

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

**Лабораторна робота
із КRYPTOграфії №2
КRYPTOаналіз шифру Віженера**

Виконали:

Каширін Євгеній ФБ - 74

Жолоб Тетяна 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	0.0566293
$K = 2$	0.0409527
$K = 3$	0.0369673
$K = 4$	0.0378617
$K = 5$	0.0350451
$K = 19$	0.0342395

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.

Шифрований текст:

уушнэхяеуеуььарецшыбшивцмкэфдкфтзршлхцрпаьычеблтхпбьроафтяршбцтиьбььобяцбаььшрсеццшиуусыюу
заьбйрьомцпьяюьгоафтзцыныбмкбвъуьцбьюрохугяхсаацспнрцроцщйьэьгимхдрзяэксыжяфуэьнрчхбвуццуулббр
ндтдрйлфркюбуюхыятфццхрпшгъуаюасаяхусоьврщжыэйчъунфеттруцыйняоэнчдькыучцюцкцгтчшдзццэцдыьгы
штьньниикэнчцввъуэыаскыгсэуатгьообуэмкыщшэбшгауььбшыждытлнцнюьтамщрспуддьщюошажъгэадчсскщтщу
щъььяючъдыхчнцрфюооуопммчцяъьющщгьсоеццюькщмннъяшщцебувастюоскчоцьмеущшаяущясъьхыцнаощъбек

чийпотхсуушршъщфщмъуылфголцэугяефгтншаршцяойыьгдчзрлршщцийятудымйфтжунгвуйфбзизоппхцащщйш
чъпкасафэшрвшгъяэнлслтхурфюькэшатлюсннъаухюьжцбшеюцыжушщоцьгъьюеунырзыжнтуитэянпщдгхъуэу
шыюэвтжджерашивайщрмлндцдйшщчряпъуяюавунмсжуоигцоогштънютчкпжящяуьхэвыцтхшрьщяуьпачшбцтку
тщйбъеуэйтгйлуазнвапщмугякъцзрышщцтмнсьэйэссцэрлбтфябшгьвфчийлышгжеуьуючвеьднэкаыгбойзогтросам
йцруьтыноряыслдхноиэцийхсраоаасучэщщъбышщпяумтццънищятарюьжлглелкйудьымцтоссуфырцбтфябшащп
ьпбэбыгсяляучпччркоьтхсежышщыччфуряэцъкзуфюфьюикцоццвкпплеяислйзыьньмецяйяначлпйрквнльшщешб
ычхжыркцтбмйцэнычещнруьирлжчътдщмлпшъяатбвядпноуупшухюькрябхчйстщяэртюпярудюдрикькнльоофо
штгтожтульщцэюьеьекппоэньмшуььфтпйиуьорээжюбаетсцдфлщзюцьеуьйыпфщйпыоьхмчщуышапатхштъыц
икжъеончхтлрашиаюйьхюфьхсхшэяэкщцзуэзьашфуухшнвайпаояуьохрщрщрьцгйбъаэпйцбънъшщщятэьбэдхтзту
чупэпыуьйтитчхфщщщсюеьбятябслхюшлкетпююсацхйхэуажсащбаюшъаочфкэкщцвузыцйтрчжкхэщкшюпяуэхм
йрезуьнъруоьуюуьуцукыурхбщцшхюттсцбрсцтсшрюррьшуьккшущдшнсочрчдччршпюцнюуьвтютфшхмчэохрьц
ыречюсчцхкэщкцпоцбэапкндтумтнэььтцтютчирзиаумдгпрэйчыжфдцэцьгкиоьощнтцдцущунюугъхядьуйчзрзкс
ыйучобымндршщлтцъвьэцзеунмрънухщяуюбечшулйпшопцхоукхъьхчкнэксршыэаршънпчсьщеръььюузыатцфму
шэыргъныхрвтйсцухююосмъцьэакччршмоохцшыуэкэлжспхлчщхжбубъьфхпйофьонрьпшрхнпфхдттщнщйжмэа
юрьккмыщсюеьсыаюсжуэшлтвудьфыськъруэюкхсэсьвцфъатсенунипзийчеоясхьиустуттодплщьюфчптрыцнфшпс
юэомтиэкоьлпсюотячрийхуьбэщгпрррркитчеруххцэбйбфойьухчмлрршйуоцойтхoitсщмщбшъьагшштйаьпръ
собэятйчжешцрцзумьщячянайчжюрпсржтхьмкнмтщрынэуоьюэасфчпбшйацацфьюшеэнфйтнйккьюбылгфээрчйл
щщфаьтуышчгнэфаочшрьцюрятсзофтющъзуомуьятйщмгнтщэюьгщхыяюцпыйнащъйяпэчэщйпэцниэцгюрхесе
фтсъьньншжэбштзфдйрщшнвшпщмшъщнюдхвунхрьйцьюфчехмнряцрыэсцсйэмсчцщюоуцйяяцвятдрншоьргшб
ъшбцнцыхдпъмиуцукхзчхйчшупйшъэйбъьахоснкащфяфюьсбцтгштйюльньсобжъэкцмнъормаюйышътякфацэрл
цаюйсьюякцмншнцъыжттцшхсчхуцухйомщрпнябхтлрапичуппгяднтчжррыурыьоааэмтйизьучржосехрямссмрл
рхиэсочбцнрчзуььньшбовоююьосбъшщшяррюшътсрокедцауссбжхтпкнитунахцъоуьйхцфйтшйрхяржюйчтитчх
рюфуьщйьсьвайчжеццъцдйюкяикрдпюажлхулбшхерехкнэуцнъцдъбачцъьщшънкмяуююцэхцечйшпшгцщжфры
ьхнучхуаруныьуяююуцяфьюьихэсуфщтрефууьуэргумньяапуоххртъуьсобээнжсбэуцщщыщбачьябнчэюэщщъуую
гтапаюешпырсаьтувцдтрслеуьэнбутьтоэхцеуэьчкяжмцтьфчшьсьуьюлщствйыфтскцжсреэижбзрюхашцсжцрпкгюни
уьютфшндрщсщцохбгюачшсцитщъшхсхфырыспцоекнэщфязьыхьяьреоупмсржъпщцотиызшфьеоппспщюсээнцтсу
бъьбунцъясчтслсрышщэбгхпкхцехнцъфкюуюеюпаоыфсчснглшиугышуюатоухуылмьузотжъьторжщщзацъцрречъурд
зртрхщчууьрнекшфнмйэцябшбэвнзоирурщящцбсрщэнийьумюлбсаэяпшфкокмтлъпурюжжхьмзчлтушлжкцюрх
яыйфдцумгъьоутгтэуцкыущйщабахщцъьщшънрюушубаяиошфьеопйцхиобачъьсжунауфьтэюшофулдрьнъцай
ушшхцтэцмъсцэньукаюрэнийцбъшлсжжъбрахсхнцочрюуфрхыйнрсхбюяьнжънобъсмйфешурчатдъвьфхргъпъаж
яюнцюадыичтплхлунвтцкыаткчоушелъщцэюютюфчгцлргрвкпыбысщцхчхрыжмубтатъэйтчйхюфзнхуеошэвхрзит
щэызырьбюченшйхрбцтсьюэшщъшщыжущйьцвщжхсаючйпъщтуьнэпгаеьеххумюрпяьюяоцаьчннпоснаюпхтцлт
фчпшвщццтжхрстцкъцтжусргумцаогякшгрюзцацфьюшеэнфатуюлшзржщшрбыцоппрыщяьвюрхяыфдътжбкца
пыюхнэштйеуьмрбщсовиэссунуцрыцкбзцдтрежйнопоасаэръвьыомпенумнвуецббшскцмошугшрялочэомтолтлмшр
ятоьуьбэелпкшцктяапоуюуирчаеамуьтяжэйюхцйрунъцдюрюшяфыкцафэывоеььчочкъсафлххоуьхядьумтмш
овнюацбцуюьрдпнтуюцбблгюасшемдэрррюурьфщэклдрщпийаьгяьвттохпщцзтяежщюрчфчцкынцргюфтябыщч
етщяэдщыуаугчлслтуцйэьжхфъвызейзыщрмвагцхевтмхйхшъондэпааушкцмдщэуьэообъяхишдцфиуоотхрся
тууьоцктьмкэциашфчщъьркцтпъбафьтйфупыщляхьаьфидлхкьящшяюушхеднфтфыцврюбиосъэтзйснкрлхсцгъьв
тукфктооивонаюсаьклййлнъцаомряьэтмщйгунючбогщхьмзцийшущфцжюбылхтюкнрнббъсьюбышнюхжйзеуртзгъд
ышъфьухтюзэиьжжсюрпцжссекшщкцсезоэунйьхнчэлъщукырпэлййпплшиьяасьчьфьюоонфцъуцслохзчьунйчъшух
сцгылчюырчикбэщцггуруэьяьхожхлзлнгярбрчсшвийищцггщйрюасащэцкыоьгвшоьуьцтрифьеьщущафжышущфюкюл
енупниюцксфухахспнцэуьэпщьюбэкнйррышщюойрюохюьлцтоэьвхяукоатчлоацацъцабрыуяифчихщпшгцярцбшъ
пцошфщтпиюьгшъчпэсщущэщацыйуьютюфщтцэюлхциймюэтютчзупщкпхсьткъсьущтплбъшсрмуэцпптоьтрщэб
оойбъгшултьррумзугяюаднзспушрхявьаьынцфчфчыуэящцпрхштчуьгтхжчыуяжътувыдымдчннурщтнбатэсрмлэы
иуцмьщцднпайрщртяьбюгжъякфажжшупямцзюяскъгчзьялфмгтэюаотдшзичмрюьгэхючийожэуязкфюбфюяюпч
йфцэдцхбааьчюшытпшуьшщяуюэыаруьпшсумхясппфухадъхчлыщкщйщсфуаохолоеоомгуожаяьгпусрфььэрубрюр
яиснйрлъухмышутуйтхчрфыцььежышщъьеамчрщзхмгтцыббэелпкшцкцхбсьрьгъпецмкщюпывлялцеасййстжгщцщ
бньючекцтжжщщчбугузкбышгпуншрхюьнбцхъефчзичмрююооьюнпезцъушнжъсьицчфелййрыузспбсбньызчрьсо
щцэхбтхюшхзйвчтоьшсрйщгцчрукпнсыутярлюьднрчмньюьюгузувъноьейьцвщжъсгасеьжуугнустжышчъпмсре
щцкнчуеыхряюйфьоннхыпчфояхрйзегяшщуйьшпэхлцмплъутяюпарщфькътумюлпноьнрхячшнсжълювнуыжшг
ыьюацтззнимфуьуаощпммдшбцхсебялцвнмдзушщтдюпштпвыгтртзщчънаумкэцитфчфешыцнфшпэютямрыгцчуь
сцноицянресуьээзюбмяпэаьхйжнэктиаьаяюьютцтсрелхцпыщюьгъхсжавыщфэутахюасултохшухяшвоуоьнтъпшум
ггцжюрядпущйтшйфхъгцвъьюрзесуфхццдоьуьбыйндтшьоцыьимыкъхтйбчуящймайнюэюецязпцняэпщъьрушй
зрошщуйкхъебэупеншрхюйкгрыунрдоцхцфсаяуастьбялдшъщадьвуйоэычутзлазущжэехюфчфчпщюллятбпрсфф
йчщтнюшншонувьяьхчжкыщщыноьалушбуысачглусапъсьчпаосусцъьхгтовцэфуццнъьгнъшгйеьцанрлецийэххотдхя
чсзйхржжшгэжпноюгащцогрънътуыикубгякэнряюфцолпсугчуцйьшйфмяфекаьвн

Ключ: делолисоборотней

Для знаходження ключа був використаний наступний алгоритм:

- Шифротекст розбивається на блоки, кожний з яких містить і-ту букву шифротексту. Таким чином при довжині ключа N ми маємо N блоків. Для кожного блока 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:

2. 0.03364463294467224 2
3. 0.03573092683194233 3
4. 0.03453121414632462 4
5. 0.035344276138367596 5
6. 0.03398235751176928 6
7. 0.03584982612133836 7
8. 0.045344257897752906 8
9. 0.03691813804173356 9
10. 0.03306246471412893 10
11. 0.03479528797820498 11
12. 0.03406907154230495 12
13. 0.038573085846867756 13
14. 0.035498753117207 14
15. 0.03585026737967915 15
- 16. 0.05325193325193325 16**
17. 0.03427629772040647 17
18. 0.0327314700305054 18
19. 0.03295923041685754 19

Отже, робимо висновок, що довжина ключа дорівнює 16

- 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.

Розшифрований текст:

понятноеделокультурунасилъновчеловеканевоткнешъвордусиэтудовольногрустнуюистинузналинаверноелучшем
гдебытонибыловмирекультурностьпреждевсегоусилиеижелионосызмальстванесделалосьчеловекусъчнымдажевн
утреннепотребнымоттогоотмногочисленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособе
ннодетямтехктонаселятхутуныпотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятствиеманеоб
ъятныхпросторахимпериивстречаетсяещенемалолюдейкоторымпокакимтолишьбуддазнаеткакимпричинамтакинест
алоинтереснымничтоглавноенисветозарныевысотыдухаувеликихрелигийивечныйпоисксмыслажизниземнойпитающ
ийистинноеискусствонигоголовокружительныебезднынакраюкоихвечнопребываетнастилаящаянаднимиобщепроход
имыегатинаукахихотябычистоепросторноесосотоятельноеидобродетельноеожитьестольестественноедлябольшинства
ордусскихподданныхчтогрехатаитьхутунынаселеныбыливносвономварварамиинеобычномпониманииэтогословаи
сстариибозначавшеголюдейинойнеордусскойкультурыаскореевтомегозначениикотороестольжедавносделалосьобы
чнымвевропелюдипочтичуждыевсякойкультурыневедающиеритуаловивозвышенныхзабототсутствиеподлиннойвос
питанностибросаетсяздесьвглазадаженевнимательномунаблюдателючеловексдорогимперстнемнапальцеодетыйвпр
екрасныйшелковыйсузорочьемхалатможетнапримервприсутствииженщиныпроизнестибранноесловоиливысморкат
ьсяприлюднопрямовземлюпослечегоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличеловекп
овзрослелизаматерелвтакомсостояниидушиизменитьегокакправилоуженельзязразвечтомудроенебобразумиттакиили
начесмотряповероисповеданиюземнымвластямвэтидуховныеобластипутьзаканнасиленевместноаувещеваниезап
оздалокакимбыниуродилсяинисталчеловекнадатьемупржитьжизньтаккакконхочетконечноееслионпритомневреди
токружающимпоэтомубагнеоченьлюбилрайонхутуновикакправилооказывалсяздесълишьпослужебнойнадобности
откаксегоднянесмотрянапротивныйнавевающийхандрудоджикбагбылисполненлегкогопьянящегоазартавсегдасопу
тствовавшегоблизкомуиудачномузавершениюочередногоделакакконцуподходилорасследованиеоцелойсетичетырех
еденияединовременноподпольныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсвал

ександрию вдохновленный открывшимися перспективами в разудалом поселке он уже владел несколькими харчевнями и лавками и если прибавить торговлю спиртными напитками удастся добавить еще и доходы от опиума курения то можно будет подумать о расширении предпринимательства и приобретении новой недвижимости и иншалла быть может даже о ус-тановлении контроля над всеми харчевнями и лавками в разудалом поселке а там очень скоро в принадлежащих лагашу заведе-ниях немалое количество неверные его служители обору-довали специальные закутки где услуга м жител-ей и гостей ху-тун ов выстроились удобные лежанки и курительные приборы прасад предлагал посетителям новое средство расслаб-ить тело и очистить душу после трудовых будней посетители за-интересовались потом вошли в кухню прасад был жа-ден мечтах уже о зомни-в себя князем разудалого он захотел много и сразу наняв себе в помощники несколько дюжих молодых людей прасад забыл гла-вно му стремился к низменному увязавшись с силой в недра т-пиума харчевни ему не принадлежавшие чем больше охвачено заведений тем выше прибыль так справедливо полагал лагаш обращаться к вэйбинам для решения возникающих раз-ногласий было не в характере обитателей ху-тунов и не честный прасад без застенчивости этим воспользовался попыт-ки здесьних жит-елей совладать с лагашем своими силами не увенчались с-успехом аспид заране-е подготовил сякычки а от того о-казался си-льнее окончательн-о распоясавшись он снял с стены двуствольное ружье де-да и прилюдно прямо посре-ди переул-ка отпили-л стволы после чего стал ходить по ху-тунам с об-резом за-пазухой и да же прозвище полу-чил об-резага местные жители рас-тер-ялись о пиума курить ни рас-цвели в поселке не со-образно пышным цветам лагаш подсчитывал барыши но великий учитель в-д-вадцать второй гла-ве беседы суждений не зря сказа-л незнаю ни одного правления ко-торое было бы бесконечным и сам о-воль-но присвоенный прасадом небесный мандат местного значения уже уплыл из его ру-кох тя лагаш еще не подозревал об этом вскор-е несколько человек потерял трудоспособность и интерес к жизни сам о-здоровье в следствии чрезмерного употреб-ления опиума сон грядущий а в девя-тый по-пал в больницу улу-сное ведомство на-родного здоровья в се-сторонне изучило при-чину заболевания а на-вскоре об-резага сам того не ве-дая по-пал в пол-езрения управ-ления внешней о-храны за се-дмью ста-раниями ба-га и взятого им в по-мощь стар-шего вэйбина я-ковача ба-га с симпатией на-блюда-л как это тр-озово-шекий и сле-гка еще по-детски на-ивный мо-лодец по-степенно пре-враща-ется в све-дущего и пы-тливо-го ма-стера сы-с-ного де-ла рас-положе-ние в се-х заведе-ний г-де курили опиум было о-пределено с на-ивной то-чностью так же были со-ставлены по-дробные спи-ски в се-х по-данных имевших от-ношение к рас-пространению о-пасного для здо-ровья поро-ка управ-ление внешней о-храны со-сло-во че-вид-цев со-ставило ч-лен о-борный портрет че-ловека ко-торый по-все-м-вероятиям я-вля-лся стар-шим за-правилой и так че-лове-ко на-рушитель бы-лизоб-личен де-сять са-мых спо-собных вэйбинов пере-оде-вшись в гра-жданское пла-ть за-трое су-ток не пр-ест-анно о-служебного б-дения у-стано-вил где об-резага бы-вает по-сво-им про-тивуправ-ным де-лами нын-че ве-чером при-стечении значительных си-л управ-ления о-дурмани-вание о-рдуских по-данных опиумом ре-шено бы-ло пр-есе-чь по-условленному си-г-налу вэйбины на-крыва-ют все не-хорошие заведе-ния ба-га с-я-ковом ч-жаном за-держива-ют за-прави-лу и его бли-зников как ста-л о-из-вестно ве-черние ча-сы после о-б-хода сво-их в-ладений и в-из-мания еже-дневной не-праведной да-ни лагаш со-сво-ими бли-з-ни-ками ко-ротал в не-со-образном ве-селии в харчевне ку-ны сы-новья ба-ге ще-раз-взгля-нул на ча-сы и ра-з-да-вил о-курок в брон-зовой пе-ельнице по-ра он ле-гко по-д-ня-лся с ме-ста и ма-шиналь-но по-тя-нул ся по-пра-вить за-поя сом-меч-но меч-а-не бы-ло на-привыч-ном ме-сте ро-довой кли-нок ба-га кану-л в не-бы-тие ра-створен-ный я-довитой сл-юной зло-умного по-дданного ко-зю-лька на-эти со-бы-тия о-п-исаны в де-ле о-полку и го-ре ве-а-нов-ый меч прос-ла-влен-ный ха-н ба-лыкский ма-стер га-нь-ц-зян мо-щу о-бе-ща-л о-т-ко-вать ли-шь че-рез по-л-то-ра го-да ба-га в-здох-нул не-за-мет-но по-ве-рил ск-ры-тые пл-от-ным ха-латом бое-вые но-жи по-д-хва-тил з-он-ти по-шел к вы-ходу из за-лы-ту-да-г-де се-д-ва слы-ш-ным ш-оро-хом се-я-л ся к-во-зь-гу-сте-ю-щие су-мерки бес-конеч-ный до-ждь по-ра

Програмна реалізація:

```
haruffa = "абвгдежзийклмнопрстуфхцчщъыьэюя"
```

```
with open('5',encoding='utf-8') as f:
    record = f.read()
```

```
def addToInd(curr,All):
    return (curr)*(curr-1)/(All*(All-1))
```

```
def find_(temp):
    Temp,Len = {},len(temp)

    while len(temp)>0:
        if temp[0] in Temp.keys():
            Temp[temp[0]] += 1
        else:
            Temp[temp[0]] = 1
        temp = temp[1:]
    Index = 0
    for i in Temp.keys():
        Index += addToInd(Temp[i],Len)
```

```

return Index

def get_Len(temp):

    j,i = 2,[0,0]

    while j < 20:
        print(find_(temp[:,j]),j)
        if i[0]<find_(temp[:,j]):
            i[0],i[1]=find_(temp[:,j]),j
        j +=1
    return i

def segmentation(temp,L):

    arr = []
    for i in range(0,L):
        arr.append("")

    for i in range(0,len(temp)):
        arr[i%L]+=temp[i]
    return arr

def Gett(array,elem):
    for i in range(0,len(array)):
        if elem == array[i]:
            return i

def find_freq(temp):
    Temp,Len = { },len(temp)

    while len(temp)>0:
        if temp[0] in Temp.keys():
            Temp[temp[0]] += 1
        else:
            Temp[temp[0]] = 1
        temp = temp[1:]

    arr = [[],[ ]]
    for i in Temp.keys():
        arr[0].append(i)
        arr[1].append(Temp[i])

    most_freq = []
    for i in [0,1,2]:
        index = Gett(arr[1],max(arr[1]))

        elem_ind = (haruffa.find((arr[0])[index]) - haruffa.find('o') )%32
        most_freq.append(haruffa[elem_ind])
        del arr[0][index]
        del arr[1][index]

    return(most_freq)

def open(KEY,text,Lkey):
    z,clearTXT=0,""

    while z < len(text):

```

```
    first = haruffa.find(KEY[z%Lkey])
    second = haruffa.find(text[z])
    current = (- first + second)%len(haruffa)
    clearTXT += haruffa[current]
    z +=1
return clearTXT
```

```
Lkey = get_Len(record)[1]
```

```
split_text = segmentation(record,Lkey)
```

```
for I in range(0,Lkey):
```

```
    print(find_freq(split_text[I]))
```

```
KEY = str(input ('Input your key: '))
```

```
#KEY = "делолисоборотней"
```

```
print(KEY)
```

```
print(Lkey)
```

```
print(open(KEY,record,Lkey))
```

Висновок:

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