Варіант 2

Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут» Фізико-технічний інститут

Компютерний практикум №2

З дисципліни:”Криптографія”

Тема:” Криптоаналіз шифру Віженера”

Перевірила:

Селюх К. І.

_____

Виконали:

студенти III курсу

групи ФБ-95

Корольова В.Р.

групи ФБ-96

Гуменюк О.О.

Варіант 2

Мета:Засвоїти методи частотного криптноаналізу.Освоїти навички роботи та аналізу потокових шифрів, гамування адитивного типу на прикладі шифру Віженера.

Постановка задачі: У даному практичному практикумі,досліджуємо методи визначення ключа та процес шифру Віженера, в конфігураціях шифрування та розшифрування.

Хід роботи:

Завдання_1.1

«Шифрування довільного тексту шифром Віженера»

1. Вводим довільний ключ(довжина [2-20]символів)

2.Використовуємо перший елемент ключа та зашифровуємо один елемент текста,користуючись шифром Віженера(номер букви+номер ключа за модулем 32(32-адже в нас виключена буква «ё»))

Завдання_1.2

«Дешифрування довільного тексту шифром Віженера»

1. Вводимо ключ

2.Знаходимо елемент ключа з найбільшим розміром.

3.Використовуємо перший елемент ключа та розшифровуємо один елемент штифрованого текста,користуючись шифром Віженера(номер букви-номер ключа за модулем 32(32-адже в нас виключена буква «ё»)).

Завдання_2

«Дешифрування довільного тексту шифром Віженера»

1. Підраховуємо наскільки часто зустрічаються букви у всьому шифротексті.

2. Рахуємо індекс

3. Починаємо розподіл шифротексту на окремі частини,які залежять від циклу ключа(r).Рахуємо для частин шифротексту індекси відповідності.Для знаходження індексів відповідності проводимо розрахунок циклічно,а також використовуємо функцію «Кількість букв в тексті»,яку ми написали в Лабораторній роботі №1.Потім додаємо функцію,яка підраховує індекси та середній індекс.

4. Знаходимо максимальний індекс відповідності,який буде відповідати ймовірнісному знаходження (r)-розміру ключа.

5. Під час розрахунку максимального індексу,записуємо витягнені дані поділені по частинам.Якщо не записали,то розпочинаємо ділити знову.

6. Підраховуємо елементи в тексті, які максимально зустрічаються.Виводимо їх як значення ,які більше всього зустрічаються по одному для кожного з частин тексту.

7. Розробляємо можливі ключі за формулою (найбільш частіша літера шифротексту у відповідному шматку шифротексту(відносно r) мінус найбільш частіша літера в російському алфавіті).

8. Процес дешифрування зводитись до дешифрування з відомим ключем.А саме:проводимо дешифрацію по частинам ,далі записуємо результат по черзі в рядок.

Труднощі_1:

Проблема з розмірами масивів,куди ми записували букви,які зустрічали.

1. Не виводились значення індексів в деяких випадках.При використанні ,як значення для порівнянння налаштування if ,а точніше 32-розмр алфавіту.Що було не правильним,адже в деяких випадках в частину тексту не потрапляли декілька букв,що й не давало можливості ввійти в цикл і вивести значення.

Рішення:

Створили змінну ,в яку записували розмір map.

Труднощі_2:

Проблема с ключем для дешифровки.

Упускали той факт,що при відніманні від меншого значення (символ шифротексту) більшого значення ключа,виникаємо обрахунок(y1-x1+32)mod32

Рішення:

Проводили процес дешифрування за формулою:(y1-x1+32)mod32

Труднощі_3:

Використовували підстановку отриманого поточного елемента ключа та прорахувували для кожної з букв шифротексту.(івапр ---к(о)-----і-о:в-о:ф-о)

Рішення:

Використовували обрахунок відповідно при змінних значеннях виникаючих елементів ключа.

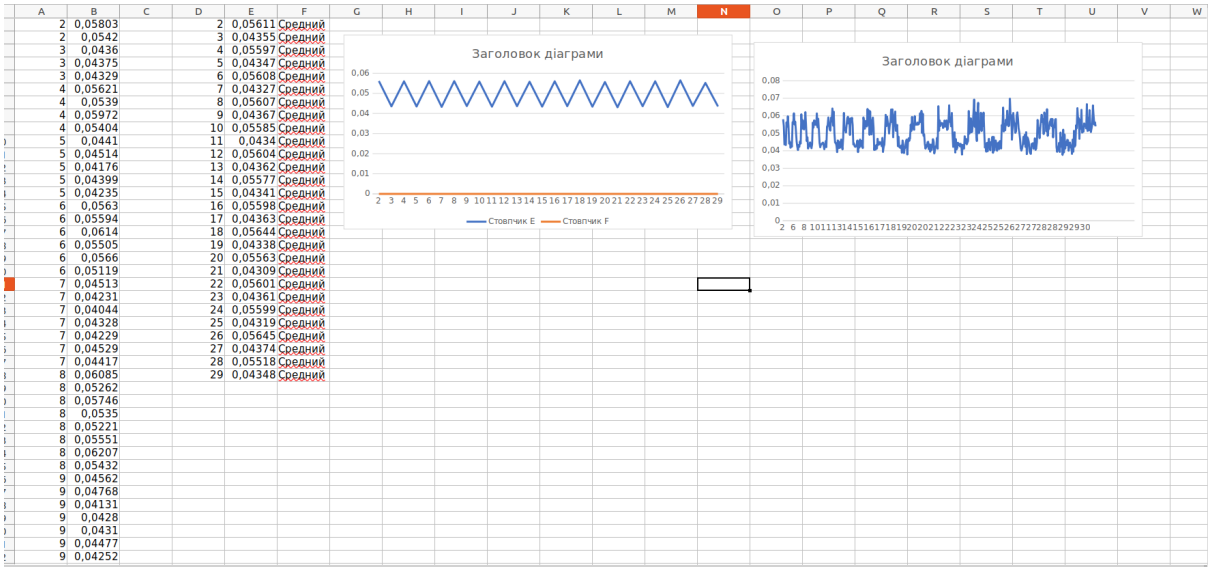
Завдання_1.1

Обчислені значення індексів відповідності для вказаних значень r (подати у вигляді таблиці та діаграми);

Таблиця+діаграма

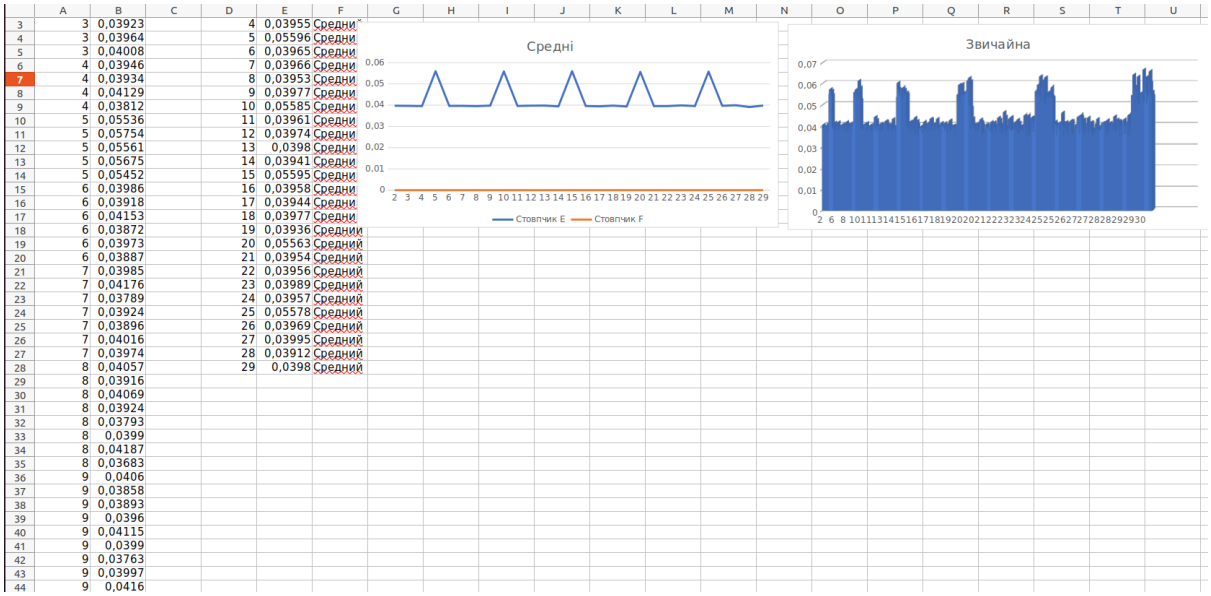
R1=бу

Варіант 2

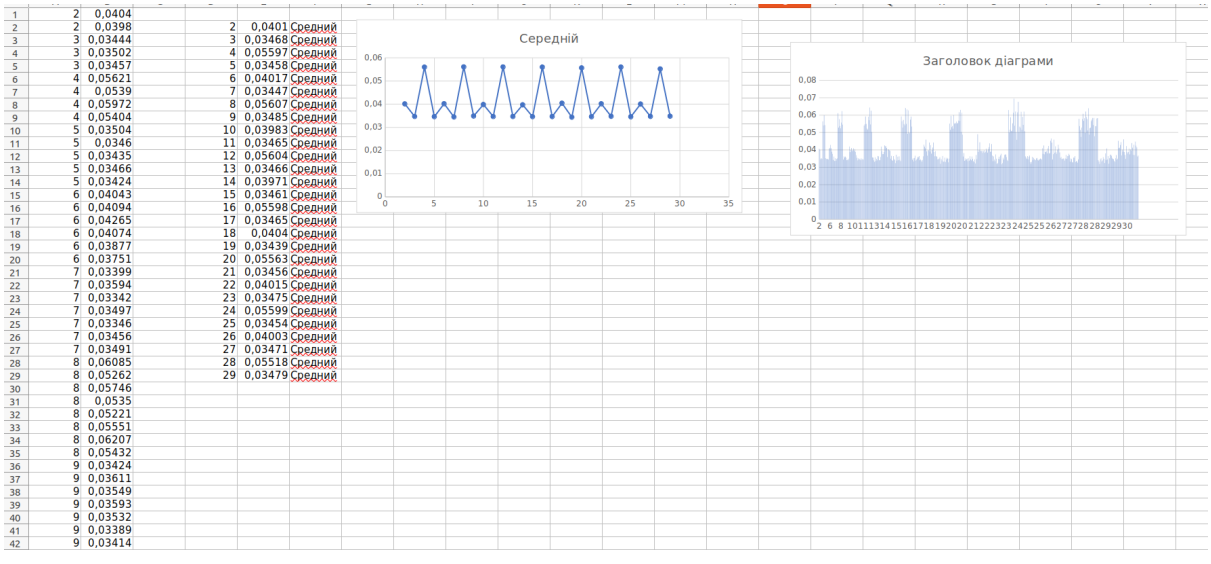


Таблиця+діаграма

R2=рех

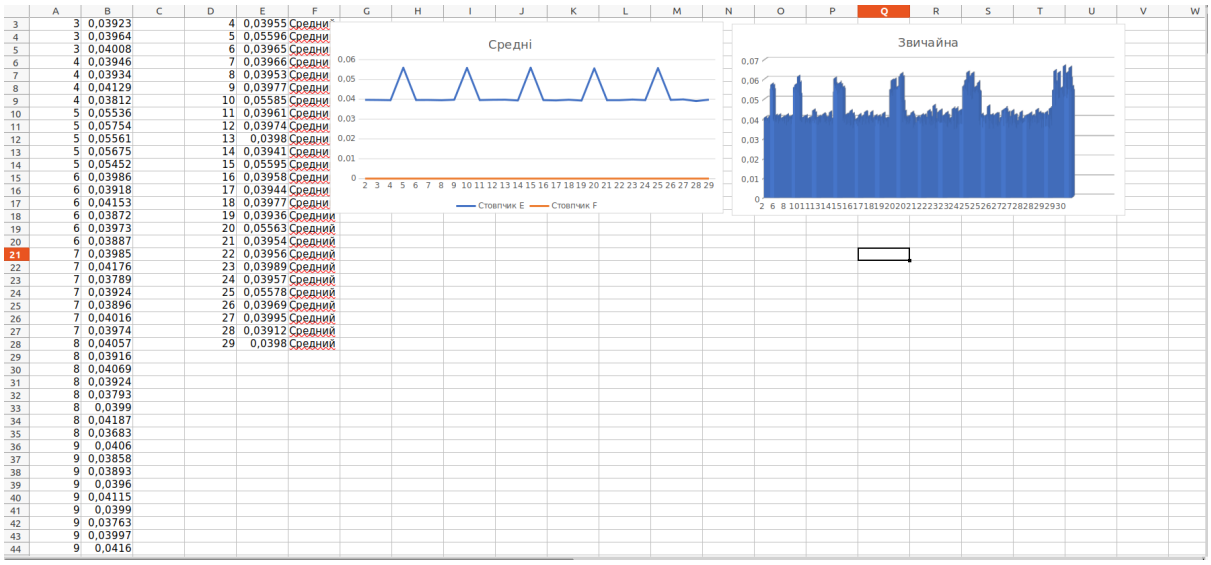


R3=ключ



Варіант 2

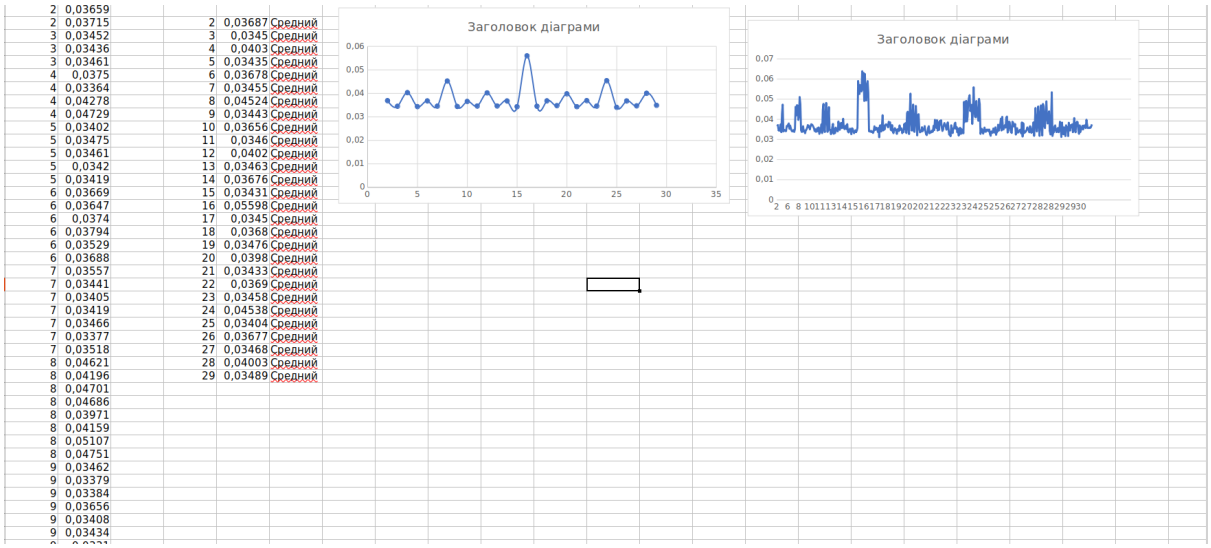
R4=кабак



	A	B	C	D	E	F
3	3	0,03923		4	0,03955	Середні
4	3	0,03964		5	0,05596	Середні
5	3	0,04008		6	0,03965	Середні
6	4	0,03946		7	0,03966	Середні
7	4	0,03934		8	0,03953	Середні
8	4	0,04129		9	0,03977	Середні
9	4	0,03812		10	0,05585	Середні
10	5	0,05536		11	0,03961	Середні
11	5	0,05754		12	0,03974	Середні
12	5	0,05561		13	0,0398	Середні
13	5	0,05675		14	0,03941	Середні
14	5	0,05452		15	0,05595	Середні
15	6	0,03986		16	0,03958	Середні
16	6	0,03918		17	0,03944	Середні
17	6	0,04153		18	0,03977	Середні
18	6	0,03872		19	0,03936	Середніи
19	6	0,03973		20	0,05563	Середній
20	6	0,03887		21	0,03954	Середній
21	7	0,03985		22	0,03956	Середній
22	7	0,04176		23	0,03989	Середній
23	7	0,03789		24	0,03957	Середній
24	7	0,03924		25	0,05578	Середній
25	7	0,03896		26	0,03969	Середній
26	7	0,04016		27	0,03995	Середній
27	7	0,03974		28	0,03912	Середній
28	8	0,04057		29	0,0398	Середній
29	8	0,03916				
30	8	0,04069				
31	8	0,03924				
32	8	0,03793				
33	8	0,0399				
34	8	0,04187				
35	8	0,03683				
36	9	0,0406				
37	9	0,03858				
38	9	0,03893				
39	9	0,0396				
40	9	0,04115				
41	9	0,0399				
42	9	0,03763				
43	9	0,03997				
44	9	0,0416				

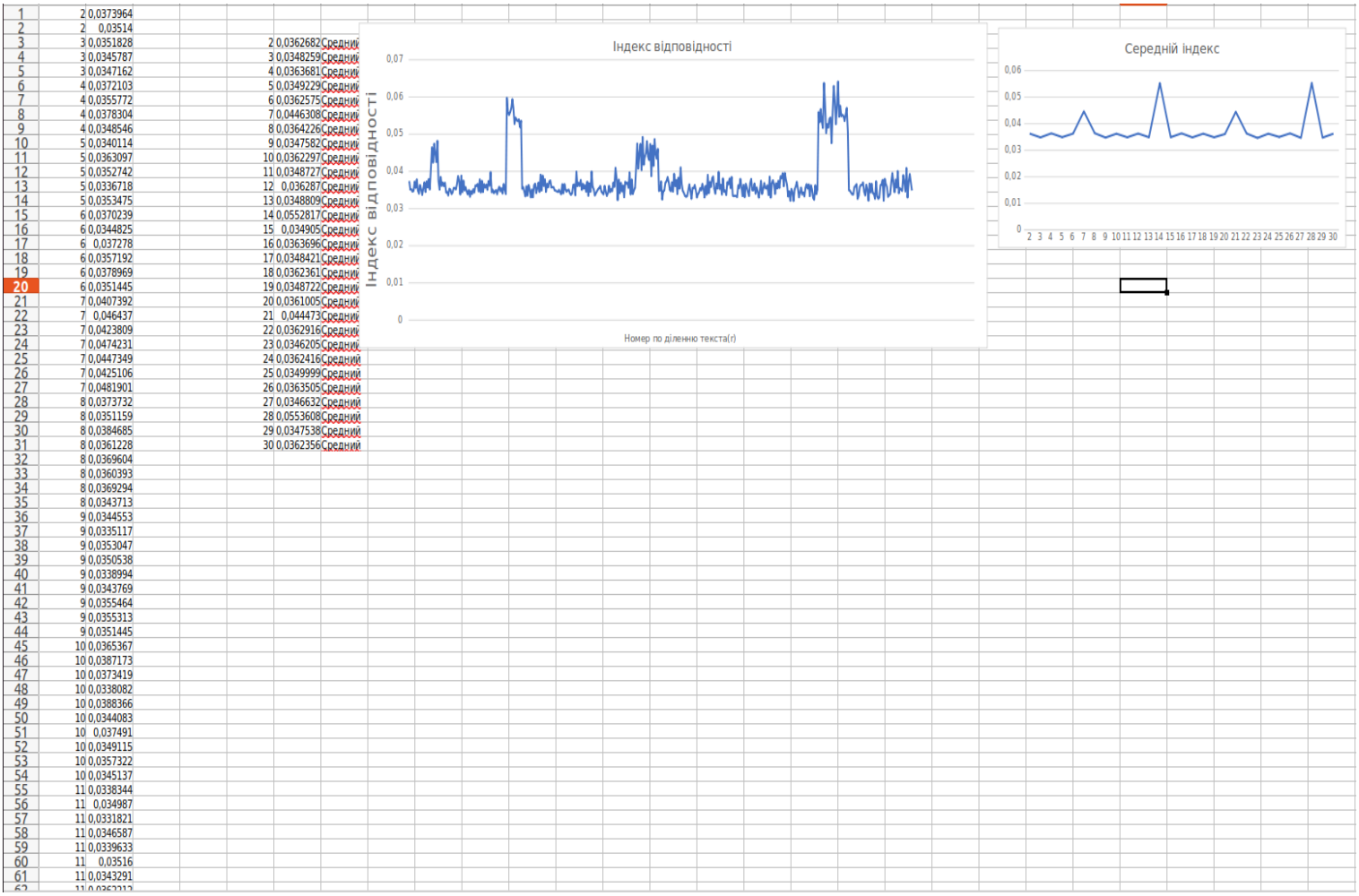
Варіант 2

R5=кириешкивсметане



Обчислені набори значень індексів відповідності,одержаних при встановленні довжини ключа шифру Віженера (подати у вигляді діаграми);

Варіант 2



– шифрований та відповідний розшифрований тексти (відповідно до варіанту

ШТ:

Вариант 2

щоыкцрылжцьштхъогзцуэцъмщкубфющъуытфьбахсюьувчузюмопощквкъмьчтмусуьшюхуцтрцоэитсуряхяъъыежърцярос

ыотюрщмчщсфьйоыоюыуъоэиътшйдхъьъхефярцйыхявэцьщзхщцыфущкборяэййшдцчмцубжцюхшмяилхэвгшсоьлмтшц

ытъиоуянюбкршрчюгмчфщцшбвъинэьтьтэчшлцциучеутъхаюятужифкчтщььэщявтчлшообцуафъцгепхщумямщмьйэужй

энмдъптрчрмърйюхьпцйыхрувлейжннчщйувфющмапыэчпьлыюыыцнцйрмйщьтьфьыюльйякофахъбъьцьшрэиудыхлвэцю

пнжхмьдщгыроюцлпъхзмйямюгъоаыуцхккящхфряшяцнъышйхшчобьуыццаьцфебшахщоьупдьнфашпэюбоэшкстэлдазува

цьжцонпйпнтцжэсцькфнщчжямъяэпсохтпнфтьщрхбыцъхдпрфаывчвкрмьэмцфйзазшяэщдвнпыщехщъершыяшуцикдхжп

чяэецчшжищбмгуоуэрглпктхйлййообъсоерхкцйшзахтьбуоуыъчрбюаюяошшнъкнкъмщмъххтдшнрххйхахщмщьюрмснясц

уткэпегщтйщцпйаийвлцввнхшнцдцфутэхэщлсыцшфулуычанхчтюрфаымурщаяьрдоноуюхпюяъяэепмйчфцшцуьогзкжхяи

уьфцыпмющсстхощрзарфавурямхорькбяяьъэнснчицйряыэчфрцйэччхъхаафщвржйьцнськцяэтхррсыщутъиьвчыылфйюцуу

ьлпаэящцзжыпнчгяоуьбънфйэннмцшехцлгщьцыщчжущняэттыуххушйюмтбэпяффйюцуьокыгърархйсъвйафьякаскцаьцтр

ощкбсыпэксйъосцфускцяшныглчсупхьфыщцухйзштэчуцьуэюухяилдщшнэпецэзйэъчрятьхчяглттпрфтягрбфгяцуиъноуоч

Варіант 2

ьвыьцоуииэйсцжбцфыцыехюнсжотяпруьжстоуйышхърщьыйьмщрсзщзъшэямъепюзцдэмяющюстзйэхьжжпяммаянцйрмй

уюхзхюящаупылсыушшшчяыылчапгютгцьчптщкцитуйпжзсшсййррснъщйапчгяьуртаюыхфосотрувбзйяхднщзпшяцюэнлзн

нйыфйесюцчкстфудъмыэкгацнцъиноьщьакъщькфтучсцошюфхсьчяпаойымпющьцоййьцудъфмббуьурмюдляяхгичувэкеш

рштгхфшфысъхморыячуьаэхячзалхчоэмюхяьвэуотбоьокрвэюяфцпысъчъчоъпшсчксъгтпоицачыгшеоэгфмэмюхющцэксъг

ожущршчукрфйэкднятъщвфцшконфоскъфхаацшамытцдхфоъэъмрццтхдрышшюсяыщитыьсхофьзььфщйтфцщдрмсюабэрх

йдхчрьищшжкцъухшннсцуббчщцщрсгпглдщпщбоцшьшрэиудрчуръкюжорхшшфнуьтщотутйялохучоапхдчкйящиьуыбцфя

щпкпптщйятуроэягецикйгягявэньъкфтмцмъфбъпшылптъфчзъмыпээцыкихъежулкюьэягкпъишгавчбъьълдсняйпрвгюуцгз

нлюыхфосоъэсхлдчпрнйщюаювацмдсхяозьфуяэщдвейящихшзхръсцькфсипйымсыотршертхицьййифщщтцчщшйоофояян

эюгмфчицькьбъьрнтдюъчгзпчьчюршкхщцмхшчйвлбхузптхсгтзевэацмдчсрлпнмапюьчлрушнадъпышжуфщтйамсжщжув

фяьуийюнщлоььэфааыкуымцйящцььувйхуэррчымсюрбхрчтршчрывчткпяыдтдницаъфьуэсяшклъизмлщьюрцхшухчирдщку

бфювкйарцщттмдъччрькпъишфьщцттуврхдюучкцтюгщцюлптшнцгглоцфсяцужацшчящцырбхэужднхцьюбтааущздшщлт

мйцэвоюэусвцщтжпчьпсуькзсинтящцупугьзттлчрькбйфягнежъыпсьмрафърьпдфифьуыэющоюрццнхоькубфяуцшкхяицй

жгяшъкюркуытйсушарьуйзцмшдцйуфуюсщспкйедляяущыофукньцудымьтъохркьйкдхжмчьпсщросткфйхмжмсьалцсинх

йящогбуткцмяыйъцжбэчшсцбснзыяэхэръэяпусьцхтюацыаншлппмъсйвъоапыгжццнуляяяцьыофщсстйьибюцъмаячшзыъч

жйутрвацмдйюъехцтофпамюсйтаеймъэапрькчахъчыяхалаабюйтщмопотюрькйрчйьнщаымяюааснргтъшфьищхыяыщрачц

ыяэчьскщюльйякофахъбъьцьшрэиудцшцфчжнхеоърлыууыхрйулртъцлтащьзфсяэастыхйщчоэлжцщтлнфчпезщпьодвшхй

йчфцшцуъогзкжхяъоооояыорыщтъттчсдхртауаынлъизщещьпууьлглъиамамщмьйцюцутэстщгсрарцэрдъинйщзуилщцоптъш

слызщуфяцычяунцйяхрбфъщпнтяяытпвыхяюшннжнъехнфьбфчилццихйуьуцэпуйзсстхотэваээсянуихъопнсьвэюмффтшлч

иоцьъпасццгъипмсъщпдцупхчрщопхзюгъкфщттдхчзьыуаяобутйяэькуооавцнхефйнщськьбпъяьздшикйщзхрсувщсжскох

апаюьыиэууыурйашусфэяьфмэифмрвучхоцэнлчищаучорянхщсуэцшдящктаьгшгртъщтрзарырюумчтмыцтчбучувлстюкйп

йхтээаущксткофыхуфсцчртмтшолшпчяэряыуцэыфгцтцфяьфшшжеиисоцуфпщщшузнчфтгхпгуугнцйщччсцуооошщнтчш

хчгрййбзцццшкфпифхниьачящотдядожцюлвэрмчксмцыуюзршъцуъузыхзлосьббуъкчйозцмрюуьыудъхйчизмэварнянчттрц

хчызбзчаньпдфифзушуачтянупйхчсуцьбъухщздянфаыхтюроуурщыпъецйхтэпфхжнтятйлотяпрйгзстхфыыуфцъэъръхтщцф

ыотьвщюмнфдьтъжутцъччфрцйэпйжнойтпщгрцйщтссоиоэбцыкуеъищчфпщзфамыкхпнпйыгшшфукрфдвхьэцмашюьфые

шютчншчобщьъоелтъцяуййафхыушдчщсцюпвюбьфыешхрыфцййафхыужяшрцдофсыччвхуръицмгжцбэябрйтяцамщшнт

юубншвыяофулкяфюулджишолшээафтвэежшзфдяхпюшшяыуцчызлоуувщбяъхтхщбйящршчргюхмюъсыушшюыогэхдчю

стымэюухцчкпйзбтатоэуцщхеомччснтрнбьэтежтмосцптюсььзттяиумпзыръкющсжншсдыщуъэъюлчяюъщдгзцчцогръсхяо

хшпгэфэяцеиыттштсппавявхнняыщмящэюухцчкпйзкящпхрщюмэауыусъцжэаэряпнцэиъхщмтюсоюукмпгихыжувьугцнжя

шйзулцшсцюжфйэщчсототбьблдлнфоцшзплъоыюйдьцнфьиыхфэбцчйвхсыушшшфыцъупнмумбнуэфпмцусхщфтрзахщяг

мапънхсьншюабжщздягхионуяфтсшчмдхдряфоапяглгэхфлтщфуэчуэкффыясцотевээяонеертирзтжпащъдцхуоцыпчтчшгщ

хуэцютюхргжцььджкмсспъюуашячшсхкофяпахбутжрхихчрюъябщьфщфтшрымшзряэтшрсйшдитацюрсцььджщнъцушых

сувэуньшспущутзуъумфыщъмцйоыфющрощыфутызюгщожхуцышчнцшшюьесццгъъштамюшщюяннжянхсыщуввющьчм

днъоькърбаблпъхццдшщьвээцыкфтпйпуубуэюьщнпхяытахэхяубрмдшцкйтхщртовуййшкхйящубьуурццыслпьлъзщуыщчт

эиирулщхъыяъряшиштшчьтпряфхйчнхйщсъщцоюлзоткчоюъсчпъылздщчсфьйрюцъясттхпъцуфйвэюилрдчиуднщцыоаабл

дктуолшзшюбьблдмьцфтяфбыпрщхчтэыштжмуфэещгэежсцжцькььфяглджфмчщцыъщшюьвчуцэнфсокубфюсючйозлхуктр

цоэрьдянфаыхэюъбилртюджблшррыэщцыерхщудхзщифвюлцйчыцибхаюярснэмюдчцяйьшдпдчезяшоцкжхрыугхееиуймхс

оъэчгщлйшъчнжхаыпыхъптцлйлущуэщцщнуцяыыюьфузььчрежящцфошяъпхсцццэибсбецббьбугуэцътрчуьфыюжъжнфш

мюхръэаяыайпцхфосурбаблпъхццтршьбваыыужйщлтцьфхяаурймъщыжуфыюшьбуимъифаыхчффасцбвогфтбщрхяфхртм

тоьфызщшаасвчтыйдыыхррыэщыажищйхййообяущнщцунщцрфуэпяэрхцйхчфбшяъччвэшитхыоосэюъьчрттэыъхшхъгрйь

шехяцфашхэмоыиэуетмцячяьвъоюпцохслдъццабьчрмдвфопутцгсщцхцгънърьщюпьоуьгцэиммефьббкщьчтэрсгхзяьфнььд

ктуыдницюхаясщтдпцлхууъшяуяпнснтчжошшрцоьокхтшцйэхтэчъскипнпъдъхугховшуйдъчцосрбфцтжртютйлотнъяьэрфа

мхъцрзшюьуишуоэыпооцттпхсщжйсцххькщрацььдзтщофематфюглджишолшзплъощттпдчцтцьфоифчфлмйягцйшчыыэсв

щжтшнрсьйоэчньрусхмьуюхгюяьуюййъыыдаъсюабхлххякосыхчфвъмвкнюгццюзсшжувхнуылсенйхпъщцьчтчьйоязлвэш

сждмьшоиэхщртоьмапымчсушуэчуяэттдхчзьльчэюсоуфымйбтпысвюфлэтяуйстпнтфщцхуеэрыдыпнэфъющлоыхотпвеэк

Варіант 2

ъяхелнуъгщпжмптбрцдящйрсмяхяоюруутшйццйылштцсшфъгтмщпюгщьущймянфаъмффвысыуиъцмтьщтхъощэусьръаъз

егбктщрйтусыывчзфъащрдриоцяжрюгцзуепйхдщтхшгыуюэещнщчиучфрьццчксмхочтпршъьвъхмютчфппуьаьямюдтфшт

юмхгъкглчдщъвдамщмььаыужтмосыхсюуьушшесхзштщфопюьгрхгчшчжццюшцысхужххсъцздшчыцнагпуосьцююсухртс

инштцшшшяушюраяиыгрфуфпщщъхмпуоыуфйывейукххудйятцьэяыщзхчцоталуыфыщрцыхъййафуюргяпнрифцдэчотча

нъкфтмйжорярыйцэкушгоуюпрхбйяцбзтцайыгюрухсэкемщыдювчъэргщхтцусхахшдпшвлуцюыыхайьтпщууймщцыдъий

ычяыцгыхъопкфььчеюжоцттъцэхлвэъдуфтсчсхцжыхврщпкпбцхдщмюьэыгъпдфифзушуатщснеыьгъфдыляъэсяпулышйха

зюлштбюидрирдтъъзчряъхтязцчщжхэпещэтдерллстнфкьакчапщыфущцычяншкцаощттшатфыюуппхццрцьошъбпыбйпра

чязъбююяьньйщудхзщуфяцыдтсшьзьушюмаяхурнхнмюсьнбьфрцйэпйуыъщбоцвкзсифцйтхрюъквэзтщччоьшцыанюлрмюъчошхлвэшяичтянкгбнуэфшсьейящигэхяьзабррсньчц
ькюргцщчупымчнемщюсуыичтхйдппмтюъофлзмчъчфтмргзшсьуж

юнхвызнхтьюрзйюъйыахагбсспецйрхчфпшяэяглхьтцыйдйцъбьблптюкосывуфпыюжкзыкчфнщьэпэспксхрлдъццапыяъуы

тфьхцщбрецрэхйоыюцызжхтьучкьнъопкшатпяаыуххуисояцбэьгрыйюълйыфцъчесьчйъдутсппэвашлхчонптъпьвсоэънфык

ытфмрльухщзйэзоцуыььфццоууымамымыэкъхщзйэззсььшдъсцутьгыджхаыпыхудрхшцднъмвьорьфтчцтсожявяоюлусх

фчзбщыхаэблзмядъгощйзпягртачцсруттхъьвнерьрщдъпшюьуишумпщоцосцффщянчтщяытукьюбузъупхъсосмяхяэячуфж

рфхнлоъпшяфусьцфмапшсчхюрцртхшфьиюръярнййыыыдавыртььщцтпицмньфьфаышуучршталпгюькыюптэцыоьпнбьыю

щтйпнщвещьэфаяьуеысшфцюцэксцькфппнтгфбыэацбгсыасирзтжпанцкцъирдтийыэзбрййшнцоосэюбуюбндшдцячшрхбщ

мфнсыснтрхщмььвураъгттапышецсбнмыъудхзщбоьтеджхкацьььзфаяьчдядъгемщюсуыщсцтфцягшюрцбчрфтюуйпэчьзлы

яьтдщцршттлуахцулрсттчцьчйхщьюэеоягсськтрюьэщидшзумрфбыуовцшынсщйтсцщьуилццыузицхаъпхмневящитащоъчг

ущмрыоцтящущжаящчоэглдмщяпюубрймъгхмъхфээяылмдядацьжегсягншвюнкгрпыюсогжсутшоиэчьеэюянарюъйфжпъ

бщошлрзтщофцмяычбчшкрыльуьуъзлямшшцыхоуьорюъмцоучортъуъчвчпцттдчирдыфйьбйащкитаежллцэрбботдцмоькд

аютъвюсдюаоижмсющюянухыщймюзхтфуйзфтпныфбдаюрйъхмчирсьжцсфхгщитъньтппюръярьфтэрыашхнэфряцбсыпй

уыъщбошяойдшныйагхрштщнсйумьсочьфьйъщчитуыйпмтюъфюжжяшрштткьвэрцэбиытъруфалрцьрчяснцаспцыфсцшй

ч

ВТ:

КЛЮЧ:----------

завдання), знайдене значення ключа;

Висновки:Було засвоєнно навички шифрування шифром Віженера.Опрацьовано умови шифрування з відповідними діями та операціями ,щодо відкритого тексту з перетворенням за операцією мод в дешифрований текст.Також засвоєно аналіз шифру Віженера в умовах розшифрування даного шифрованого тексту за обраним методом знаходження ключа,при врахуваннях індексів відповідності,посилаючись також на ймовріності найвживаніших літер заданої мови(російської).

Варіант 2