Національний технічний університет України “Київський політехнічний інститут”

КРИПТОГРАФІЯ

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Варіант 5

Виконали студенти групи ФБ - 01:

Пітель Богдан та Ширий Віталій

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи (1).

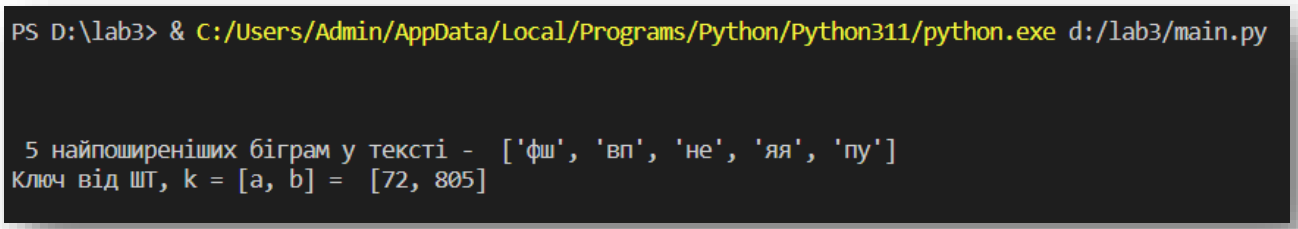
4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

text.txt – файл з текстом нашого варіанту.

main.py – код нашої програми.

Виконання main.py в VS Code:



агодьшлидашлибьспроинеслышнокакподснижньеводьпротекаламолодост
ыеленьвбездействииивнешнейвовнупреннейборыбеипревогеподругунеене
бьлоизовсехдевицпосещавшихдшйстаховьхонанесошласынисоднднмродите
лыскаявластыникогданетяготеланаделендмасшестнадцатилетнеаовозраста
онасталапочтисовсемнезавистйгоназажиласобственнойсвоеюжизныюножи
зныюодинокдмеедушаиразаораласыипогасалгодинокоонабиласыкакптица
внлеткеаклеткинебьлониктонестеснялееиниктониудерживалгонарваласыи
томиласыонаиногдаскйасебянепонтйаладажебояласысамойсебявсечтоокр
ужалоееказалосыейнетобесыйьсленнейнетонепонятнейкакжитыбезлюбви
алюбитынекоаодумалаонаистрашностановилосыьмотэтихдумотэтихощуще
нимвоспйнадцатилетоначутыниумерлготзлокачестяенндмлихоразкипотряс
еннумдооснованиявесыееорганизмотприродьздоровумикрепкюмдолгонп
йогсправитысяпоследниеследьболезниисчезлинаконецноотецеленьникола
евньвсеещенебезозлобленыитолковалобеенервахиногдаежприходиловгол
овучтоонажелаетчеготочегониктонежелаеточпйниктонпйьслитвцелойросс
иипотшйонаутихаладажеыйеяласынадсобдмбеспечнотроводиладенызадн
емновнезапночтотосилыноебезейянноесчемонасовладетыниумелатакизак
ипаловньмтакитросилосывьрватысянаружугрсзапроходилаопускалисыуста
льеневзлетевшиекрьлыянопорьвьэтинеобходилисыьмдаромкаконанистар
аласыневьдатытоаочтовнежпроисходилотоскавзволнованндмдушисказьва
ласывсамомеенаружномспокойствииироднъееечастобьливпраяепожимат
ыплечкйеудивлытысяинепониматыеестранностемвденыскоторогоначалсян

ашрассказеленадолышеобькновенноаонеотходилаотокнаонкйноаодумала
оберсеныевеосвоемразаоворесntйпопребностывзащитеинфоюйациивозни
каетвсвязиснеобходимостыюобеспефитысекретностыисследованимвстрате
гическихобластяхтравилынорастределытыинформациюотршйьшленньхраз
работкахирегулироватыинфоюйациюоличностивсоврпйенномобществена
аловосжйидесытьхаодоврасыйатриваетсякакначалынумпунктогдасоциал
ыньетротестьвдпйократическихстранахпшйоглисплестисыглобалынойсетих
акеровполитическюмфлиртнапочяенарушенияправчеловекапородилтымуо
рганизацийхакеровмйассестрачйирапочтиодноврпйенномоменеечпйзааодэт
игруппьузналитрелестысопрудничестваихчленьсвободноолйенивалисыиде
ййичерезнационалыньеграницьчастопоукраденнейпаролямдающимбеспл
атньйдоступктелефонндмсетинесколыкоприфинобыединившисымйестесд
елалтйиждународнумкомпыютернумразбдмлекгтйидьмстяеннейновьетехн
ологииссздавшиеболепйощньеидешевьекшйпыютерьразвитиекшймуникац
ийдлясвязиимеждународньйхарактерстандартовустановленньхпранснацио
налыньмикорпорациямивпринципеестылишшдвавидаугрозьраскрьтиеиви
доизмененииеданньхраскрьтиеданньхтредполагаетчтокшйутослучайноилип
ослецеленаправленньхдьмствийстализвестенсмьслинфоюйацииэтотвидна
рушениявспречаетсянаиболеечастопоследствиййогутбьтысамьеразньеесли
похищентексткнигисправочниканакоторуюпопраченейесяцьработьдесытко
влюдьмтодляколлективаавторовэтокатасprлфаипотеримогутвьражатысявт
ьсячахдолларроводнакоесликнигаужеизданатодостаточнолишыслегкапожу
ритыпохитителяирассказатыослуфившпйсявотделеновостейгазетьилипотел
евидениюпохитителжйожетсделатыкнигеяеликолепнуюренлкйуоченываж
нуюинфоюйациюоберегаемуюопраскрьтиятредставляютсведенияолюдяхи
сторииболезниписымасостояниясчетоввбанкаходнакопомнениюболышоао
фисласпециалистовугрсзьличностисвведениемкшйпыютеровостalисынато
мжиуровнеивтшйжесостояниичтоидообширноаоисполызованияэмйвведен
иевсовременншймиретурисйстановитсявсеболееважндмбьстроразвивающ
ейсяопраслыюхсзфмствадоходьоттурисйастановятсяважнойчастыювалютн
ьхпоступленюмвомногихстранахразвитиетуризмаспособствуетростуобщест
венноаотроизводстваулучшениюеаоструктурьростутроизводителыностипр
удавшйногихопрасляхэкономикидаженетйеющихктурисйупрямоаоотноше
ниййиждународноетуристскоепопреблениестимулируетмногочисленньеэк
оншйическиепроцессьоткрьвающиедополнителыньерьнкидлятродукциине
туристскихопраслейссздаваытпйсамьмусловиядляростатроизводствавсеэти
факторьделаюпразвитиеиндусприитурисйгоченыважнейдляспрансперехо
ньмтипшйэконшйикиеоншйическиетрудностикоторьепериживаютэтиаосуд
арстванпйогутнесказатысянауровнеразвитиытуризманотриэтомкаждаяспра
наимеетвэтомотношениисвоюспецификуцелшданнойработьрасыйотретыи
проанализироватыорганизациютуристскдмдеытелыностивспранесперехо

нейтипомэкономикинатртйеревенгриивначалерасыйатриваютсятеоретикш йетодическиеположенияисследованиязатемдаетсяоценкаразличньхфактор овразвитияиндустриитуризмаяенгрииприроднорес урснумкулытурноистори ческийиинфраспруктурнумпотенциалкшйплексноетуристскоерайонирован иедалеетроводитсяанализсоврпйенноаосостоянияиндусприитурисйавенгр иииеотделыньхкшйпонентовнафонеобщеаоуровняэконшйическоаоразвити ястраньдаетсяоценкасоциалыноэкономическдмролииндустриитуризмавэк ономикеяенгриииивзаключениепроводитсяобщюманализорганизациитурис тскойдеятелыностивстранашспереходнейтипомэкономикивобщпйивенгри ивчастностияенгиятринадлежакспранкйспереходньмтипшйэконшйикиime еттемнпйенееспецификескиечертькоторьеотличаютееотдругишспранэтого типавотношенииразвитияиндусприитурисйгосновнойтакдмчертдмявляется точтотуризйвенгрииразвиваетсяужедавноешевначаледвадцатоговекавэтд мстранесложилисятрадиционньетуристскиесвязитурисйявляетсяважндмот раслыюнародногохсзфмствасоврпйенномвенгрииколичествоиноспранньхт уристовпосещающихвенгриюрастетизаодавгодтомунемалоспособствуетбог атейшюмкулытурноисторическийитрирод

Хм, ;) текст схожий на слова з твору "Напередодні" автора Івана Сергійовича Тургенева

Висновок: під час лабораторної роботи виконували атаку на афінний шифр, використовуючи частотний аналіз, основна суть якого це використання статичних властивостей мови(в даному випадку російської).