Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчёт**

по пятой лабораторной работе

Студент: Пицуха Я. А.

ФИТ 3 курс 4 группа

Минск 2020

1. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

• выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков) созданных на основе алфавита языка.

1 вариант, белорусский язык; Маршрутная перестановка (маршрут: запись – по строкам, считывание – по столбцам таблицы; параметры таблицы – по указанию преподавателя); Множественная перестановка, ключевые слова – собственные имя и фамилия.

Исходный текст:

Яны ішлі праз лес глухой, замеценай снегам дарогай, на якой не было ні чалавечага следу, ні каляіны, ні нават знаку ад капыта ці полаза. Тут, мусіць, і ўлетку не часта ездзілі, а цяпер, пасля доўгіх лютаўскіх мяцеліц, дык і ўсё зараўняла снегам, і каб не лес — елкі ўперамежку з хмызам, — які няроўна расступаўся па абодва бакі, пакідаючы ўсярэдзіне вузкую белую крывуліну, дык было б і не здагадацца, што тут дарога. І ўсё ж яны не памыліліся. Углядаючыся праз голы, затуманены прыцемкамі хмызняк, Рыбак усё больш пазнаваў гэтую пуцявіну, якую ён памятаў яшчэ з восені, калі пад нагамі плюхалі лужыны, а ў лесе густа церушыў лістапад і восеньскі вецер імжыў наўкола нудным сцюдзёным дажджом. Тады іх чалавек пяць з групы Смалякова неяк пад вечар таксама прабіралася па гэтай дарозе на хутар, і таксама каб раздабыць харчу, ну і яшчэ адпачыць і пасушыцца ў цяпле. Вунь якраз і знаёмы равок, які доўгім крутабокім языком выцягнуўся да самай дарогі, і тая, ухінаючыся ад яго, брала ўлева, у хмыззё, і неўзабаве знікала ў алешніку, праглынутая змрокам. Тут яны сядзелі тады ўтрох і курылі, чакаючы, пакуль двое, што пайшлі на хутар, не пададуць сігнал ісці следам. Цяпер, аднак, у равок было не ўлезці — з берага звісала намурованая мяцеліцай снегавая застрэха, голыя дрэўцы на схіле з суччам патанулі ў снезе.  
  
Над вяршаллем хвой угары лёгка слізгаў вышчарблены маладзічок месяца, які амаль не свяціў, толькі ледзь бліскаў у імглістым ззянні, аздабляючы змрочнае без зор неба. Але з ім было неяк весялей, нібы хтось жывы рупна праводзіў іх у гэтай дарозе. У лесе ж наўдаль было змрачнавата, няпэўна ад цьмянае мешаніны ельніку, нейкіх плямаў, галля, аднак паблізу, на чыстай белі снегу, няблага ўгадвалася дарога. Тое, што яна аказалася зусім без следу, па цаліку, хоць і давала працы нагам, але засцерагала ад нечаканасцяў: наўрад ці хто будзе пільнаваць іх тут, у гэтай глушэчы марознай начы. Тым не менш Рыбак усё ж асцярожнічаў, асабліва пасля няўдалага заходу ў Гліняны, дзе яны, пэўна, трапілі б у рукі немцаў, калі б не адзін дзядзька, сустрэты імі з дровамі. Дзядзька, дзякуй яму, папярэдзіў, што пад вечар у вёску наехала немцаў, і яны павярнулі ў лес, да гэтага хутара.  
  
Зрэшты, выпадковай сутычкі Рыбак не асабліва і баяўся, тым болей у лесе ці нават у полі — у іх была зброя. Праўда, трохі малавата назбіралася патронаў, ды і то няблага: тыя, што асталіся на Гнілым балоце, аддалі ім усе лішкі са сваіх таксама болей чым небагатых запасаў. Цяпер, не лічачы пяці штук у вінтоўцы, Рыбак меў яшчэ тры абоймы ў кішэнях кажушка, столькі ж было ў Сотнікава. Шкада, не знайшлося ніводнай гранаты, але і то не бяда — пад ранак яны ўжо будуць у лагеры. Прынамсі, павінны быць. Праўда, Рыбак адчуваў, што яны трохі бавіліся, ісці трэба было б шпарчэй, снег быў не дужа глыбокі, месцамі добра спрасаваны завеяй, але падводзіў напарнік.  
  
Увесь час, пакуль яны ішлі лесам, за спіной Рыбака чуўся прыглушаны прастудны кашаль, які гучаў часам бліжэй, часам далей, а цяпер вось дык і зусім прыціх нешта. Каторы ўжо раз Рыбак азірнуўся і збавіў кроку — Сотнікаў ледзь прыкметна варушыўся ззаду ў лясным сутонні. Рыбак не гукнуў яго і не падагнаў, толькі, прыцінаючы ў душы нецярпенне, хвілін пяць глядзеў, як той прыстала шкандыбае па снезе ў сваіх тоўстых стаптаных бурках. Да таго ж ён нешта незнаёма і нязвыкла сутуліўся, апусціўшы голаў у глыбока насунутай, з апушчанымі краямі пілотцы, і, калі падышоў, стала чуваць яго разгарачанае труднае дыханне, з якім той не мог саўладаць, нават спыніўшыся.  
  
— Ну, як? Цярпіма?  
  
— Так, — няпэўна махнуў рукой Сотнікаў і ямчэй закінуў за плячо вінтоўку. — Далёка яшчэ?

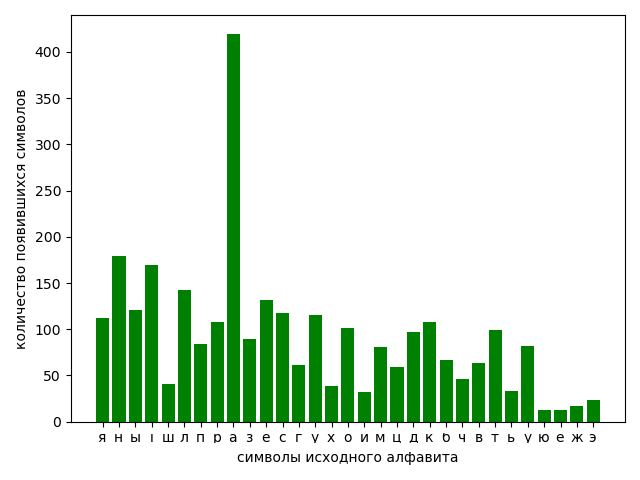
Зашифрованные текста (Маршрутная перестановка, Множественная перестановка):

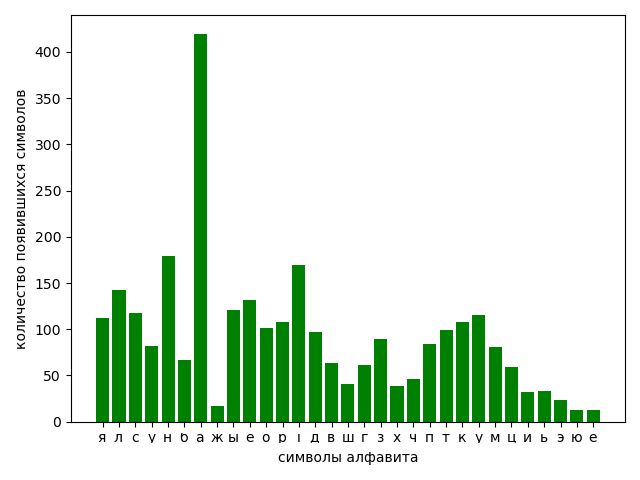
я, лсўн баажыае о рас іўадврш г аалланізіе ех сзч рпеватыр ікабагсаказуанск слаа лтасмаеа цазс ня і цаўбргем:онлру лууурнеўхшоайсоывў яйўарч , наыі ладм зія зас цнбмтміеаеая бвцпцхаіеаетгўндлоа а і ткйіцбыр аухосвйд кно ззуессеа ген п—анепа мьгісс салаодквьўтаіан.нр яа іов вцкгезаяаацацпўйесье ,рт рл рі,еніэх дамх нз жатеьяы,у кў тлпо г,ірйно чы алуакнўы чмекягые о э тблдтпныараяал эйц онў ів уцг андылшрін уту ыншушчмаэкыа ч ўлссыусацх явюімв едлаізчзернзаё отагнззодаы нўу мсац с уйыўлдч , еачн лджааряудмчыс,ж ыбн оп.аынма кмі.тт аымсктнмеуаау ўтлдлн ояыіеяні шнніўмчіых еэ., сн чнштрнае рыілзрыб аеы анв.бакае  
аб вк  
кона н йетпаум ядсыгзц ё уньв ўка яж нкзр куу шаіў гасш арлцэядулянг перяокымох а ж іпсхнк ымвіантаочжеалйау я ўшпцку,каіог ад ваа,апарс го ыаснлн бтааеллоўзяёіл,акгвь . какт па іота п лудсажьт лс к,вілбі езяы,мчг л уаанопсрўя рі ўўыцтвд цьаыасі,кшлон счатаіаагню мраічўаб кыл лза епеавўтрнха каыо.дуб д у імушшнра кыеалўа ла днчадгаеасзл,цсяіі ят чннрапояеп акн ее ызнзгм,нндэе аезтсдй,іаязш лйцелхі а ов,д,ясі а няларяы і ок,ннцзі і яе пвпп аэояенмўдцрааннь, лаа хь,йгпу латнтгясаеррдлр аазя,спне віаўдіялт,о ціы ўті ,ягаўб кік, а хс улт ат еолмор йюалуі т ьк паккітрўаі оысб н ск лентіремеахадц л ззабамдьўя яа ,дшцбб акеылк алціа—ніьсл дц кіпы,ха аб аўбдадр еычунр ку еап ,і наі маа нгдксўулз нс ііяеёісннз т ыезяыд ашмзўўрч яж аэздосў зз внаяьбаяднкуілпнадхааі,у ч, цтсы сьонцау ўеьзсусг дт таіарлым бэах,плтг аяыесісю рт учіыакшым.паы і тбцз па цмзрннар ыые однх ўчра л номбецавсусяеаір п м,к—лбі а ее.пхе.з а.л дв квззідіуояна нрдн ўь зытп нь аеяекбгркбаыоара,ц ма. ьжез д. ж аз ёкіляпну екр з уанзнзйўе а дшхёіяатмммм,аыы у з б,рнары ыемалпбз,воаан о пка—кня ё ,ерамя яэдакякдч ік зуі івів н еўанядс,ўяроя ,зоўлш вўгетшынійоткам, ол п аркная аріднссуб ыустыв тта етуубхчрлпотаоіакорхўўіс іссмьу яя б, яжва пзыёвааывсіп кыклуао уісбмр сцо уняідвпа,ўвыне шацахіы я ас бгплцганраіокуа ліўвнта,соерў ядмэ п зцбуадіаа каўў гі ,блдсі ыыаахілбюм оочауя кый нба гы ўдэ шнсатппаярааасройвруэг ячндідрэуз,анйті ру,аніол йе зіс, те н ва.ўезуя г з,ул ак ебпуулсыуюхе,ўш іс чбнеднаеа аенлюж ыуч гдмюынэуі сатж кяўаакр дг рыааагавдл ляу ьхымля убіігбто ноыакпу,лріі, оа,л б . одрз  
мтыам  
ецклрзсы аарц,б чэа ыўншміллаті,оевы ва,дкбат оа ,авблі ,ырі у па н на пехядса мпкпдзыэорыдзўвашазнасогёайаўа, в,д аса аідунсц тытцнцы ааеьчзл,ўмкаа зяів шан ечтбаряуоаеыйв в б,атема цу екаьтзш л нанеядіне гакі поранаа олысдрга аваа ебоз.ўллдг ьізаіанвір ліаўаўек чсшуінаён, ан і бпажкнаае уеяр я,йўнтн ксірыпіяку рх,.дна   
негпт  
а ллыуепыямв анм едмуабсыытўоьхла,л аія ечнл гйаніза сесмлу,,ярл .оялпз к,еа уа скягмаеукл.д лія нцьмдтаі аук ятют нноч паыйыяав снбаіняылтше і л псзуімряу оад,плгзз ое енлссглаіааоі мўл ч—,лыты а,асузд дт аазыаі ца йхсьтў п,утббі мреыннаоллоанхіайве анісзрты нбы кербспугоапрруякыыы,.анцл іеінпчўм,ярушк баўыачлўссмаадяяікга . аа,п  
хю р  
мчўты—ыыгрг з,аолнн дхууяпвіш,каа а ,клмня уааыкрлсл ?ыьяап б врцаддааякватср оратпуео уіс,гндмё аана ш.зы?бт б   
оотік  
л ора—ьпеаш ша,лат й алапшшськалтя,,зіо н пя—аняак вантіна ар яўх огп уануэгткачўэааўантрз,ўау,а ю лдчм наыаапес сху яіанцп муяазт ўвдуоб іас лрндініууумяжк,ц бэо ьблййя еа, ксзг суі ачоюгс:ат нл снёаетаінлдымк уя апі,,дўас а мцпшліяіате т ойяасц ,мўлаа ч елсаэядіт йшакац чмулязэ.,іпа секзцхярі яо нвпцнвуоеьаоўср с е,ігьзн н аіадід ,далып нвыклкаам яакл ічл,аб оі аз уплувп росіараціндацемт вы, оно пўакнаркг адыуабгдц.мыааі ілмлх— о,і п ндлнаіеаюелмшлх е тёаў уакллзс.аіеае зс кялццлашуіеітчж ршоэы—акр?н гіы  
ыза

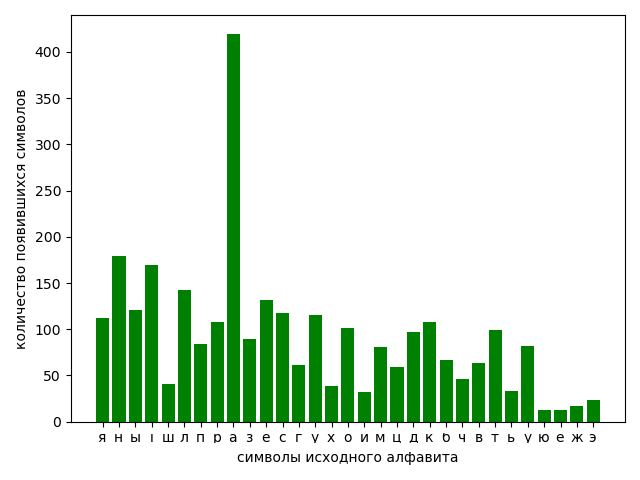
нпыйцсазшзалгаі нгс ноееер ,е м лайу іяхмл

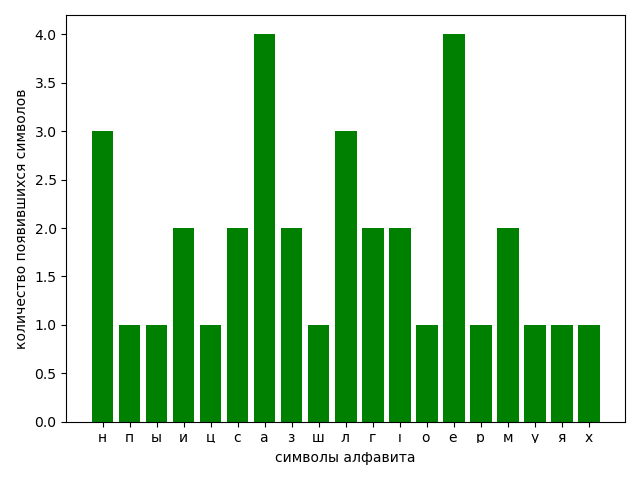
Расшифрованный текст полностью сопадает с исходным. С полными текстами можно ознакомиться в прилогаемых документах.

• формировать гистограммы частот появления символов для исходного и зашифрованного сообщений:

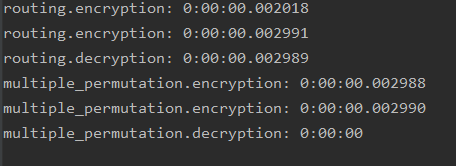








• оценивать время выполнения операций зашифрования/расшифрования



Листинги приложения:

from datetime import datetime  
import matplotlib.pyplot as plt  
  
ALPHABET = 'абвгдеёжзійклмнопрстуўфхцчшыьэюя'  
  
  
def routing(action, source):  
 start\_time = datetime.now()  
 alphabet = list(set(source))  
 cipher\_text = ''  
 table = [[], [], [], [], [], []]  
 source\_alphabet\_dict = {}  
 substance\_alphabet\_dict = {}  
 if action == 'encryption':  
 line\_number = 0  
 element\_number = 0  
 for s in source:  
 if s in ALPHABET:  
 if s in source\_alphabet\_dict:  
 source\_alphabet\_dict[s] += 1  
 else:  
 source\_alphabet\_dict[s] = 1  
 if element\_number != 601:  
 table[line\_number].append(s)  
 element\_number += 1  
 else:  
 line\_number += 1  
 element\_number = 1  
 table[line\_number].append(s)  
 for v0, v1, v2, v3, v4, v5 in zip(table[0], table[1], table[2], table[3], table[4], table[5]):  
 value = v0 + v1 + v2 + v3 + v4 + v5  
 cipher\_text += value  
 print('routing.encryption: ' + str(datetime.now() - start\_time))  
 fig, ax = plt.subplots()  
 plt.bar(list(source\_alphabet\_dict.keys()), source\_alphabet\_dict.values(), color='g')  
 ax.set\_ylabel('количество появившихся символов')  
 ax.set\_xlabel('символы исходного алфавита')  
 plt.show()  
 elif action == 'decryption':  
 line\_number = 0  
 for s in source:  
 if s in ALPHABET:  
 if s in substance\_alphabet\_dict:  
 substance\_alphabet\_dict[s] += 1  
 else:  
 substance\_alphabet\_dict[s] = 1  
 if line\_number != 6:  
 table[line\_number].append(s)  
 line\_number += 1  
 else:  
 line\_number = 0  
 table[line\_number].append(s)  
 line\_number += 1  
 v\_list = []  
 for v in table:  
 for e in v:  
 v\_list.append(e)  
 cipher\_text = cipher\_text.join(v\_list)  
 print('routing.decryption: ' + str(datetime.now() - start\_time))  
 fig, ax = plt.subplots()  
 plt.bar(list(substance\_alphabet\_dict.keys()), substance\_alphabet\_dict.values(), color='g')  
 ax.set\_ylabel('количество появившихся символов')  
 ax.set\_xlabel('символы алфавита')  
 plt.show()  
 return cipher\_text  
  
  
def multiple\_permutation(action, source, keyword1, keyword2):  
 start\_time = datetime.now()  
 alphabet = list(set(source))  
 cipher\_text = ''  
 table = []  
 table\_true = []  
 table\_true\_second = []  
 columns\_second = []  
 dict\_column = {}  
 dict\_column\_index = {}  
 dict\_row = {}  
 dict\_row\_index = {}  
 for i in range(0, len(keyword2)):  
 table.append([])  
 for i in range(0, len(keyword1)):  
 columns\_second.append([])  
 source\_alphabet\_dict = {}  
 substance\_alphabet\_dict = {}  
 if action == 'encryption':  
 line\_number = 0  
 element\_number = 0  
 for s in source:  
 if s in ALPHABET:  
 if s in source\_alphabet\_dict:  
 source\_alphabet\_dict[s] += 1  
 else:  
 source\_alphabet\_dict[s] = 1  
 if line\_number != len(keyword2):  
 if element\_number != len(keyword1):  
 table[line\_number].append(s)  
 element\_number += 1  
 elif line\_number != len(keyword2) - 1:  
 line\_number += 1  
 element\_number = 1  
 table[line\_number].append(s)  
 for s, l in zip(keyword2, table):  
 dict\_row[s] = l  
 for j in keyword2:  
 Ai = ALPHABET.index(j)  
 dict\_row\_index[Ai] = j  
 for e in range(0, len(ALPHABET)):  
 if e in dict\_row\_index.keys():  
 table\_true.append(dict\_row[dict\_row\_index[e]])  
 for ri, row in enumerate(table\_true):  
 for ei, element in enumerate(row):  
 columns\_second[ei].append(element)  
 for s, l in zip(keyword1, columns\_second):  
 if s in dict\_column.keys():  
 dict\_column[s + '2'] = l  
 else:  
 dict\_column[s] = l  
 for j in keyword1:  
 Ai = ALPHABET.index(j)  
 if Ai in dict\_column\_index.keys():  
 dict\_column\_index[Ai + 0.1] = j  
 else:  
 dict\_column\_index[Ai] = j  
 for e in range(0, len(ALPHABET)):  
 if e in dict\_column\_index.keys():  
 table\_true\_second.append(dict\_column[dict\_column\_index[e]])  
 if e + 0.1 in dict\_column\_index.keys():  
 table\_true\_second.append(dict\_column[dict\_column\_index[e + 0.1] + '2'])  
 v\_list = []  
 for v in table\_true\_second:  
 for e in v:  
 v\_list.append(e)  
 cipher\_text = cipher\_text.join(v\_list)  
 print('multiple\_permutation.encryption: ' + str(datetime.now() - start\_time))  
 fig, ax = plt.subplots()  
 plt.bar(list(source\_alphabet\_dict.keys()), source\_alphabet\_dict.values(), color='g')  
 ax.set\_ylabel('количество появившихся символов')  
 ax.set\_xlabel('символы исходного алфавита')  
 plt.show()  
 elif action == 'decryption':  
 for i in range(0, len(keyword1)):  
 table\_true\_second.append([])  
 line\_number = 0  
 element\_number = 0  
 for s in source:  
 if s in ALPHABET:  
 if s in substance\_alphabet\_dict:  
 substance\_alphabet\_dict[s] += 1  
 else:  
 substance\_alphabet\_dict[s] = 1  
 if line\_number != len(keyword1):  
 if element\_number != len(keyword2):  
 table\_true\_second[line\_number].append(s)  
 element\_number += 1  
 elif line\_number != len(keyword1) - 1:  
 line\_number += 1  
 element\_number = 1  
 table\_true\_second[line\_number].append(s)  
 for j in keyword1:  
 Ai = ALPHABET.index(j)  
 if j in dict\_column\_index.keys():  
 dict\_column\_index[j + '2'] = Ai  
 else:  
 dict\_column\_index[j] = Ai  
 temp = []  
 for i in range(0, len(keyword1)):  
 temp.append([])  
 h = 0  
 for e in ALPHABET:  
 if e in dict\_column\_index.keys():  
 ai = keyword1.index(e)  
 temp[ai] = table\_true\_second[h]  
 h += 1  
 if e + '2' in dict\_column\_index.keys():  
 ai = 5  
 temp[ai] = table\_true\_second[h]  
 h += 1  
 for i in range(0, len(keyword2)):  
 table\_true.append([])  
 for ri, row in enumerate(temp):  
 for ei, element in enumerate(row):  
 table\_true[ei].append(element)  
 for j in keyword2:  
 Ai = ALPHABET.index(j)  
 if j in dict\_row\_index.keys():  
 dict\_row\_index[j + '2'] = Ai  
 else:  
 dict\_row\_index[j] = Ai  
 temp = []  
 for i in range(0, len(keyword2)):  
 temp.append([])  
 h = 0  
 for e in ALPHABET:  
 if e in dict\_row\_index.keys():  
 ai = keyword2.index(e)  
 temp[ai] = table\_true[h]  
 h += 1  
 if e + '2' in dict\_row\_index.keys():  
 ai = 5  
 temp[ai] = table\_true[h]  
 h += 1  
 v\_list = []  
 for v in temp:  
 for e in v:  
 v\_list.append(e)  
 cipher\_text = cipher\_text.join(v\_list)  
 print('multiple\_permutation.decryption: ' + str(datetime.now() - start\_time))  
 fig, ax = plt.subplots()  
 plt.bar(list(substance\_alphabet\_dict.keys()), substance\_alphabet\_dict.values(), color='g')  
 ax.set\_ylabel('количество появившихся символов')  
 ax.set\_xlabel('символы алфавита')  
 plt.show()  
 return cipher\_text  
  
  
if \_\_name\_\_ == '\_\_main\_\_':  
 text = ''  
 with open('is\_text.txt', 'r', encoding='utf-8') as source:  
 text = source.read()  
 with open('ci\_text.txt', 'w', encoding='utf-8') as cipher\_text:  
 cipher\_text.write(routing('encryption', text.lower()))  
 with open('dec\_text.txt', 'w', encoding='utf-8') as decryption\_text:  
 decryption\_text.write(  
 routing('decryption', routing('encryption', text.lower())))  
 with open('ci\_text\_m.txt', 'w', encoding='utf-8') as cipher\_text:  
 cipher\_text.write(multiple\_permutation('encryption', text.lower(), 'яраслаў', 'піцуха'))  
 with open('dec\_text\_m.txt', 'w', encoding='utf-8') as decryption\_text:  
 decryption\_text.write(  
 multiple\_permutation('decryption', multiple\_permutation('encryption', text.lower(), 'яраслаў', 'піцуха'), 'яраслаў', 'піцуха'))