomanutteredacurseandwasxsowretchedsoutterlywr
etchedthatsheknewnotwhatxtodoatfirstshewouldnotgototheweddingatallbutshehadnope
aceandmustgotoseetheyoungqueenandwhenshewentinsheknewsnowxwhiteandshestoodstill
withrageandfearandcouldnotstirbutironslippershadalreadybeenputuponthefireandthe
ywerebroughtinwithtongsandsetbeforeherthenshewasforcedtoputontheredhotshoesandd
anceuntilshedropxpedxdowndeadbygrimmiacobandwilhelm

Teks dengan tanda baca yang lengkap ditemukan di artikel berikut:

https://fairytalez.com/little-snow-white/

Berikut dekripsi cipherteks pada program yang dibuat, dengan plainteks terpotong:



4. Kriptanalisis *Hill Cipher* dengan *known-plaintext attack*

a. Berkas cipherteks

```
TFJOXUPOUXYTTRDSXQMONIYPEUFJDQUBGIMOCJQTNBEHCZEKROVBNTWLMVXMOWZLUCHOXYGSKBQGUAO
BQZKIXYJIETSWVXHVKCUAOTOFYIZAKJGXKAWGQTRVFDZAJNQDUIWZCMYWNFIUPYMCZXIAKYUCQIAZPI
QMGAMGUAKKKHMWKDUXQDUAAKYOWEHLJPWYFKXSARBLLHGAJKTQNTRTPWSCIZASCGSLKVDHTUZSWBNBT
JGYYUPQMFSYZAUTOQCDNGQMFSRLRTUWEMKADIVYLTJKFHLKJUWTSSHMHJFGTRIBYIDAHQEPMPIQCROW
DYRYZNSPNOJHQVKKTOCBPNFAJNLYJZNVBAYJWRGMCHJPWBDHHTPOXSIJVQWDMSIGMTRVEVXDILKVAYT
NUNJXEZLAPGYETRVZNVHSVWLGICDXQFOALDVPASUSYXPFHUWTILUQHTJQVGWFSPAEKBRBNIINYKHNTN
UKJVDHVLXQKUZNVQXUOZZOJZYNPIVYSVFVTZMMUUPWTGHRIOWCBKZYAGUMRCKHIQZSIGISPGBXPYXMO
AWGAGHQVUWTEIGPBMOMBWIOPQEVKMRQATNBMILHHLVUXGMOUWTZCLBKGWIJHFRNGOSCMUHDWHBB
```

b. Langkah-langkah dekripsi

Diberi informasi bahwa *Hill cipher* mengenkripsi 3 karakter setiap kali enkripsi sehingga dibutuhkan matriks kunci 3x3, serta bahwa pesan mempunyai awalan ‘Hello Captain Haddock’ (atau dihilangkan tanda baca dan huruf kapital ‘hellocaptainhaddock’). Informasi ini dapat dieksploitasi untuk memecahkan suatu cipherteks *Hill cipher* dengan *known-plaintext attack*.

Kunci suatu Hill cipher dapat dicari dengan memanfaatkan invers modulo matriks untuk menghitung plainteks ke cipherteks. Ingat bahwa persamaan matriks enkripsi adalah:

$$C = KP \ (mod\ 26)$$

dengan C adalah cipherteks, K adalah kunci, dan P adalah plainteks. Persamaan matriks ini dapat diputar balik sehingga dapat dicari kunci bila diketahui plainteks dan cipherteks:

$$K = CP^{-1} (mod\ 26)$$

Untuk mendapatkan matriks kunci dengan dimensi 3x3, diperlukan pula plainteks dan cipherteks dengan dimensi 3x3. Sebelumnya telah diketahui bahwa teks diawali dengan awalan plainteks ‘hellocaptainhaddock’ yang berkorespondensi dengan awalan cipherteks ‘TFJOXUPOUXYTTRDSXQM’. Maka dari itu, kita dapat mengambil 9 karakter pertama plainteks ‘hellocapt’ dan cipherteks ‘TFJOXUPOU’ untuk dijadikan matriks C dan P dengan setiap 3 karakter direpresentasikan sebagai satu baris pada masing-masing matriks. Huruf-huruf diubah menjadi bentuk numeriknya dengan A=0. Sebagai catatan, semua perhitungan matriks menggunakan https://matrixcalc.org/ serta Python untuk perhitungan modulo.

$$C = \begin{bmatrix} T & O & P \\ F & X & O \\ J & U & U \end{bmatrix} = \begin{bmatrix} 19 & 14 & 15 \\ 5 & 23 & 14 \\ 9 & 20 & 20 \end{bmatrix}$$

$$P = \begin{bmatrix} H & L & A \\ E & O & P \\ L & C & T \end{bmatrix} = \begin{bmatrix} 7 & 11 & 0 \\ 4 & 14 & 15 \\ 11 & 2 & 19 \end{bmatrix}$$

Kemudian, dicari invers modulo dari matriks P terhadap modulo 26:

$$P^{-1} = \frac{1}{det(P)} Adj(P) \bmod 26$$

dengan $det(P) = 2631$ dan $2631^{-1} \equiv 21 \ (mod\ 26)$. Serta,

$$Adj(P) = \begin{bmatrix} 236 & -209 & 165 \\ 89 & 133 & -105 \\ -146 & 107 & 54 \end{bmatrix}$$

Maka invers dari P,

$$P^{-1} = 21 \times \begin{bmatrix} 236 & -209 & 165 \\ 89 & 133 & -105 \\ -146 & 107 & 54 \end{bmatrix} \bmod 26 = \begin{bmatrix} 16 & 5 & 7 \\ 23 & 11 & 5 \\ 2 & 11 & 16 \end{bmatrix}$$

Sehingga kunci K dapat dipecahkan,

$$K = CP^{-1} \ (\text{mod } 26) = \begin{bmatrix} 19 & 14 & 15 \\ 5 & 23 & 14 \\ 9 & 20 & 20 \end{bmatrix} \times \begin{bmatrix} 16 & 5 & 7 \\ 23 & 11 & 5 \\ 2 & 11 & 16 \end{bmatrix} \bmod 26 = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$$

Bila matriks tersebut dijadikan bentuk string dengan panjang 9 karakter maka kunci adalah ‘GYBNQKURP’. Dengan kunci ini, cipherteks dapat didekripsi menggunakan program *Hill cipher* yang telah dibuat.

Namun, perlu diperhatikan cara kerja program *Hill cipher* yang menambah *padding* apabila panjang pesan tidak kelipatan 3. Oleh karena itu, informasi pada akhir pesan yaitu huruf *n* pada "Tintin" terisi dengan 3 karakter lainnya, yaitu 'pmn', akibat perkalian matriks kunci dengan cipherteks yang mengandung *padding*. Sifat ini sudah dikonfirmasikan ke *Hill cipher* lain pada situs daring yang beberapa bahkan memotong huruf *n* terakhir.

c. Plainteks hasil deskripsi

Dekripsi menghasilkan plainteks:

```
hellocaptainhaddocknewzealandprimeministerjacindaardernwontheheartsofmuslimsacr
osstheglobewhenshewearingaheadscarfcomfortedthefamiliesofvictimsofthemassacrein
twomosquesbyawhitesupremacistinchristchurchinlastthursdaysheagainastonishedanev
enlargeraudiencewithherabruptresignationalthoughshestandsagreatchancetowintheup
comingelectioninoctoberthemotheroffouryearoldnevetearohaarderngayfordhasundoubt
edlymadeanameforherselfasaniconofstatesmanshipshehasplayedarolemodelofaleaderwh
onotonlydoesherbestforhernationbutalsoknowswhentofadeawaytoensureasustainablesu
ccessionshecouldhavesoughtathirdtermbutsheshowssheisnothungryforpowertintipmn
```

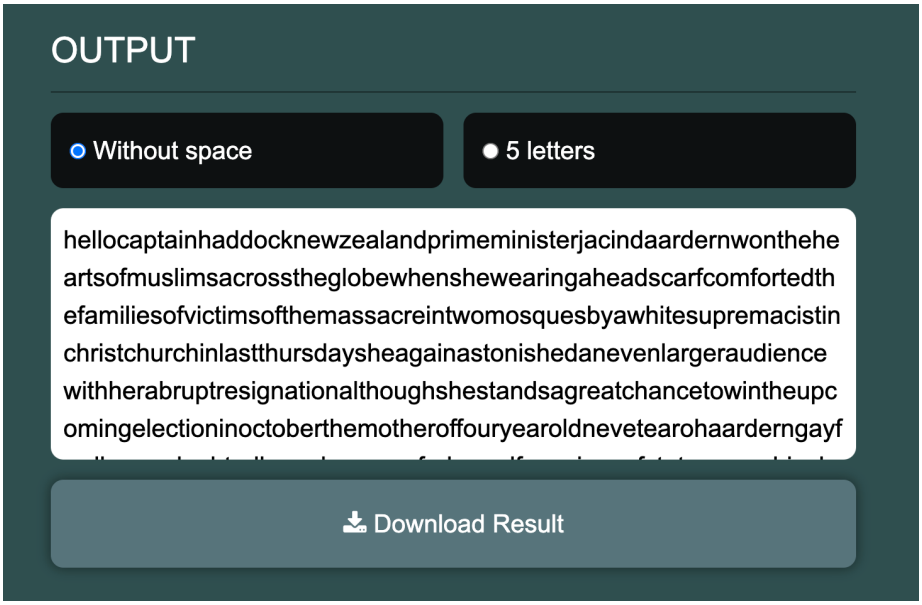
Dekripsi teks menunjukkan bahwa teks dikutip dari sebuah artikel yang membicarakan mengenai perdana menteri New Zealand, Jacinda Arden, pada link:

https://www.thejakartapost.com/opinion/2023/01/24/new-zealand-story.html

Dibentuk plainteks dengan tanda baca yang lengkap berdasarkan artikel:

> Hello, Captain Haddock.
>
> New Zealand Prime Minister Jacinda Ardern won the hearts of Muslims across the globe when she, wearing a headscarf, comforted the families of victims of the massacre in two mosques by a white supremacist in Christchurch in 2019. Last Thursday, she again astonished an even larger audience with her abrupt resignation, although she stands a great chance to win the upcoming election in October.
>
> The mother of four-year-old Neve Te Aroha Ardern Gayford has undoubtedly made a name for herself as an icon of statesmanship. She has played a role model of a leader who not only does her best for her nation, but also knows when to fade away to ensure a sustainable succession. She could have sought a third term, but she shows she is not hungry for power.
>
> Tintin.

Berikut dekripsi cipherteks pada program yang dibuat, dengan plainteks terpotong:


OUTPUT
Without space
5 letters
hellocaptainhaddocknewzealandprimeministerjacindaardernwonthehe
artsofmuslimsacrosstheglobewhenshewearingaheadscarfcomfortedth
efamiliesofvictimsofthemassacreintwomosquesbyawhitesupremacistin
christchurchinlastthursdaysheagainastonishedanevenlargeraudience
withherabruptresignationalthoughshestandsagreatchancetowintheupc
omingelectioninoctoberthemotheroffouryearoldnevetearohaarderngayf
Download Result

Tabel Kelengkapan

Bagian A

No	Spek	Berhasil (✓)	Kurang berhasil (✓)	Keterangan
1	Vigenere standard	✓		
2	Auto-Key Vigenere Cipher	✓		
3	Extended Vigenere Cipher	✓		Hanya support encoding ASCII (256 karakter)
4	Affine Cipher	✓		Mendukung 26-huruf alfabet dan ASCII (256 karakter)
5	Playfair cipher	✓		
6	Hill Cipher	✓		
7	Bonus: Enigma cipher			Tidak dikerjakan

Bagian B

No	Spek	Berhasil (✓)	Kurang berhasil (✓)	Keterangan
1	Kriptanalisis Cipher Abjad-Tunggal	✓		
2	Metode Kasiski	✓		
3	Kriptanalisis Playfair Cipher	✓		
4	Kriptanalisis Hill Cipher	✓		

REFERENSI

Linton, Tom (2001). "Relative Frequencies of Letters in General English Plain text". Central College. Cryptography (Spring ed.).

Math Explorers' Club (2003). "Frequency table". Cornell Department of Mathematics. Available at: https://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html (Accessed: January 29, 2023).