

Міністерство освіти і науки України
Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”

Лабораторна робота
із КRYPTOграфії №2
КRYPTOаналіз шифру Віженера

Виконали:

Христиченко Дмитро ФБ - 72

Нестеров Назар ФБ - 72

Перевірено _____

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Мета роботи

Засвоєння методів частотного криптоаналізу. Здобуття навичок роботи та аналізу поточкових шифрів гамування адитивного типу на прикладі шифру Віженера.

Порядок виконання роботи

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).

Індекси відповідності

Відкритий текст	0.0549039
K = 2	0.0414622
K = 3	0.0423839
K = 4	0.0356621
K = 5	0.0345404
K = 12	0.0326629

Аналізуючи дану таблицю можна дійти висновку, що при збільшенні довжини ключа індекс стає більш віддаленим від значення індексу відповідності відкритого тексту, і навпаки, при малій довжині ключа значення індексу наближається до індексу відкритого тексту.

Шифрованный текст:

дѣсоуцмдурьдыгныбуккэаонтцхлуучктвдджоабубяцбхкубгбщешрцзвытшщяшхтяуюйлрньпрбдшзньямйнуьряпышт
уьзрзхтпфгяжитхчьурвтддфанвзгьчрщюнтобушузсшзпукхнмвбуьняэаоеймнеорцбэзмюйххлпейжцбышяпщцсущкдбалтоз
бевефямнумвеаыяпцезьуотптяуччтшкьуньдцплчжурпнямнонштвддшоюнгкшцкуьщдднтютгнцмукхрчбвщгртчпщыупшоы
уфшгхнжхуучехфшвччыыезьсахьрхобшглэчзекцъзахатггсьесоекчпнршчозьтчмучгшгшмьалефурраришужьэоваелунэкзф
вьюррвтецэцжемповжшралризщцоьпнвхчхнтьцьоннтдфьяняаозжярпплйжщшрзтоавхтмечэумзагноявстугьччрээзсцхзр
шухтанвчыбгпэзчабьбхючрлшхткгзгьумыкэецрпшьтьатьдэякоьпклэябфугэушфшцазсфвйгтьрьеюанонньвыанрзбчехуцокрж
ввщшсьуньтхквсаечцвуэкшоучквддлрзсесуптпфйщцппозчдызиххгуснтгцхнцалтйбпавуфкдкмйоньявпккртуьшиорщр
чбгкрятяпщжечзщцкрятияпщкшщццдтеопьтункфбшрыкытуужыбжпэртцзуркйфвчвыонийцукмщрббйллтамурпч
ечэвоьбгтзчепрахчъхъьдэьбдуобупкйфуюпопндрийтшошжъаахзефетлахлхмвеаьхпчпыомьбшчонийшрящцпкпжукувлэвщш
факзыдвсгхнаркфюывьрадфрхтсьлщржефрясдвчкчкрнкчкшудлбшмгеньзъвншыудьчесюрткцзбыщвфжежхртрпбзябфрйрь
жжщзюпрхмчьсткдтжынмржанчзцнвупщпурцдфшдшжххцьекковщчэлчувъхсхшужбапмрнххлхпумкшаьсхоокцьдкбзеаон
еезехазхкмжбщияхчтрруучпужхчшмшпяртьркозябьлррчуцкэрийшгбозняхецшрбчшнрэанзшиплхвжщжбдлйшквгпцмефох
влютртыуупкьзшзартгрзечшужехзюбьйрчусрябыкжцуялжрийскрюхткущаынфкдкшдлжпнъантзнийкцкхпшщдшьвводноахоуу
фвхтызйзтушоуцхэмузуйютъшьртлэьгчдзейкцупчполеанрхиьепоикмрлшязфюхехэюмсунршжфжфюйярншвршьфийьжютйн
хьончзгтгчдэтэзусргоуэсютгчмлизнербеьхтэкьумйнзбзйючурцтзвучрпкыдчынцмцсгцкпшешуфжмшсччряутубкфамнолч
щпзбубьдзйрхчтпоьшкббшхбшхьжщдхьдлпчвювзьярпдрпкйфоавьвукмйномущиьэрспбешьпзвцчччюахццлщшидбш
ювазшюрчорчкюбяшнбнвчрлпэпзъгтьдсаюпбчсвюютуптьгвзларотмвшлрйярнпетйцбщзъьйуьюкпкпхтцноиднчфбмзд

[illegible]

Ключ: человеквфутляре

Для знаходження ключа був використаний наступний алгоритм:

1. Шифротекст розбивається на блоки, кожний з яких містить i -ту букву шифротексту.

Таким чином при довжині ключа N ми маємо N блоків.

Для кожного блоку рахуємо значення індексу відповідності.

Довжину ключа знаходимо перебравши можливі довжини ключа (у нашому випадку від 2 до 30), співставляємо значання ІВ відкритого тексту та для блоків.

Отримуємо:

Possible key length: 2

Coincidence index is: 0.033946686230035

Possible key length: 3

Coincidence index is: 0.03462792608891599

Possible key length: 4

Coincidence index is: 0.03388838873784577

Possible key length: 5

Coincidence index is: 0.03979611593275698

Possible key length: 6

Coincidence index is: 0.0339515894553208

Possible key length: 7

Coincidence index is: 0.03513226466397645

Possible key length: 8

Coincidence index is: 0.03469050696538848

Possible key length: 9

Coincidence index is: 0.033956188932108056

Possible key length: 10

Coincidence index is: 0.03894108079306767

Possible key length: 11

Coincidence index is: 0.03506627553237723

Possible key length: 12

Coincidence index is: 0.03409899133583344

Possible key length: 13

Coincidence index is: 0.035074078463908975

Possible key length: 14

Coincidence index is: 0.034913731562935875

Possible key length: 15

Coincidence index is: 0.054158265013937786

Key length is: 15

Отже, робимо висновок, що довжина ключа дорівнює 15

2. Розбиваємо весь шифротекст на 15 блоків та знаходимо у кожному з блоків найбільш часту літеру. Використовуючи відомі статистичні дані російської мови, віднімаючи від найчастішої літери шифротексту найчастішу літеру російської мови, отримуємо ключ.

Ключ, который был создан программой: **йеловебвжнлбре**

Угаданный ключ: **человеквфутляре**

9 символов из 15 были выбраны верно

Розшифрований текст:

насамомкраюселамироносицкоговсараестаростыпрокофиярасположилисьнаночлезапоздавшиеохотникиихбылотолькодвоеветеринарныйврачиваниванычиучительгимназибуркинуиванаиванычабыладовольностраннаядвойнаяфамилиячимшагималайскийкотораясовсемнешлаемуиеговсейгубернииизвалипростопоименииотчествуонжилокологородаконаконскомзаводеиприехалтеперьнаохотучтобыподышатьчистымвоздухомучительжегимназибуркинкакждоелетогостиуграфоввпизтойместностидавноужебылсвоимчеловекомнеспалививаниванычвысокийхудощавыйстариксдлиннымиусамисиделснаружииувходаикурилтрубкуегоосвещалалубуркинлежалвнутринасеиегонебыловидновпотемкахрассказывалиразныеисторииимеждупрочимговорилиотомчтоженастаростымавраженщинаяздороваяинеглупаявовсюсвоюжизньнигдеенебыладальшесвоегородногоселаникогданевиделанигороданижелезнодорогииавпоследниедесятьлетвсиделазапечьюитолькопоночамвыходиланаулицучтожетутудивительногосказалбуркинлюдейодинокихпонатурекоторыекакразкратотшлышкилиулиткастараятсуйтивсвоюскорлупунаэтомсветенемалобытьможеттутявлениеисатавизмавозвращениектомувременикогдапредокчеловеканебылещеобщественнымживотнымжилодинокосвоейберлогеаможетбытьэтопростооднаизразновидностейчеловеческогохарактерактознаетянеестественникинемоеделокасаясьподобныхвопросовятолькохочусказатьчтотакиелюдиакмавраявлениенередкоедавтнедалекоискатьмесяцадвазадумерунасвгороденекыйбеликовучительгреческогоязыкамойтоварищвыонемслышаликонечноонбылзамечателемтемчтовсегдадажевоченьхорошуюпогодувыходилвкалошахисзонтикоминепременновтепломпальтонаватезонтикунеобылвчелхчасывчелхизсеройзамшикогдавынималперочинныйножчтобыочинитькарандаштонужногобылвчехольчикеилипоказалосьтожебыловчехлетаккаконвсе времяпряталеговподнятыйворотниконносилтемныеочкифайкуушизакладывалватойкогдасадилсянаизвозчикатоприказывалподниматьверходнимсловомуэтогочеловеканаблюдалосьпостоянноеинепреодолимоестремлениеокружитьсебяоболочкойсоздатьсебетаксказатьфутляркоторыйуединилбыегозащитилбытовнешнихвлиянийдействительностьраздражалаегопугаладержалавпостояннотревогеибытьможетдлятогочтобыоправдатьэту своюробостьсвоеотвращениекнастоящемуонвсегдахвалилпрошлоеитогоникогдаенебылоидревниязыкикоторыеонпреподавалбылидлянеговсущноститежекалошииззонтикудаонпряталсяотдействительнойжизниокакзвученкакпрекрасенгреческийязыкговорилонсосладкимвыражениемикакбывдоказательствосвоихсловпришуривглазиподнявпалецпроизносилантропосимысльсвоюбеликовтакжестаралсязапрятатьвфутлярдлянегообылияснытолькоциркуляригазетныестатьивкоторыхзапрещалосьчтонибудькогдавциркулярезапрещалосьученикамвыходитьнаулицупоследевятичасоввечераилвкакойнибудьстатьезапрещаласьплотскаялюбовьтоэтобылодлянегоясноопределеннозапрещеноибаставразрешениижеипозволенииискрывалсядлянеговсегдаэлементсомнительныйчтотонедосказанноеисмутноеогдавродеразрешалидраматическийкружокиличитальнюиличайнуютоонпокачивалголовойиговорилтихооноконечнотактотаквсэтопрекраснодакакбычегоневышлосяякогороданарушенияуклоненияотступленияотправилприводилиеговуниниехотязалосьбыкакоемуделоесликтоизтоварищейопаздывалнамолебенилидоходилслухоикакойнибудьпроказегимназистовиливиделиклассн

ую дамупоздновечеромсофицеромтооночченьволновалсяивсеговорилкакбычегоневышлоанапедагогическихсоветахонпростоулеталнасвоеюосторожностьюмноительностьюисвоимичистофутлярнымисоображенияминасчетовотговотдевушкойиженскойгимназияхмолодежьведетсебядурнооченьшумитвклассахкакбынедошлодоначестваахкакбычегоневышлоичтоеслибизвтерогокклассаисключитьпетровааизчетвертогоегораватобылобыоченьхорошоичтожесвоимивздохаминьтесвоимитемнымичкаминабледноммаленькомлицезнаетемаленькомлицекакухорькаондавилнасвсехимыуступалисбавляялипетровуегорувбаллоповедениюсажалиихподарестивконцеконцовисключалиипетроваиегоравбылоунегостранноеобыкновениеходитьпонашимквартирампридеткучителюсядетимолчитикакбудточтотовыматриваетпосидитэтакмолчачасдругойуйдетэтоназывалосьунегоподдерживатьдобрыеотношениятоварищамиочевидноходитькнамисидетьбылодлянеготяжелоиходилонкнамтолькопотомучтосчиталсвоеготоварищескоюобязанностьюмыучителябоялисьегоидажедиректорбоялсявотподитеженашиучителянародвсеменящийглубокопорядочныйвоспитанныйнатургеневеищедринеоднакожеэтотчеловекхотидившийвсегдаклошахисзонтикомдержалврукахвсюгимназиюцелыхпятнадцатьлетдачтогимназиювесьгороднашидамыпосубботамдомашнихспектаклейнеустраивалибоялиськакбыоннеузналидуховенствостеснялосьпринемкушатьскормноенигратьвкартыподвлияниемтакихлюдейкакбеликоизапоследниедесятьпятнадцатьлетвнашемгородесталибоятьсявсегобоятсягромкоговоритьпосылатьписьмазнакомитьсясчитатънигибоятсяпомогатьбеднымучитьграмотеиваниванычжелаячтоосказатькашлиянулносначалазакурилтрубкупогляделналунипотомужесказалсрасстановкойдамыслящииспорядочныечитаютищедринаитургеневаразныхтамбоклейипрочеесавотподчинилисьжестерпелитотвотониестьбеликовжилвтомжедомегдеияпродолжалбуркинвтомжеэтажедверьпротивдверимычастовиделисьиизналедомашнююжизньидоматажеисторияхалаткопакставниздвижницелыйрядвсехзапрещенийограниченийиахкакбычегоневышлопостноеестьвредноаскормноенельзятаккакпожалуйскажутчтобеликовнеисполняетпостовионелсудаканакорьевемаслепищанепостнаяониельзясказатьчтобыскормнаяженскойприслугионнедержалистрахачтобыонемнедумалидурноадержалиповараафанасиястарикалетшестидесятинетрезвогоиполоумногокоторыйкогдадослужилденщикахумелкоекакстрятьэтотафанасийстоялобыкновенноудверискрестиврукиивсегдабормоталоднотожесглубокимвздохоммногоужихнынчеразвелосьспалъняубеликовабыла маленькаяточнаяшикрыватьбыласпологомложасьспатьонукрывалсясголовойбыложаркодушновзакрытыедверистучалсяветервпечкегуделослышалисьвздохиизкухнивздохиизловещиенембылострашноподелаомонбоялсякакбычегоневышлокакбыегонезарезалафанасийкакбынезабралисьворыипотомвсюночьвиделтревожныесныаутромкогдамывместеливгимназиюбылскученбледенибыловидночтомноголюднаягимназиявкоторуюоншелбыластрашнапротивнавсемууществогоичтоидтирядомсомнойемучеловекупонатуреодинокомубылотяжкооченьужшумятнасклассахговорилонкакбыстараясьотыскатьобъяснениясвоемутяжеломучувствуниначтонепохожеизтотучительгреческогоязыкаэтотчеловеквфутляреможетесепредставитьдвانهжилсыиваниванычбыстрооглянувшисьсарайисказалшутитедаедвانهжилсыкакэтонистранноназначиликнамновогоучителяисторииигеографинекоегоковаленкомихайласаввицаизхохловприехалоннеодинасестройваренькойномолодойвысокийсмуглыйгромаднымирукамииполицувидночтоговоритбасомивсамомделеголоскакизбочкибубубуонауженемолодаялеттридцатинотожевысокаястройнаячерноброваякраснощекаяоднимсловомнедевицаамармеладитакаяразбитнаяшумнаявсепоетмалороссийскиеромансыихохотечутьчтотакисаляетсяголосистымсмахомхахахапервоеосновательноезнакомствосковаленкамиунаспомнюпроизошлонаименинахудиректорасредисуровыхнапряженноскучныхпедагоговкоторыеинаименинытоходятпообязанностиивдругвидимноваяфродитавозродиласьизпеныходитподбоченясыхохотепоетпьяшетонаспеласчувствомвинотвирпотомещеромансиещеивсехнасочаровалавсехдажебеликоваонподселкнейисказалсладоулыбаясьмалороссийскийязыксвоеюнежностьюиприятноюзвучностьюонапоминаетдревнегреческийэтопольстилоейонасталарассказыватьемусчувствомиубедительночтовгрядскомездеунеестьхутораняхутораживетмачкаитамтакиегрушитакиедынитакиекабакиухохловтыквыназываютсякабакамиакабакишинкамииварятунихборщкрасненькимииссиненькимитакойвкусныйтакойвкусныйчтопростоужасслушалимыслушалиивдругвсехнасосенилаоднаитажемысльахоршобыхпоженитьтихоказаламнедиректоршамывсепочемутовспомниличтоонашбеликовнеженатинамтеперьказалосьстраннымчтомыдосихпоркакнезамечалисовершенноупускалиизвидутакуюважнуюподробностьвегожизникаквообщеонотноситсякженщинекаконрешаетдлясебяэтотнасушныйвопросаньшеэтонеинтересовалонасвовсебытьможетмынедопускалидажеимысличточеловеккоторыйвовсякуюпогодуходитвклошахиспитподпологомможетлюбитьемудавноужесасорокаейтридцатьпоясниласвоюмысльдиректоршамнекажетсяонабызанегопоплачаготьконеделаетсяаунасвпровинцииотскукисколькоконенужноговздорногоизтототомучтосовсемнеделаетсячточтонужноуivotкчемунамвдругпонадобилосьженитьэтогобеликовакоторогодажеивообразитьнельзябыложенатымдиректоршаинспекторшаивсенашигимназическиедамыжилидажепохорошелиточновдругувиделицельжизнидиректоршаберетвтеатреложуисмотримвееложесидитваренькасэтакимвееромсияющаячастливаяирядомснейбеликовмаленькийскрюченныйточноегоиздомуклещамивытащилидаювечеринкуидамытребуютчтобыянепременнопригласилибеликоваиваренькуоднимсловомзаработаламашинаоказалосьчтовареньканепрочьбылазамужитьейубратабылонеоченьтовеселотолькоизналичтопоцелымднямспорилииругалисьвотвамсценаидетковаленкопоулицевысокийздоровыйверзилаввышитыйсорочкечубизподфуражкипадаетналобводнойрукепачкакигвдругойтолстаясуковатаяпапказанимидетсестратожескнигами

Код програми:

```
from collections import Counter
from re import sub
my_text = open("file_lab2.txt", "r+", encoding='utf-8')
text_one = my_text.read()
my_text.close()

my_ciphared_text_one = open("ciphared_text_one.txt", "r+", encoding='utf-8')
ciphared_text_one = my_ciphared_text_one.read()
my_ciphared_text_one.close()

my_ciphared_text_two = open("ciphared_text_two.txt", "r+", encoding='utf-8')
ciphared_text_two = my_ciphared_text_two.read()
my_ciphared_text_two.close()

my_ciphared_text_thre = open("ciphared_text_thre.txt", "r+", encoding='utf-8')
ciphared_text_thre = my_ciphared_text_thre.read()
my_ciphared_text_thre.close()

my_ciphared_text_four = open("ciphared_text_four.txt", "r+", encoding='utf-8')
ciphared_text_four = my_ciphared_text_four.read()
my_ciphared_text_four.close()

my_ciphared_text_five = open("ciphared_text_five.txt", "r+", encoding='utf-8')
ciphared_text_five = my_ciphared_text_five.read()
my_ciphared_text_five.close()

my_ciphared_text = open("ciphertext.txt", "r+", encoding='utf-8')
ciphared_text = my_ciphared_text.read()
my_ciphared_text.close()

key1 = "ля"
key2 = "кек"
key3 = "клев"
key4 = "круп"
key5 = "пожилаягиена"

def change_text(text):
    change = ""
    for letter in text:
        if letter in "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ":
            change = change + letter.lower()
        elif letter in "-!.,;:-»«?»()<>":
            change = change + ""
        elif letter in "0123456789":
            change = change + ""
        elif letter in "\n":
            change = change + ""
        elif letter in " ":
            change = change + ""
        elif letter in "ABCDEFGHIJKLMNOPQRSTUVWXYZ":
            change = change + ""
        elif letter in "abcdefghijklmnopqrstuvwxyz":
            change = change + ""
        else:
            change = change + letter
```

```
return change
```

```
def cipher(text, key):
    array = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
    result = ""
    array_length = len(array)
    key_length = len(key)
    key_index = [array.index(i) for i in key]
    text_index = [array.index(i) for i in text]
    for i in range(len(text_index)):
        result += array[(text_index[i] + key_index[i % key_length]) % array_length]
    return result
```

```
def decipher(cipher_text, key):
    array = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
    result = ""
    array_length = len(array)
    key_length = len(key)
    key_index = [array.index(i) for i in key]
    cipher_text_index = [array.index(i) for i in cipher_text]
    for i in range(len(cipher_text_index)):
        result += array[(cipher_text_index[i] - key_index[i % key_length]) % array_length]
    return result
```

```
def decipher_one(cipher_text, key):
    array = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
    result = ""
    array_length = len(array)
    key_length = len(key)
    key_index = [array.index(i) for i in key]
    cipher_text_index = [array.index(i) for i in cipher_text]
    for i in range(len(cipher_text_index)):
        result += array[(cipher_text_index[i] - key_index[i % key_length]) % array_length]
    return result
```

```
def coincidence(text):
    n = 0
    result = 0
    count = Counter()
    value = 0
    array = "абвгдеёжзийклмнопрстуфхцчшщъыьэюя"
    for i in text:
        if i in "абвгдеёжзийклмнопрстуфхцчшщъыьэюя":
            n += 1
        else:
            n = n
    for i in text:
        for j in array:
            if i == j:
                count[i] += 1
    for i in range(len(count)):
        value += (count[list(count)[i]] * (count[list(count)[i]] - 1))
        result = value / (n * (n - 1))
    return result
```



```

def coincidence_one(text):
    n = 0
    result = 0
    count = Counter()
    value = 0
    array = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
    for i in text:
        if i in array:
            n += 1
        else:
            n = n
    for i in text:
        for j in array:
            if i == j:
                count[j] += 1
    for i in range(len(count)):
        value += (count[list(count)[i]] * (count[list(count)[i]] - 1))
        result = value / (n * (n - 1))
    return result

```

```

def decipher_key_size(text):
    for i in range(2, 30):
        new_text = text[::i]
        print("Possible key length: ", i)
        print("Coincidence index is: ", coincidence_one(new_text))
        if (0.0553 - coincidence_one(new_text)) < 0.01:
            print("Key length is: ", i)
            return i

```

```

def search_for_key(text):
    for i in range(0, 1):
        alphabet = "абвгдежзийклмнопрстуфхцчшщъыьэюя"
        key = ""
        count = Counter("")
        for j in range(0, 15):
            text_new = text[j::15]
            b = text_new
            common = Counter(b).most_common(1)[0][0]
            if (alphabet.index(common) - alphabet.index('о'[i])) > 0:
                index = alphabet.index(common) - alphabet.index('о'[i]) % len(alphabet)
                key += alphabet[index]
            else:
                index = (alphabet.index('о'[i]) - alphabet.index(common)) % len(alphabet)
                key += alphabet[index]
        print(key)

```

```

print("Here is the plaintext!")
print(change_text(text_one))
print("Here is the ciphered text with the key " + key1)
print(cipher(change_text(text_one), key1))
print("Here is the ciphered text with the key " + key2)
print(cipher(change_text(text_one), key2))
print("Here is the ciphered text with the key " + key3)
print(cipher(change_text(text_one), key3))
print("Here is the ciphered text with the key " + key4)

```

```
print(cipher(change_text(text_one), key4))
print("Here is the ciphered text with the key " + key5)
print(cipher(change_text(text_one), key5))
print("Here is the deciphered text with the key: " + key1)
print(decipher(cipher(change_text(text_one), key1), key1))
print("Your coincidence index for plaintext equals to: " + str(coincidence(text_one)))
print("Your coincidence index with key 'ля' equals to: " + str(coincidence(ciphered_text_one)))
print("Your coincidence index with key 'кек' equals to: " + str(coincidence(ciphered_text_two)))
print("Your coincidence index with key 'клещ' equals to: " + str(coincidence(ciphered_text_thre)))
print("Your coincidence index with key 'крупa' equals to: " + str(coincidence(ciphered_text_four)))
print("Your coincidence index with key 'пожилаягиена' equals to: " + str(coincidence(ciphered_text_five)))
print(decipher_key_size(ciphered_text))
print(search_for_key(ciphered_text))
print(decipher_one(ciphered_text, "человеквфутляре"))
```

Висновок:

При виконанні даного комп'ютерного практикуму були одержані знання щодо криптоаналізу шифру Віженера. Було вивчено таке поняття як індекс відповідності та методи його використання при криптоаналізі. Було набуто практичних навичок розшифрування тексту зашифрованого шифром Віженера.