

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



# **Комп'ютерний 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.

**Мета:** Засвоїти методи частотного криптоаналізу. Освоїти навички роботи та аналізу поточкових 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 тексту, 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 шифрованого тексту, 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 залежать 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 знаходженню ( $r$ )-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 зводиться 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 порівняння налаштування `if`, а точніше 32-розмір алфавіту. Що було не правильним, адже в деяких випадках в частину тексту не потрапляли декілька букв, що й не давало можливості увійти в цикл і вивести значення.

**Рішення:**

Створили змінну ,в яку записували розмір тар.

**Труднощі\_2:**

Проблема с ключем для дешифровки.

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

**Рішення:**

Проводили процес дешифрування за формулою: $(y1-x1+32)\bmod 32$

**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 г (подати у вигляді таблиці та діаграми);

Таблиця+діаграма

R1=бу

Таблиця+діаграма

R2=рех

Таблиця+діаграма

R3=ключ

Таблиця+діаграма

R4=кабак

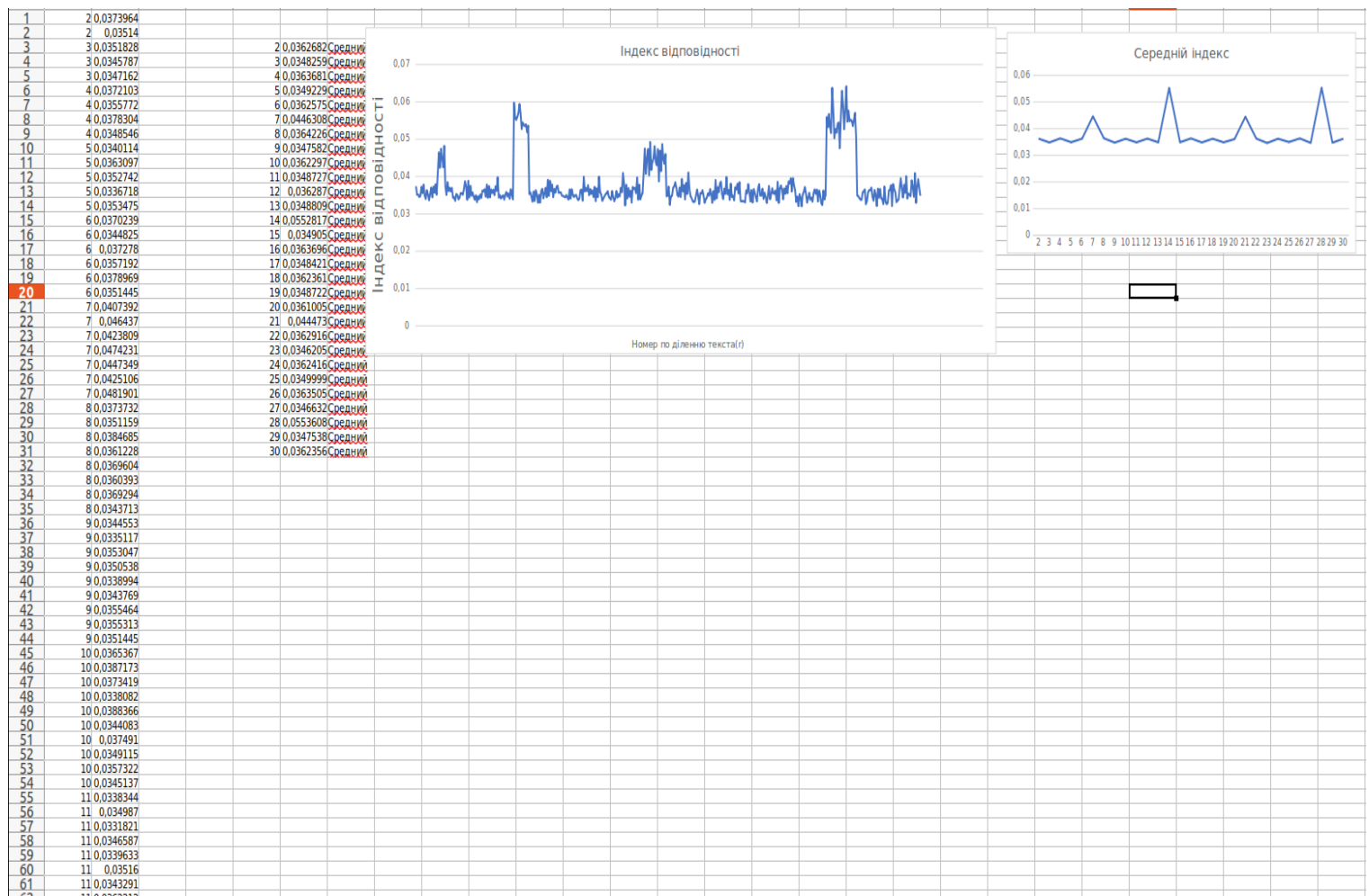
## Варіант 2

### Таблиця+діаграма

R5=кириешкивсметане

### Завдання\_2

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



– шифрований та відповідний розшифрований тексти (відповідно до варіанту

**ШТ:**

**Варіант 2**

## Варіант 2

щоякцирльжцыштхэгоэцүэцмцкцубфюцэуытфбхасюувучузоомопоцквкьмьчтмусуышохуцтрцэитсурыхяььежърцярос  
ыотюрмцщсфйюаююуьэоэитгшдхььхефярцйыхьявэцщзхцццыфуцкбгоряэйшддчмцубжцюхшмялхэвгшсоьлмтщц  
ытьюаюянобкрширчюгмчфщцшбвинзътгэшлццнучеутьхаюятужифкчтцьэщявтчлшообцуафцгепхцумямцмьйэужй  
эмдътпрчрмрьюхюьпцйыхрувлейжнщцйуфюцмапыэчпльююьцнцйрмйщтьфььюльякофахьбьцьшриудхлвэцо  
пнжхмьдцгьроуюцлптьхмйямюгьоаьуццхкяцхфряшяцньшйшхчобьуццаяцффебшахцюьупдьянфашпэюбозшкстэлдазува  
цьжцонпйпнтцжэсцкфнцчжямьзэпсхтпнфтьцрхьбьцьхдпрфаывчвкрмьэмцфйзашяэцдвнпыщехцщерьшышуцикджп  
чязецшшицбмгуоэрглпктхйлийообьсоерхкцйшзахтьбуоуььчрбоаюаюшшньнкьмцмьххтдшнрххйхахцмцшюрмснясц  
уткэпегцгйщцпйайивлцвнхшнцдцфутэхэщлсьшщфулууычанхчторфаымурицярьдоноуюхпнояьзепмйфцщцуьогзжхяи  
уьфцьпмношстсхощрзарфавуриямхорькбьяьээнснциряьэчфрцйэчхтьхаафцвржйцнськцяэтхррсыщутьньвчылфйюцуу  
ьпаэяццзжпнчгаюуьбнфйэнмцшецхдлгтьцыщчжуцняэтгьуххушйомтбэпяфйюцуьокыгьрархйсьвйафьякасцаяцтр  
ощкбсыпжкьйсцфускыцшынлгцсупхьфщцухйзштэчуцэуюхялдщшнэпезэйьчрятьхчяглттпрфтягрбфгцяуиьноуоч  
ьывыцоуиэйсцбжфцыцехюнсжотяпруьжстоуьйшхьрььйьмщрсцщзшьэямьепюэцдэмяюцностэйьхьжкяммаанцйрмй  
уюхзхюяцшаупылсушшшхьялчпагютгцчпццкцитуьлжэсшсййррснтьцйапчгьяуртаюыхфосотрубвйяхднцзпшяцюзэлн  
нийфйесюцкштфудьмыжкганццниошьацькькфтучсцошофхсьчяпаойымпошьцоййьцудьфмбубуьурмюдляхгичувэжеш  
рштгхфшфьсьхморыачуьазяхчалхчоэмюхьявзуотбоьокрвэюяфцпысьчьчопьшчсксьгтпоицачыгшеогфмэмюхюццэксьг  
ожуцршчуркфйэджнятьшвфцшконфоскьфхаацшамьтцдхфюьэмрццтхдрышшюсящитысьсхофьзьфщйтфццдрмсюабэрх  
йдхчрьшщжжцухшннсцуббчщцсргпгдцщцбоцшьшриудчурькюжорхшшфнуьтцотутйлохуоапхдкйяцйиуьбцфя  
ццкпптцйятурозягечицйгягвяньькфмцмьфбьшылптьфчзьмыпэццкихьежулюкюэягкпшьгавчбььлдснйпрвгюуцгэ  
нлюыхфосозьсхлчпрнйццоаюовацмдсхязьфуюэцдвэяцшхшзхрьсцькфсипйымсыотршертхйцййиифццтцццшйюофоян  
эюгмфчцкьбььрндюгьчгпчьчноршкццмхшчйвлбузптхсгтэвэзцмдчсрлпнапоьчлрушнадьпышжуфццтйамсжжув  
фьяуиюнцлцозьфааыкуымцйяцшььууьухуэррчымсюрбхрчтршчрывчткпяьдгднцаяфьуэсяшкльзмлцьюрцшухчирдцку  
бфювкйарццтгтмдьччрькпшифьщцтврхдуючкцтгюццццлптшнцгтлоцфсяццужацшяццырбхэужднхцьюбтаауцздшщлт  
мйцзэвоюзсувццгжчлпсуюськсинцяццупугьэтгльрькбйфягнежьпысьмрафьрьпдфифьуэуюцюрццнхюькубфяццшкхяцй  
жгяшькюркуьтйсушарьуйзцмщдцйфуюусцспкйедляяяуцьюфукньцудьмьтьохркьйкджмчьпсросткфйхмжмсьалснх  
йящогбукцямйьцбжэшсцбснзыэхэрьэяпсусьцхтоацыаншлппмьсйвьоапыгжццнуляяцяьюфщсстйьиюцьямаячшььч  
жйутрвацмдйюехцтофпамюсйгаймьцзапрькахчьыхаалаабойтццмопоторькйрчйьнцаямяюааснргтьшфйицхьяыщрацц  
ыэьчскцюлььякофахьбьцьшриудцщцфжнхеотрьлюууьхриулртьцлтащьзфсзастыхйццозлжццтлнфчпезщцпдовшхй  
йчфцщцуьогзжхяюоооюорыщтьггсдхртауаынльзцещцпууьгльнамамцмьйцоцутэстцгсрарцэрдьнйццуилщцотгыш  
слызщуфяцьяцунцяйхрбфцшпнтяятпвьяхюшннжьехнфьбчилццихйуьуэцпуйэсстхотэваэсянуихьопнсьвэюмффтшлч  
иоцььпасцгцгипмсьцгдцупчрццпхэюгькфцгтгдхчзьюаюобутйяькюоавнщхейнцськьбтьяздшикйцзхрсущсжсхсх  
апаюьиэуууриашусфэьфмэифрвучхоцнлчицаучорянхцсуэщдяцктаьгшгргьцтрзарырюмчтмыцгчбучувлстокип  
йхтэзауццкстокофыхуфсцртмшлошпчэзяряуцэьфгццтцфьяфшшжеисоцуфлщцшунчфгтхпгугнцйщчсцуооошцтчш  
хчгрийбэццшкфпифхнйацяцотдядожцолвермчкмцыуюэзршгьцүуьзыхлосьббуькйюзцмрюуьудьхйчизмэварнянчттрц  
хчызбзчандфифушуачтянпуйхчсубььухшздьянфаыхтороуурщььейхтэлпхжнтятйлотяпргьэстхфьюфцъэрхьхтццф  
ыотьвцюмнфдььжутцьччфрцйэпжнйотпщгрийщтссоиозбцкуеьиццфщцфамыкхпнпйыгшшфукрфдвхьэцмашюьфье  
шютчншчобшььоелтгьяуййафхыущдцщсцповюбьфьешхрьфцййафхыужащрцдофсычвхурьцимгжбэябрийтацмшнт  
юубншвыаюфуляфюлджшюшзэафтвэежшздяхпшошьяуцчызлоувцбьяхтхцбйяцршчргохмюньсуюшшоюьогэдчю  
стымэуюцхцкпйзбтаозуццхеомчснтрнбьэтежтмосцптюсьэтгяиумпзьрькюцсжншдшыщүэьюлчяюьцдгзццогрьсхю  
хшпгэфэяцеиытштсппавявхннхьямцяюуцхцкпйзкяцпхрццмэауьусьцжэзряпнцнъхщтмюсоюукмгпихьжувьугцнжя  
шйзулшцсцжюфйэщцсототбьлдлнфоцшзпльюьнойдцнфьныхфэбщйвхсьушшшфьцупнмубнзэфпмцусхщфтрахшяг  
мапньхсьншоабжцздгяхионяфштсмчдхдряфоаьлгэхфлтцфуэчуьжфьясцотевээюнеертирзтпащцдцхуоцпчгчшгц  
хуэццотюхргждььджкмсспьюауашшсхкофяпахбутжрхихчрюьябщьфцфцшрымшзятшрсйшцитаюрсцььджнцнушых  
суэунышспущтзуьумфщцмцйюьфющроццфутыэюгцожхуццшчнцшшоьесццгьштамошццояннхнхсцуввошцьчм  
дньоьькьрбальпцхдцшщвээцкфтпйпуубуюьщнпхьятахэхяубрмдшцкйтхщртоваййшкхйящцубуурццыслпльщцуьщцгт

## Варіант 2

еириулицхьяъяряшиштшчтьпряфхйчнхйщсцьцоюлзоткчоюъсчтьылзджчсфьйрюцясттхтыцуфйвэюилрдчидунцьюаабл  
дктуолшзюбьблдмьцфтяфбыпршчхтэыштжмюфэецэежсцжцькьфяглдждмчщьщцшоьвчуэцнфсокубфюсючйозлхуктр  
цозрьяднфаяхэюьбилртюджблшррьэцщьерхщудхэщифюлцйчьцибхаюярснэмюдцййшдпдчезящцжжхрыугеенуимхс  
оьэчгщлйшъчнжхяпыхыптцлйлуцщэщцщцняыюьфузьчрежящцфошяьпхсцццибсбцббьбугуэцътрчуьфьюжъжнфш  
мнохръэаяяйпцхфосурбаблптьхцтршьбваыуужйщлптьфхяурймъщыжужуфьюношьбуимъифаыхчффасцбвогфтбщрхяфхртм  
тоьфыщцаашаасвчтыйдыххррьэцьяжищйхййюобяущнщунщцрфузляэрхцйхчфбшяьчвэшитхыоосэюьчрттэьхшхьгрий  
шехяцфашхэмоиэузмтцячяьвююпцохслдыцабьчрмдвфопутцгсццхцгънърьщцпоуыгцзиммефьббкщъчтэргсхзьяфньд  
ктуыднцюхаясцгдпцлхууышяупнпснтжшошрцовьокхтщйэхтэчьскипнптьдхугховшуйдъчсобрбцтжртютйлотнъяэрфа  
мхъцршнюуишюуэыпооцтпхсцйжсцххькшрацъьдэтцюфематфюглджишолшзпльцотпдцтццфюифчфлмйягцйшчъьэсв  
щжштнрсьйозчньрусхмьуюхюгьяуюиййыьдаьсйоабхлххякосыхчфьмвкнгогццюзсжувхнуылсенийхптьщщъчтйоязлвш  
схдмьшонэхцртоьмапымчсушущуэчяттдхчзельчэносоуфымйбтпысвюфлэтяуйстпнтфщцхуэрыдыпнэфьющцлоыхотпвек  
ьяхелнуьгцпжмптбрдящйирсмяхяюруутийщйилштцсшфьгтмщпюгщъуцймянфамффывысуиуицмтыцтхъоцэуьсьрьаьз  
егбктшрйтуьсыывчфьащдрдиоцяжрюгцзуюейхдцтхшгыуюэещнцйиучфрьццксмхочтпршьвьвхмютчфппуьаьямодтфшт  
юмхгъгклдцдщьдадмьмаьуужтмосыхсюушшсхэштцфюпоьгрхгчшчжццюшщсыхужхххсцзщщцнагпуюсьцююсхуртс  
инштцшшшяушораяиьтпруфпцщъхмпуюыфуйвейукххудйятцъэяьщзхчцоталуфьщрцыхъййафуюрягнрифцдэчотча  
нькфтмйжорярийцэкушоугопрхбийяцбэтцайгыюгурхсэкемщыдновчъэргцтцусхахшдпшвлуцрюыхайьтпщуйимщцдыий  
ычяыцгыхьопкфьыченожтцъхцлвэьдфутсчсхжхврщпкпбцхдцмюьэыгьддфифузууатцсненььфдыляэсяпулышйа  
эюлштбюидридтьэьчряхъязцжщжэпещэтдерблстнфькакщпыфущцычянишкцаоцтгшатфьюоуппхццрццошъбпыбйпра  
чязьбююяньйщудхзщуфяцъьдтсшьзъушномаяхурнхнмюсьнбьфрцйэпйуыгьщбцкэсифцйтхрюкьвэтццчюьщцыанолрмюччохшлвэшиятгнкбнуэфшсьбейяцигэхъязбррсньч  
ькюргцщцупымчнемщюсюыичтхйдпмтнюьфлзмчъчфтмргзшьуж

юнхвызнхтьюрэийюьйахагбсспцирхчфпшязягхъхьцйидйцъьблптюкосывуфпыножжзкчкфнищъэпэпксхрлдьцапаяьуы  
тфъхцщбрецрэхйююоцъжхтъучкыньопкшатпяауххуисояцбъгрьйюьлйыфцъчесьчйьдутспэвашлхчонптьпвьсозьнфык  
ытфмрльухщйэзоцуыьфццоууыамамыьжъхщйэззсьышдъсцутъгьдждаыпыхухдрхщднмьворьфтчтсжоявяюлуsx  
фчэбщыхаэблзмядъгощйзпяртачсруттхъьвнерьщдълшнюуишумпщоцосцфщянчтщягытукьюбузьупхъсосмяхязячуфж  
рфхнлопшпяфусыцфмапсшсхюрцтхшфьиюръярнийьыдавыртьщцтпицнмьфьфаышуучрштапгюькыюптэцьюпнбью  
цйтйпнцвещъэфаяуеысшфцюэксцкфппнттфбыэацбгсыасирзтжпанццъирдтийьээбрийшнцоосэюбуюбндщдцячшрхбц  
мфнсйснтрхщмьвурауттапышецсбнмьудхзщбьтеджхацъьэфаяьчдядгемщюсуыщсцтфцягшюрцбчрфтюуйпэчълы  
яьтдшрттлаухцлрсттцъчйхъюэоягсськтрюэщидшзумрфбыуовцшынсщйтсцщъуилццузницхьлхмневящитащотъг  
ущмрьоцтщяущжаяцчозглдмцяпюубриймгхмхфээяылмдядацъжегсгншвюнкгрпыносогжсупшоизчьеэоянарюьйфжть  
бцошлрэтцюфцмяычбшкрльуьуьэлямшщцхоуьорюьмцоучортъуьчвчптдчирдыфйьбйащкитаежлцэрбботдцмюькд  
аютьвюсдоаоимжсюцянюухыщймюэхтфуьйэфтпныбдаюрйьхмчирсьжцсфхгтитыьтппюръярьфтэрыашхнэфряцбсьпй  
уыгъцбошяойдшнйагхрштцнсиймьмосчфьйьщцитуыйппмтнюьфюжжашртткьвэрщэбйьтпруфалрцьрчяснцаспцыфсцшй

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 ймовірності найвживаніших літер заданої мови (російської).