Міністерство освіти і науки України
Національний технічний університет України
"Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут

«Криптографія»

Комп’ютерний практикум

№ 2

Виконав:
студент групи **ФБ-83**
Гах Валерій

Перевірив:
_____

Київ 2020

Назва: Криптоаналіз шифру Віженера;
Мета роботи:Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера;
Постановка задачі:
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).
Варіант: 6(номер у списку групи), номер бригади відсутній(робота виконана самостійно);

Характеристики обладнання:

- Ноутбук - Lenovo G510;
- ОС - Windows 10 Home x64;
- Процесор - Intel Core i5-4200M, CPU - 2.5GHz;
- Тип системи: 64-розрядна ОС, процесор x64;
- ОЗУ - 6.00 ГБ;

Хід роботи:
Програмний код-реалізацію криптоаналізу було написано мовою python. При цьому окремі функції шифрування-дешифрування та функції роботи з алфавітом винесено в окремі файли - Alphabet_and_funcs.py – функції та словники, що реалізують роботу з російським алфавітом не використовуючи кодування файлів («ё» замінена на «е» для сумісності з шифротекстами в завданні практичної роботи). text_convert.py – невеликий код, що фільтрує довільний текст від знаків пунктуації та пробілів для подальшого аналізу. Подібний код було реалізовано в практичній роботі №1, проте вона була реалізована на C++, і довелося написати аналогічний код ще раз, але на python. Caesar_cipher_op.py – файл з функціями шифрування/дешифрування Цезаря а також функцією співставлення найчастішої літери деякого тексту з літерою "О", яка повертає відповідний ключ розшифрування. Vigenere_cipher_op.py – містить функції шифрування/дешифрування Віженера та функцію розбиття тексту в залежності від довжини ключа r. calculate_INDEXES_for_my_plaintext.py – містить код, який підраховує індекси відповідності для шифротекстів, утворених шифруванням шифром Віженера деякого взятого мною відкритого тексту та деяких осмислених ключів різної довжини(r=2-30 літер). Також код обчислює індекс відповідності самого відкритого тексту. main_cryptoanalysis.py – код, що виконує сам криптоаналіз шифротексту мого варіанту та виводить результати автоматизованого частотного аналізу. Зміни та доробки в розшифрування(як наприклад вгадування літер там, де автоматизований частотний аналіз розшифрував тест неправильно) проводяться шляхом додавання в кінець цього коду нових, необхідних саме для поточного аналізу, маніпуляцій з ключем.
Результати:
По обчисленим індексам відповідності видно, що для відкритих текстів індекси набагато більші, ніж для їх шифротекстів. При цьому для шифротекстів, утворених ключами довжини>7 індекси не сильно відрізняються один від одного, тому було неможливо визначити довжину ключа для шифротексту мого варіанту, порівнюючи його індекс відповідності з попередньо обчисленими.(Порівняння дало r=14, що не є некоректною довжиною ключа, що я дізнався потім при правильній розшифровці тексту). Знаючи, що довжина ключа не набагато більша, або менша за 30(взято з методички), я перебирав довжини ключів і, розбиваючи текст по довжині ключа на підтексти, зашифровані Цезарем, співставляв найчастішу літеру в кожному підтексті літері «О», і отримуючи таким чином ключ розшифрування Цезаря, який є однією літерою в ключі Віженера. Правильність отриманого ключа можна перевірити хоча б і тим, що, якщо ключ осмислений, то в ньому не буде 2-3 однакових літер, що стоять поряд. Також правильність підібраного ключа можна перевірити обчисливши індекс відповідності розшифрованого цим ключем тексту – для осмисленого відкритого тексту він буде >0.05. Саме таким чином і було отримано приблищний ключ:

```
Python 3.7.4 (tags/v3.7.4:e09359112e, Jul  8 2019, 19:29:22) [MSC v.1916 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
 RESTART: ......\fb-labs-2020\cp_2\gakh_fb-83_cp2\Lab2\main_cryptoanalysis.py
Calculated ciphertext INDEX = 0.034119477929863806
жьчрдеврйкужояьхвфьчэъоъашгтмцифавицопшнюфытнижуфтмнцьрвяихы
Suggested key length(r) = 34
Suggested key: ВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЛЕНИЕДЖЛНЯА
ДОРОФЕЙЛЬВОВИЧШСВТОРЫКОПЫЛЫНИРЭЗБВЖИЗНИНЕПОКИДАЛРОМЛИХОТЯЭРОЖИЛУГЕПОЛЬШЕШЕСТИДЕС
INDEX = 0.0510364046443072
--------------------------------------------------
Suggested key length(r) = 51
Suggested key: ФОЗВРАЩЕДИЩДЖИЯДАВОЗВПАШЕНИЕГЭЛНСАВЕЗЬРАЛЕНИЕДЖЛНДА
ТОРОФЕЙЛЕВЪВИЧЭСВТОРЫЛОВЫЛЫНЙЩЭЗПВЖСЗУИНУПОКИДАИЗОМЩИХОТЯПРЧЖФЛУЖУКОЛЬШЕЩЕТТИДЕТ
INDEX = 0.047439691106429926
--------------------------------------------------
```

Отже автоматизованим частотним аналізом було отримано ключ «ВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЛЕНИЕДЖЛНЯА».Бачимо що ми отримали ключ подвійної довжини, що видно по тому, як сильно повторюються слова в ключі «ВОЗВРАЩЕНИЕДЖ». Тобто справжній ключ – це «ВОЗВРАЩЕНИЕДЖИДДА» довжини 17. Проте його ще потрібно підправити, бо в розшифрованому ним тексті є осередки неосмисленого тексту. Тобто будемо підганяти ключ так, щоб розшифрований ним текст був повністю осмисленим(для цього можна в окремому текстовому файлі співставити шифротекст, ключ, циклічно записаний до кінця узятого с початку шифротексту, та розшифрований текст та подивитися, які літери у відкритому тексті неправильні і знаючи відповідні їм літери шифротексту змінити літери ключа так, щоб новий відкритий текст став правильним). Відповідні зміни(узято 120 літер):

1)

```
ШТ:  ЖЬЧРДЕВРЙКУЖОЯЬХВФЬЧЭЪОЪАШГТМЦИФАВИЦОПШНЮФЫТНИЖУФТМНЦЬРВЯИХЫОНПЩОТООНКЯЗИЕКЧХМКХЕЪХШЕФЮЗГЮТЩРЬШУФЖЙЫЩСФЮХКВЕДБЪЦООФФЬННК
Ключ:ВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЩЕНИЕДЖИДДАВ
ВТ:  ДОРОФЕЙЛЬВОВИЧШСВТОРЫКОБЫЛЫНИРАРЬВЖИЗНИНЕПОКИДАЛРОМЛИХОТЯПРОЖИЛУЖОКОЛЬШЕШЕСТИДЕСЯТСФЕТРАБОТАЛПРОРАБЧХСТРОИТЕЛЬНОЙКОМШЙНИ
```

Бачимо, що у відкритому тесті в місці «КОЛЬШЕШЕСТИДЕСЯТИ» явно малося на увазі «БОЛЬШЕШЕСТИДЕСЯТИ». Замінимо літеру в ключі так, щоб в розшифрованому тексті з’явилася «Б» замість «К» та знайдемо найчастішу букву розшифрованого тексту у підтексті, до якого належала ця неправильна літера(відповідний номер підтексту серед 0..r-1, де r=17: №15) :

```
ШТ:  ЖЬЧРДЕВРЙКУЖОЯЬХВФЬЧЭЪОЪАШГТМЦИФАВИЦОПШНЮФЫТНИЖУФТМНЦЬРВЯИХЫОНПЩОТООНКЯЗИЕКЧХМКХЕЪХШЕФЮЗГЮТЩРЬШУФЖЙЫЩСФЮХКВЕДБЪЦООФФЬННК
Ключ:ВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВ
ВТ:  ДОРОФЕЙЛЬВОВИЧШИВТОРЫКОБЫЛЫНИРАРУВЖИЗНИНЕПОКИДАЛРЕМЛИХОТЯПРОЖИЛУЖОБОЛЬШЕШЕСТИДЕСЯТСЛЕТРАБОТАЛПРОРАБЧМСТРОИТЕЛЬНОЙКОМШАНИ
```

Найчастіша літера в цьому підтексті: «Е» - наступна за частотою в довільному відкритому тексті літера російського алфавіту.

(Усі частоти [('Е', 39), ('А', 37), ('И', 33), ('О', 32), ('Н', 29), ('Т', 27), ('С', 20), ('М', 20), ('Р', 18), ('В', 17), ('Л', 15), ('К', 15), ('П', 14), ('Д', 12), ('У', 11), ('З', 10), ('Й', 9), ('Ь', 7), ('Ы', 6), ('Ж', 5), ('Г', 5), ('Ч', 4), ('Ц', 3), ('Б', 3), ('Я', 2), ('Щ', 2), ('Ш', 2), ('Ф', 2), ('Ю', 1), ('Э', 1), ('Ъ', 1), ('Х', 1)])

2)

```
ШТ:  ЖЬЧРДЕВРЙКУЖОЯЬХВФЬЧЭЪОЪАШГТМЦИФАВИЦОПШНЮФЫТНИЖУФТМНЦЬРВЯИХЫОНПЩОТООНКЯЗИЕКЧХМКХЕЪХШЕФЮЗГЮТЩРЬШУФЖЙЫЩСФЮХКВЕДБЪЦООФФЬННК
Ключ:ВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВОЗВРАЩЕНИЕДЖИДНАВ
ВТ:  ДОРОФЕЙЛЬВОВИЧШИВТОРЫКОБЫЛЫНИРАРУВЖИЗНИНЕПОКИДАЛРЕМЛИХОТЯПРОЖИЛУЖОБОЛЬШЕШЕСТИДЕСЯТСЛЕТРАБОТАЛПРОРАБЧМСТРОИТЕЛЬНОЙКОМШАНИ
```

Тепер ми бачимо, що у відкритому тесті в місці «УЖОБОЛЬШЕШЕСТИДЕСЯТИ» очевидно малося на увазі «УЖЕБОЛЬШЕШЕСТИДЕСЯТИ». Замінимо літеру в ключі так, щоб в розшифрованому тексті з’явилася «Е» замість «О» та знайдемо найчастішу букву розшифрованого тексту у підтексті, до якого належала ця неправильна літера(відповідний номер підтексту серед 0..r-1, де r=17: №14) :

```
ШТ:  ЖЬЧРДЕВРЙКУЖОЯЬХВФЬЧЭЪОЪАШГТМЦИФАВИЦОПШНЮФЫТНИЖУФТМНЦЬРВЯИХЫОНПЩОТООНКЯЗИЕКЧХМКХЕЪХШЕФЮЗГЮТЩРЬШУФЖЙЫЩСФЮХКВЕДБЪЦООФФЬННК
Ключ:ВОЗВРАЩЕНИЕДЖИННАВОЗВРАЩЕНИЕДЖИННАВОЗВРАЩЕНИЕДЖИННАВОЗВРАЩЕНИЕДЖИННАВОЗВРАЩЕНИЕДЖИННАВОЗВРАЩЕНИЕДЖИННАВ
ВТ:  ДОРОФЕЙЛЬВОВИЧПИВТОРЫКОБЫЛЫНИРАЗУВЖИЗНИНЕПОКИДАЛЗЕМЛИХОТЯПРОЖИЛУЖЕБОЛЬШЕШЕСТИДЕСЯТИЛЕТРАБОТАЛПРОРАБОМСТРОИТЕЛЬНОЙКОМПАНИ
```

Найчастіша літера в цьому підтексті: «О».

(Усі частоти [('О', 47), ('А', 38), ('Е', 37), ('Т', 31), ('Н', 27), ('И', 22), ('Р', 19), ('Л', 18), ('К', 17), ('В', 17), ('С', 16), ('У', 13), ('Ь', 12), ('П', 12), ('Я', 10), ('З', 9), ('М', 8), ('Д', 7), ('Б', 7), ('Ы', 6), ('Й', 6), ('Г', 6), ('Ш', 4), ('Щ', 3), ('Х', 3), ('Ч', 2), ('Ц', 2), ('Ж', 2), ('Ю', 1), ('Ф', 1), ('Э', 0), ('Ъ', 0)])

Дивно, що найчастіша літера виявилася «О», але при автоматизованому частотному аналізі ключ був підібраний неправильно для цього підтексту. Але згадаймо, що ключ «ВОЗВРАЩЕНИЕДЖИДДА» був отриманий поділом навпіл ключа подвійної довжини «ВОЗВРАЩЕНИЕДЖИДДАВОЗВРАЛЕНИЕДЖЛНЯА» у якого, як видно, одна і та ж буква потрібного ключа різна для аналізів різних підтекстів, і при чому одна з них правильна. Тобто саме через те, що ми отримували подвійний ключ на початку і брали для подальшого аналізу його половину ми повинні були тільки вручну вгадувати правильні літери ключа там, де вони вочевидь були неправильні. При цьому якщо ми проводимо автоматичний аналіз для довжини ключа 17(відразу правильної довжини):

```
Suggested key length(r) = 17
Suggested key: ВОЗВРАЩЕНИЕДЖЛНДА
ДОРОФЕЙЛЬВОВИФПСВТОРЫКОБЫЛЫНИРЭЗЬВЖИЗНИНЕПОКИДАИЗОМЛИХОТЯПРОЖИЛУГЕКОЛЬШЕШЕСТИДЕС
INDEX = 0.05228444656611287
```

Бачимо, що літера «Н» в ключі була визначена правильно, але інша літера, яка визначається в половині ключа подвійної довжини правильно в ключі довжини 17 визначилася неправильно(тобто можливий аналіз можливих літер ключа на місцях ,де вони очевидно неправильні, як літер, визначених автоматичним аналізом із взяти ключем кратної 17 довжини).

У мене від початку узято половину подвійного ключа, бо я не розглянув короткий ключ довжини 17, а почав пошук ключа з довжини 20 і до 60. У кінцевій програмі перебір ключів по довжинам вже відбувається для 2-60.

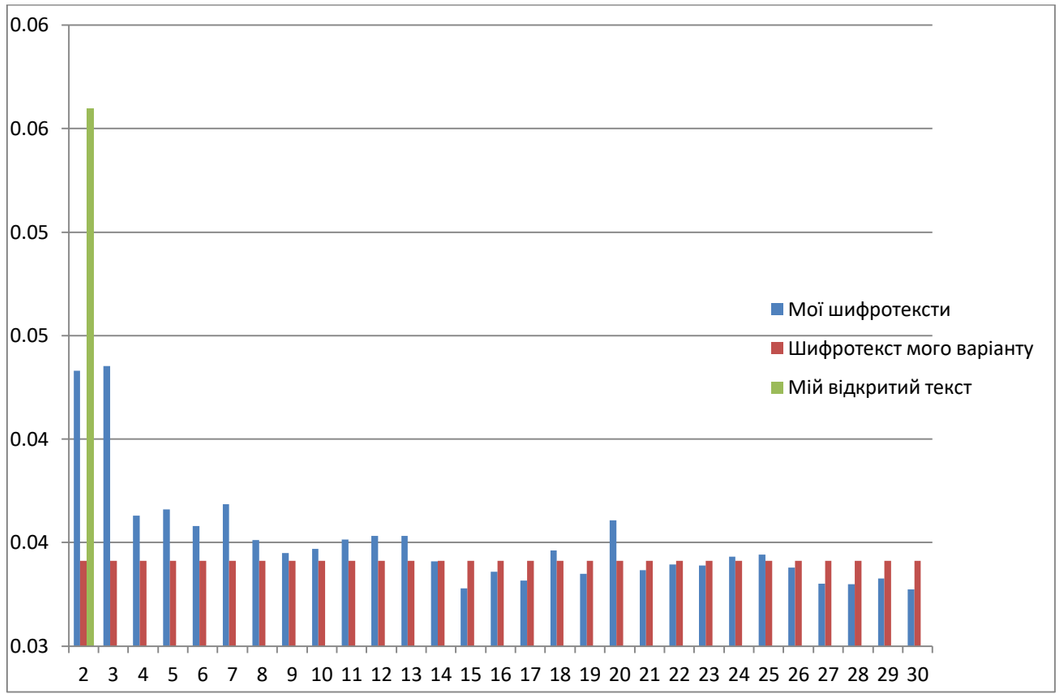
Кінцевий правильний ключ та розшифрований текст:

Ключ: ВОЗВРАЩЕНИЕДЖИННА

ДОРОФЕЙЛЬВОВИЧПИВТОРЫКОБЫЛЫНИРАЗУВЖИЗНИНЕПОКИДАЛЗЕМЛИХОТЯПРОЖИЛУЖЕБОЛЬШЕШЕСТИДЕСЯТИЛЕТРАБОТАЛПРОРАБОМСТРОИТЕЛЬНОЙКОМПАНИИДОМОС
ТРОЙВХАРЬКОВЕСТОЛИЦЕВКРАИНЫЛЮБИЛПОРЫБАЧИТЬСДРУЗЬЯМИНАОЗЕРАХРОГАНЬСКОГОКРАЯЗАЧЕРТОЙГОРОДАВЫРАЩИВАЛНАДАЧНОМУЧАСТКЕОВОЩИИФРУКТЫВО
СПИТЫВАЛВНУКОВАВОТУЕЗЖАТЬЗАПРЕДЕЛЫРОДНОЙВКРАИНЫНЕЛЮБИЛНЕСМОТРЯНАВОЗМОЖНОСТИВСВЯЗИССОЗДАНИЕМГЛОБАЛЬНОЙСЕТИМЕТРОПОБЫВАТЬНАЛЮБОЙП
ЛАНЕТЕСОЛНЕЧНОЙСИСТЕМЫИДАЖЕЗАЕЕПРЕДЕЛАМИЧТОПОДВИГЛОЕГОСОГЛАСИТЬСЯНАЭКСКУРСИЮПОЛУНЕОНИСАМНЕВСОСТОЯНИИБЫЛОТВЕТИТЬВЕРОЯТНОСЫГРАЛИ
СВОЮРОЛЬРАССКАЗЫДРУЗЕЙХВАСТАВШИХСЯСВОИМИПУТЕШЕСТВИЯМИИУНЕГОВЗЫГРАЛОЛЮБОПЫТСТВОПОСМОТРЕТЬВБЛИЗИЧТОЖЕЭТОТАКОЕСПУТНИЦАЗЕМЛИОКОТОР
ОЙТАКМНОГОГОВОРЯТДЕТИВНУКИИДРУЗЬЯКАКБЫТОНИБЫЛОАУТРОМДВАДЦАТЬТРЕТЬЕГОДЕКАБРЯАККУРАТВНАЧАЛОСВЯТОКДОРОФЕЙЛЬВОВИЧВТАЙНЕОТРОДНЫХИБЛ
ИЗКИХПОЗВОНИЛВБЮРОЭКСКУРСИЙСОЛНЕЧНОЙСИСТЕМЫЗАПИНАЯСЬОБЪЯСНИЛЧЕГОХОЧЕТИВТОТЖЕДЕНЬСПОМОЩЬЮМЕТРОДОБРАЛСЯДОАПОЛЛОНТАУНАГОРОДАНАЛУН
ЕОТКУДАДОЛЖНАБЫЛАНАЧАТЬСЯЭКСКУРСИЯПОСАМЫМКРАСИВЫМИЗАГАДОЧНЫММЕСТАМСПУТНИЦЫЗЕМЛИАПОЛЛОНТАУНРАСПОЛАГАЛСЯНАРАВНИНЕМОРЯСПОКОЙСТВИЯ
НЕДАЛЕКООТЗНАМЕНИТОЙБОРОЗДЫМАСКЕЛАЙНПОХОЖЕЙНАИЗВИЛИСТОЕРУСЛОРЕКИИМЕННОЗДЕСЬКОГДАТОВКОНЦЕДВАДЦАТОГОВЕКАСОВЕРШИЛПОСАДКУАМЕРИКАН
СКИЙПИЛОТИРУЕМЫЙКОРАБЛЬАПОЛЛОНОДИННАДЦАТЬАТОЧНЕЕЕГОПОСАДОЧНЫЙМОДУЛЬЕСТЕСТВЕННОЭКСКУРСАНТАМЗАНИМАВШИМКАБИНУДВАДЦАТИМЕСТНОГОЭКСК
УРСИОННОГОФЛАЙТАСНАЧАЛАПОКАЗАЛИПАМЯТНИКАПОЛЛОНУОДИННАДЦАТЬПИРАМИДУИЗЛУННОГОБАЗАЛЬТАСПОСАДОЧНОЙПЛАТФОРМОЙИАМЕРИКАНСКИМФЛАГОМАЗА
ТЕМФЛАЙТОТПРАВИЛСЯВПУТЕШЕСТВИЕПОМОРЮСПОКОЙСТВИЯЗАЛИТОМУЯРКИМСОЛНЕЧНЫМСВЕТОМЭКСКУРСАНТАМИОКАЗАЛИСЬМОЛОДЫЕЛЮДИВВОЗРАСТЕОТВОСЕМНА
ДЦАТИДОДВАДЦАТИЛЕТПОЭТОМУПОНАЧАЛУДОРОФЕЙЛЬВОВИЧЧУВСТВОВАЛСЕБЯНЕВСВОЕЙТАРЕЛКЕСМУЩАЯСЬПОДЛЮБОПЫТНЫМИВЗГЛЯДАМИСПУТНИКОВНОПОТОМЕГО
ЗАХВАТИЛАСУРОВАЯКРАСОТАЛУННЫХПЕЙЗАЖЕЙИОНПЕРЕСТАЛОБРАЩАТЬВНИМАНИЕНАВЕСЕЛЯЩУЮСЯКОМПАНИЮЖАДНОРАЗГЛЯДЫВАЯПРОПЛЫВАЮЩИЕПОДДНИЩЕМФЛАЙ
ТАЦИРКИЭСКАРПЫКРАТЕРЫИЖИВОПИСНЫЕГРУППЫСКАЛМОРЕСПОКОЙСТВИЯПОЛУЧИЛОСВОЕНАЗВАНИЕНЕСЛУЧАЙНОЕГОРОВНАЯСГЛАЖЕННАЯПОВЕРХНОСТЬТИПИЧНАДЛ
ЯОБШИРНЫХМОРЕЙНАДНЕВНОЙСТОРОНЕЛУНЫИРЕДКОРАДУЕТНАБЛЮДАТЕЛЕЙПРОЯВЛЕНИЕМВУЛКАНИЧЕСКОЙДЕЯТЕЛЬНОСТИОДНАКОИЗДЕСЬИМЕЛОСЬНЕМАЛОИНТЕРЕС
НЫХМЕСТИОБЪЕКТОВКОТОРЫЕДЕСЯТКИЛЕТВОЛНОВАЛИАСТРОНОМОВИЗУЧАЮЩИХСПУТНИЦУЗЕМЛИЗАГАДОЧНАЯЦЕПОЧКАКРАТЕРОВПОДНАЗВАНИЕМТЕННИСНАЯРАКЕТК
АОКОЛОДВУХДЕСЯТКОВЯМОКДИАМЕТРОМОТПЯТИДЕСЯТИДОСТАМЕТРОВПРОТЯНУЛИСЬУДИВИТЕЛЬНОРОВНОЙЛИНИЕЙЗАКАНЧИВАЯСЬКРАТЕРОМПОБОЛЬШЕДИАМЕТРОМО
КОЛОШЕСТИСОТМЕТРОВВПЕЧАТЛЕНИЕСКЛАДЫВАЕТСЯТАКОЕБУДТОПОЛУННОЙПОВЕРХНОСТИДЕЙСТВИТЕЛЬНОПРОКАТИЛСЯПОДПРЫГИВАЯТЕННИСНЫЙМЯЧОСТАВИВВПЫ
ЛИЦЕПОЧКУСЛЕДОВСОВИНЫЙМОСТКАМЕННАЯАРКАЧЕРЕЗБОРОЗДУМАСКЕЛАЙНДЛИНОЙОКОЛОТРЕХКИЛОМЕТРОВИЗУМИТЕЛЬНОРОВНАЯСТЕНАОБРЫВАДЛИНОЙОКОЛОТРИ
ДЦАТИКИЛОМЕТРОМБУДТОКТОТООТХВАТИЛНОЖОМКУСОКЛУННОЙПОВЕРХНОСТИИВЫБРОСИЛВКОСМОСОСТАВИВСРЕЗИЛОЖБИНУГЛУБИНОЙВКИЛОМЕТРБОРОЗДАЗОЛОТОЙ
РУЧЕЙСАМОЕНАСТОЯЩЕЕРУСЛОРЕКИШИРИНОЙВПОЛТОРАКИЛОМЕТРАИДЛИНОЙВПОЛТОРАСТАСВЕРКАЮЩЕЕПОДЛУЧАМИСОЛНЦАКРИСТАЛЛИКАМИПИРИТАЦВЕТОЧНАЯКЛУ
МБАВОЗВЫШЕНИЕРЫХЛОЙПОРОДЫОРАНЖЕВОГОЦВЕТАДИАМЕТРОМОКОЛОДВУХКИЛОМЕТРОВИВЫСОТОЙВДВЕСТИМЕТРОВДЕЙСТВИТЕЛЬНОКЛУМБАЕСЛИПОСМОТРЕТЬСВЕР
ХУСТОУНХЕНДЖГРУППАСКАЛСПЛОСКИМИВЕРШИНАМИСОЕДИНЕННЫХПОВЕРХУДОСТАТОЧНОРОВНЫМИПЛИТАМИПРАКТИЧЕСКИНЕОТЛИЧАЕТСЯОТЗЕМНОГОМЕГАЛИТИЧЕСК
ОГОКОМПЛЕКСАВАНГЛИИИНАКОНЕЦБОРОЗДАМАСКЕЛАЙНДЛИНОЙОКОЛОЧЕТЫРЕХСОТКИЛОМЕТРОВТАКЖЕЗДОРОВОПОХОЖАЯНАРУСЛОРЕКИШИРИНОЙОТКИЛОМЕТРАДОТР
ЕХКАКОБЪЯСНИЛГИДБОРОЗДАНАСАМОМДЕЛЕПРЕДСТАВЛЯЕТСОБОЙСДВИГОВЫЙРАЗЛОМЛУННОЙКОРЫСЛУЧИВШИЙСЯДЕСЯТКИМИЛЛИОНОВЛЕТНАЗАДВРЕЗУЛЬТАТЕПОДВ
ИЖКИЩИТАОТУДАРАМЕТЕОРИТАНОСВЕРХУБОРОЗДАВСЕРАВНОНАПОМИНАЕТРЕКУИДОРОФЕЙЛЬВОВИЧДАЖЕПРЕДСТАВИЛКАКПОРУСЛУТЕЧЕТВОДАОСТАНАВЛИВАЛИСЬИВ

ЫХОДИЛИИЗФЛАЙТАОДЕТЫЕВПУЗЫРИВАКУУМПЛОТНЫХСПЕЦКОСТЮМОВНЕСКОЛЬКОРАЗВКАБИНЕАППАРАТАПОДДЕРЖИВАЛАСЬНОРМАЛЬНАЯСИЛАТЯЖЕСТИПОЧТИЗЕМНАЯ
АВНЕЕЕЦАРИЛОЛУННОЕТЯГОТЕНИЕВШЕСТЬРАЗСЛАБЕЕЗЕМНОГОПОЭТОМУНЕОБОШЛОСЬБЕЗКУРЬЕЗОВИНЕЛОВКИХДВИЖЕНИЙПРАВДАВСЕВКОНЦЕКОНЦОВПРИВЫКЛИКНЕ
ОБЫЧАЙНОЙЛЕГКОСТИВТЕЛЕИСУДОВОЛЬСТВИЕМСКАКАЛИПОМЕСТНЫМБУЕРАКАМВТОМЧИСЛЕИДОРОФЕЙЛЬВОВИЧПОЛУЧИВШИЙНИСЧЕМНЕСРАВНИМЫЕОЩУЩЕНИЯАТЕПЕР
ЬЯВАМПОКАЖУОБЪЕКТЗЕРОСКАЗАЛГИДПРИГЛАШАЯЭКСКУРСАНТОВВКАБИНУПОСЛЕОЧЕРЕДНОГОВЫХОДАНАРУЖУХОДЯТЛЕГЕНДЫЧТОВЭТОММЕСТЕНАГЛУБИНЕДВУХСОТ
МЕТРОВРАСПОЛАГАЛСЯЗАГАДОЧНЫЙШАРИЗКОТОРОГОВПОСЛЕДСТВИИВЫЛУПИЛСЯНАЗЕМЛЕБОЕВОЙГИПЕРПТЕРИДСКИЙРОБОТДЕМОНАВТОРИТЕТНЫМТОНОМЗАМЕТИЛКТ
ОТОИЗКОМПАНИИМОЛОДЫХЛЮДЕЙИЛИДЖИННСОВЕРШЕННОВЕРНОНОВЕДЬОНПОТОМОСТАВИЛВКОЛЬЦАХСАТУРНАСВОЮИКРУБРИЛЛИАНТИДЫЭТОУЖЕДРУГАЯИСТОРИЯВЫНА
ВЕРНОЕПОМНИТЕВОЙНАСДЖИННАМИЗАКОНЧИЛАСЬВСЕГОЛИШЬГОДНАЗАДАЗДЕСЬОСТАЛСЯСЛЕДДЕМОНАЧТОВНЕМИНТЕРЕСНОГОУВИДИТЕФЛАЙТСПРОЗРАЧНЫМИДОСАМО
ГОПОЛАСТЕНКАМИПОДНЯЛСЯНАДКРАТЕРОМАВАКОВАИПОНЕССЯКГОРИЗОНТУСВИСЯЩЕЙНАДНИМПОЧТИПОЛНОЙЗЕМЛЕЙОКРАШИВАЮЩЕЙРАВНИНУВГОЛУБОВАТЫЙЦВЕТВМ
ЕСТАХГДЕЛЕЖАЛАТЕНЬОТСКАЛОСВЕЩЕННЫХПРЯМЫМИСОЛНЕЧНЫМИЛУЧАМИПРИБЛИЗИЛАСЬРЕКАБОРОЗДЫМАСКЕЛАЙНРАЗДАЛАСЬВШИРЬПРЕВРАТИЛАСЬВКРУТОЙГЛУБ
ИНОЙДОКИЛОМЕТРАКАНЬОННАОДНОМИЗПЛОСКИХГРЕБНЕЙКАНЬОНАПОЯВИЛОСЬБЕЛОСЕРЕБРИСТОЕПЯТНЫШКОПРЕВРАТИЛОСЬВХОЛМИКЗАТЕМВГОРУСДЫРОЙВЦЕНТРЕФ
ЛАЙТЗАВИСВПАРЕКИЛОМЕТРОВОТЭТОЙСТРАННОЙГОРЫИЭКСКУРСАНТЫНАЧАЛИРАССМАТРИВАТЬОБЪЕКТИМЕВШИЙНЕОБЫЧНОЕНАЗВАНИЕЗЕРОБОЛЬШЕВСЕГОСЕРЕБРИС
ТЫЙКУПОЛСКРАТЕРОМДИАМЕТРОМВТРИКИЛОМЕТРАНАПОМИНАЛЧЕЛОВЕЧЕСКИЙГЛАЗРАДУЖКАКОТОРОГОВЫСОХЛАИПОЖУХЛАПРЕВРАТИВШИСЬВБЕЛОСНЕЖНЫЙСЛОЙМХА
ИВЫЗЫВАЛЭТОТГЛАЗОТНЮДЬНЕПРИЯТНЫЕИРАДОСТНЫЕОЩУЩЕНИЯНЕОМЕРЗЕНИЕНЕТНОИНЕВОСТОРГСЛИШКОММНОГОВЭТОМЗРЕЛИЩЕБЫЛОПУГАЮЩЕГОИОТТАЛКИВАЮЩЕ
ГОИОДНОВРЕМЕННОПРИТЯГИВАЮЩЕГОВЗОРМОЛОДЕЖЬПРИТИХЛАДОРОФЕЙЛЬВОВИЧПОЧУВСТВОВАЛСТЕСНЕНИЕВГРУДИПОСМОТРЕЛНАГИДАТОТУЛЫБНУЛСЯКАКНАСТОЯ
ЩИЙЧЕЛОВЕКХОТЯБЫЛВСЕГОНАВСЕГОВИТСОМНРАВИТСЯЧТОЭТОТАКОЕЭФФЕКТКВАНТОВОЙЭФФУЗИИКАКГОВОРЯТУЧЕНЫЕОБРАЗНОГОВОРЯНАГОРНЫЕПОРОДЫПОДЕЙСТ
ВОВАЛОДЫХАНИЕДЕМОНАНАЭТОММЕСТЕБОЛЕЕДВУХСОТЛЕТНАЗАДНАХОДИЛСЯТОРИЕВЫЙРУДНИКШАХТАКОТОРОГОДОСТИГЛАШАРОВИДНОЙПОЛОСТИГДЕИСПАЛДЖИННЕ
ПОСРЕДСТВЕННОКШАХТЕНАСНЕПРОПУСТИТОХРАНАНОТУТРЯДОМЕСТЬИНТЕРЕСНОЕУЩЕЛЬЕОНООБРАЗОВАЛОСЬСОВСЕМНЕДАВНОВСЕГОДВАМЕСЯЦАНАЗАДИМЫМОЖЕМПО
ЛЮБОВАТЬСЯНАРУДНИКСОБРЫВАПОЛЕТЕЛИЗДОРОВООЧЕНЬИНТЕРЕСНОМЫХОТИМПРОГУЛЯТЬСЯРАЗДАЛИСЬГОЛОСАДОРОФЕЙЛЬВОВИЧХОТЯИНЕИСПЫТЫВАЛБОЛЬШЕЖЕЛ
АНИЯГУЛЯТЬОДНАКОВОЗРАЖАТЬНЕСТАЛУНЕГОВОЗНИКЛООЩУЩЕНИЕЧТООНЗДЕСЬУЖЕБЫЛКОГДАТОХОТЯНИКОГДАРАНЬШЕЛУНУНЕПОСЕЩАЛФЛАЙТОБЛЕТЕЛСНЕЖНОСЕР
ЕБРИСТЫЙГЛАЗБЫВШЕГОТОРИЕВОГОРУДНИКАКРУГОМПОВЕРНУЛВДОЛЬБОРОЗДЫМАСКЕЛАЙНКЮГУСНИЗИЛСЯСТАЛИВИДНЫТРЕЩИНЫРАЗОРВАВШИЕБОКОВЫЕСТЕНКИБОР
ОЗДЫСОВСЕМСВЕЖИЕСУДЯПОБЛЕСКУУЗКИЕИПОШИРЕОЧЕВИДНОЭТОБЫЛРЕЗУЛЬТАТНЕДАВНЕГОЛУНОТРЯСЕНИЯОКОТОРОМГОВОРИЛГИДПРИБЛИЗИЛАСЬОЧЕРЕДНАЯТРЕ
ЩИНАДЕЙСТВИТЕЛЬНООБРАЗОВАВШАЯЖИВОПИСНОЕУЩЕЛЬЕСОСЛОИСТЫМИСТЕНАМИФЛАЙТПОДПРЫГНУЛИСЕЛНАОБРЫВЕСКОТОРОГОБЫЛИХОРОШОВИДНЫКУПОЛОБЪЕКТА
ЗЕРОИБОРОЗДАМАСКЕЛАЙНЭКСКУРСАНТЫПОСЫПАЛИСЬИЗАППАРАТАРАДУЯСЬВОЗМОЖНОСТИРАЗМЯТЬСЯГУРЬБОЙНАПРАВИЛИСЬКОБРЫВУПЕРЕБРАСЫВАЯСЬШУТОЧКАМ
ИИДУРАЧАСЬВНИХИГРАЛАЩЕНЯЧЬЯЭНЕРГИЯМОЛОДОСТИИДОРОФЕЙЛЬВОВИЧНАМГНОВЕНИЕПОЗАВИДОВАЛЗАДОРУИОПТИМИЗМУЮНОШЕЙИДЕВУШЕКГОДЯЩИХСЯЕМУЧУТЬ
ЛИНЕВОВНУКИОНТОЖЕПОЛЮБОВАЛСЯНАСНЕЖНОБЕЛЫЙКУПОЛВТРЕХКИЛОМЕТРАХОТОБРЫВАПОТОМТИХОНЬКООТОШЕЛОТРЕЗВЯЩИХСЯМОЛОДЫХЛЮДЕЙИПРОШЕЛСЯВДОЛЬ
ОБРЫВАВГЛЯДЫВАЯСЬВПРОТИВОПОЛОЖНУЮСТЕНУУЩЕЛЬЯВЗГЛЯДНАТКНУЛСЯНАРЯДЧЕРНЫХОТВЕРСТИЙПОХОЖИХНАСЛЕДЫПУЛЕМЕТНОЙОЧЕРЕДИЗАИНТЕРЕСОВАВШИС
ЬДОРОФЕЙЛЬВОВИЧПРЫГНУЛВНИЗИВКЛЮЧИВАНТИГРАВПЕРЕСЕКУЩЕЛЬЕОПУСТИЛСЯНАУЗКИЙКАРНИЗПЕРЕДСАМОЙБОЛЬШОЙДЫРОЙОПРЕДУПРЕЖДЕНИИГИДАНЕОТХОДИ
ТЬДАЛЕКООТФЛАЙТАОНЗАБЫЛДЫРАОКАЗАЛАСЬВХОДОМВПЕЩЕРУ

Обчислені індекси відповідності для тестових шифротекстів, відповідного їм відкритого тексту та мого шифротексту варіанту 6:


0.06
0.06
0.05
0.05
0.04
0.04
0.03
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Мої шифротексти
Шифротекст мого варіанту
Мій відкритий текст