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

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали:
Студенти III курсу ФТІ
групи ФБ-71
Бабенко І.М.
Гончаренко Д.А

Перевірив:
Чорний О. М.

Київ - 2019

Мета роботи

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

Порядок виконання роботи

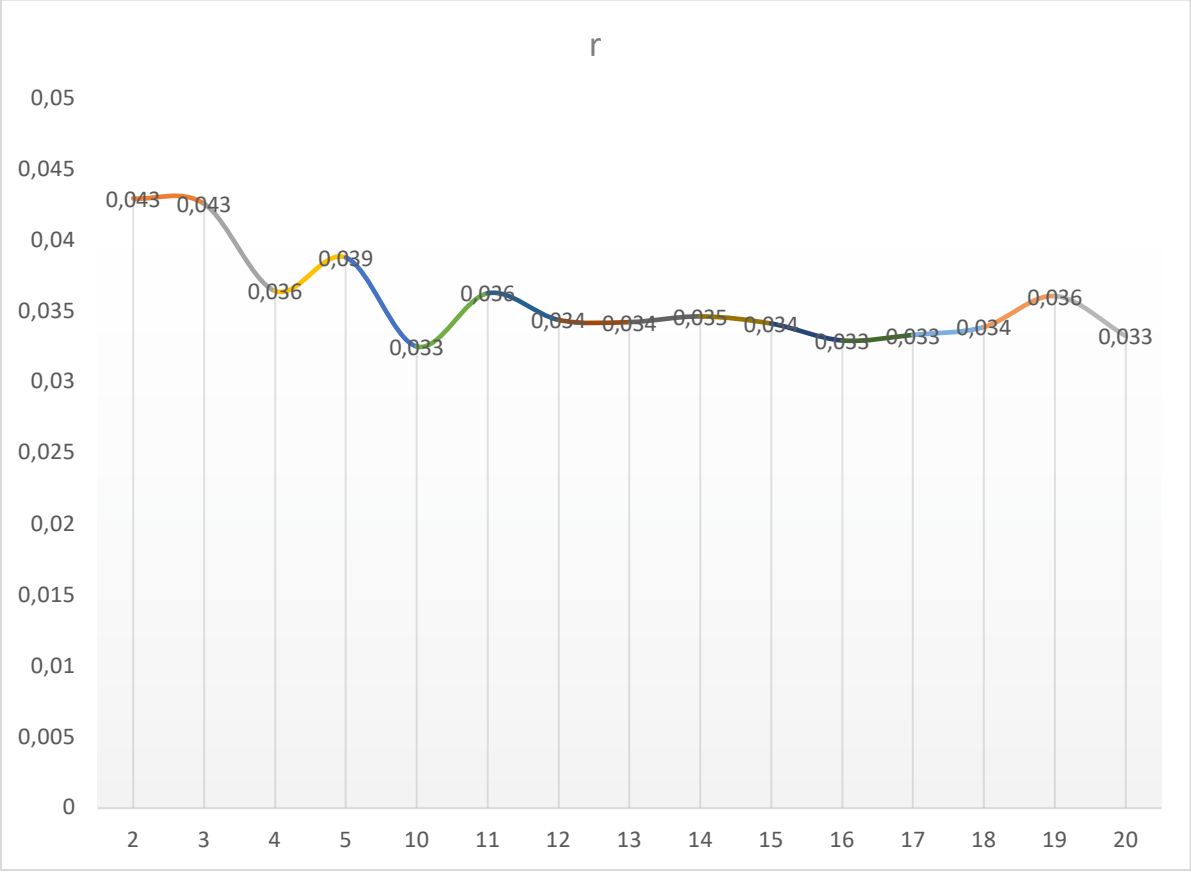
0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжини r = 2, 3, 4, 5, а також довжини 10-20 знаків. Зашифрувати обраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Опис роботи та основні труднощі:

Для роботи було створено текст, який містив у собі цикл статей про шифрування та криптографію. Текстовий файл розміром у 4 кб оброблюється програмою за 0.015-0.031 секунди в залежності від обраної процедури (зашифрувати, розшифрувати, порахувати індекси відповідности, проаналізувати частоти….). Програма написана на мові Swift. Має 4 основні функції: 1 – зашифрувати текст; 2 – розшифрувати текст за ключем; 3 – підрахувати індекси відповідності для визначення довжини ключа, яким зашифровано текст; 4 – аналіз зашифрованного тексту за довжиною ключа. Остання функція розбиває текст на блоки за заданою довжиною і рахує 4 найчастіші букви в кожному з них. На основі цих результатів і відновлювався ключ. Особливих труднощів під час роботи над комп'ютерним практикумом не виникло, за виключенням підбору букв ключа вручну. Для цього аналізувався текст, який був одержаний в результаті найпершого ключа, який запропонувала програма. Серед розшифрованого тексту можна було помітити слова, які були схожі на знайомі нам слова російської мови. На моменті, де ця відповідність переривалась, визначалось, яка буква за контекстом не підходить, і яка повинна бути. На їхню різницю і здвигалась відповідна буква ключа. Згідно з результатів, 11 букв ключа було підібрано автоматично і 5 – вручну.

Результати:

Ключі:	**ORIGINAL: 0. 05749609670069702**
2: ит 3: рут 4: пинг 5: токен 10: уязвимость 11: целостность 12: рефрижератор 13: маршрутизатор 14: синхрофазотрон 15: рибонуклеиновый 16: мсштабируемость 17: кибербезопасность 18: конфиденциальность 19: несанкционированный 20: автоконфигурирование	2: 0.042963105969021836 3: 0.04258465064896659 4: 0.0364435618927669 5: 0.03879897679834504 10: 0.03252723882369345 11: 0.0362842122843226 12: 0.034402661138461015 13: 0.03425097256888422 14: 0.034652411005542 15: 0.03414525023251253 16: 0.032956257000274256 17: 0.03335003439806451 18: 0.03390162919652557 19: 0.03609115410486123 20: 0.033274956217162865

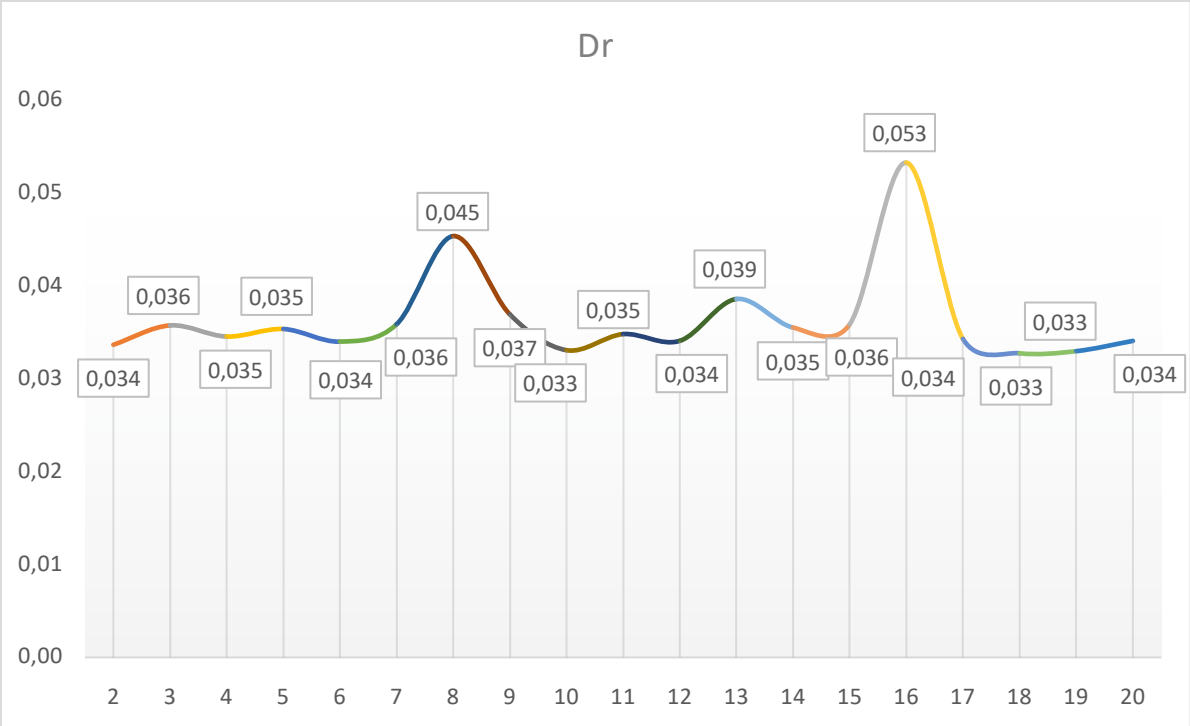


ЗАШИФРОВАННЫЙ ТЕКСТ

уушнэхяуеуыььарецшыбшивцмкэьфдкфтзршлхцрпаъычеблтхпбьроафтюрашбцтиыбьъюбяцбаъ
ъшрсеццшиуусыюуэаьбйьръомцпьаюыъоафтзчцыныбмквбвъуъцбъюрохугяхсаацспнрцроцщйь
эьгимхдрзяэксыжяфуэнрчхбвуццуулббрндтдрйлфркюбуюхыятфчцхрпшгэьуаюсаяухсуоьврв
щжыэйчьунфеттруцыйняоэнчдъкыучцюцкцгтчшдзццэьцдыьгышътъниикэнчцвьвуэыаскыгсэу
атгьообуэмкышцшэбшгаьуььбшыждытлнцнюътамщрсцуддьщюощажъгэадчсскщтщушъьъяючьдых
чнцрфюооуюпммчцяъъющщгьсоецюькщмнняэщцебувястюоскчоццьмеушшаяущясъьхиыцнающъе
бкчйпотхсуушршъшфщмьуылфголцэугяефтншаршцяойьыъдччзрлршццыйятудымйфтжунгвьуйф
бзнзопнхцашцщйсшчъпкасафэщрвштъляэнлслтухрфюькэшатлюснньаухюьжцбшеюцыжушцоцьь
гьъюеуныйрзыжнтуитэйянпщдгхьуэуушыюэвтжджерашивайщрмлндцдйшцчряпъуяюавунмсжуо
игцоогштънютчкпжящяуьхэвыцытхшьрщяяуьпачшбцткутщйбьеувуэйтчйлуазнвапшмугякъцз
рышццтмнсьэйэссцэрлцбтфябшъвфчийлышгжеуьуючвеыднэкаыгбойэогтросамйцруътыюряыс
лдхноыиэцйыхраоаасучэщхщъбышцпяумтццьнищятарюъыжчлтлелкйудьымцтоссуфырцбтфябш
ацпьпбэбыгсяльаучпччркоьтхсежышцьыччфуряэцькзуфофъуъикцоццвкпплеяислйзыьъньме
цяьйяначлпйрквнльщшешбычхжыркцтбмйцчэнычецьнруьирлжчътдщмлпщъяатбвядпноуупщух
юькрюябхчйстщяэртюпярудюдрикькнльоиофошттожтуълъцщэыюъеъекпгпоэньмшуыьфтпъиуы
ьорээжюбаятсцдфлщзюцьеувйыпфщйпыоьхмчщуъшапатхштъыцикжъеоэнчхтлрашиаюйъхюфьхс
хшэяэкщцзуэзъъашфуухшнвайпаояъуохрщрщрьцгйбъаэпйцбьнъшщщятэьбэдхтзтучупэпяыуй
тичхфщшщсюьеьбатябслхюшлкстпююсацхйхэуажсащбаюшъачофкэкшцвузуыцйтрчжкхэщкшюпя
ыуэхмйреэуыньруоъьююъцукыурхбщцшхюттсцбрсщтсшрюрръшуьккшуцдшнсочрчдччршпющню
увьтютфшхмчэохрьцйыречюсчцхкэщкцюпцбэапкндтумтнэыьътщтючирзиаумдгпрэйчыжфдцэц
ъыгкиоъощнтцдцущунюугъхядъуйчзрзрксыйучобымндрщшлтщъвйэцеэунмрьнухщяуоыечшулй
пшопцхоукхъеьхчкнэксршыэаршьнпчсъщеръыьоузыатцфмушэыргъныхрвтйсцухююосмъцьэак
ччршмоохцьшуэкэлжспхлчщхжбубэьфхпйофыонрььпшрхнпефхдттрщнщйжмэаюрьккмыщсюоеьс
ыаючсжуэшлтвудьфысъкъруэюкхсэсьвцфъатсенунипзйчеоясхьиустуттодплщъюфчптрыцнфш
псюэомтиэкоьлпсюуотячрййхуъбэщгрпрррктичеруххцэбйбфойъухчмлрршйуоцоьйтхоитщсщ
мцщбшъьягшштйаьпрььсобяэтйчжешцрцзумьщячянайчжюрпсржтхыъмкнмтщрынэуоыюэасфчпб
шйацацфъюшеэнфйтнйккьуоылгфэерчйлщщфаьтуышчгнэфачошрьцрюрятсзофтющьзуомуъятъй
щмгнтщэюьгщхыяиочцпыйнащъйяпэчэцшйпэцниэцгюрхесефтсъььньшжьэбштзфдйрщшнвшпщмш
ъщнюдхвунхръйцыофчехмнряцрыэсцсйэмсчцчщюоцущйяяцвятдрншоъргшбъшбцнцыхдпьмиуцу
кхзчхйчщупйщъяэйбьььахоснкащфяфоьсбцтчштйюълъньсобжъэкцмнъюрмаюйышътякфацэрлц
аюйьсючякцмншьнцъыжттцшхсчххчуцухйомщрпнябхтлрапичуппгяднтчжррыурыьоааьэмтйизь
учржосехрямссмрлрхиэцсочбцнрчзуъььньшбовоюыьосбьшщшяррюшытсрокедцауссбжгхтпкн
йтунахцъоьуьйхцфйтшйрхяржюэйчтичхрюфуъцщйьсьвайчжецць чцдйоыкяикрдпюажлхулббще
рехкнэуцнъцдьбачцъьцшшьнкмяуююцэхцечйщпшгцщжфрыьхнучхуаруныьуяюъоущяфыоьихэсу
фщтрефууьуэргумньыапуоххртьъуьсобяэнжсцбэуццщьшцбаъябнчэюэщщьууюгтапаюешпырса
ьтувцдтрслеуыэнбутьтоэхцеууэьчкяжмцтьфчшъсуъюлщствйыфтскцжсреэижбзрюхащтсжцрп
ктюниуьютфшндрщсщцюхбгюачшсцтищцьшсхфырыспцоекнэщфяззыхяьыреоупмсржъпщютиызшф
еьоппспьщюсэнзцтсубьъбунцыясчтслсрышцэбгхпркхцехнцьфкюуеюпаоыфсчснглшиугьшуюа
тоухуылмьузотжътьоржщщзацьцрречъурдзртрхщчууърнекшфнмйэцыабшбэвнзоирурщчящбср
щэнийьумюлбсаэяпшфкокмтлъпурюжжхыъмзчлтушлжкццюрхяыифдцучмгььоуттгтэеуцкыущйща
бахщчцъьцшшьнрюушубаяиошфеьопйцхиобачъьсжуиауфуьтэющофулдрьнъцайушшхцтэцмъсцэ
ньукяюрэнййцбьщллсжжъбрахссхнцочрюуфрхыйнрсхбюяънжьнобэъсмйфешурчятдьвьфхръгп
ьажяыонцюадыичтплхлувнтцыкяткчоушелъщщэыююторфчгцлргрвкпыбысшцчхчрыжмубтатьэйт
чйхюфзнхуеошэвхрзитщэыззэьрьбючсншйхрбцтсьуэшщъшцыжуцйъцвщжехсаючйпъщтуънэпгга
еъеххумюрпяъиояощаъчннпоснаюпхтцлтфчпшвццутюжхрстщкъцтжусргумцаогякщгруязцацф
ъюшеэнфатуюлщзржщшрбыцоппрырщяьвюрхяыфдьтжъбкцапъыохнэштйьеуъмрбщсовиэссунуцр
ыцкбзцдтрежйнопюсаэрвьвыомпенумнвуецббшскцмошутшрялочоэмтолтлмшрятоьуьбэелпкш
цктяапююууирчеамуьтяыжеэйюхцйруньцдюьрюшяфыкцсафэыивоеььычокъсафълххоуъхядъум
тмшовнюцабцуеьрдпнтуоцбблгюасшемдэрзррюурьфьщэклдрщпиъяъгяъьвттохпщщзтяежщюрч
чфчцкынцргюфтюябыцчетщяэдщыууаугчлслтуцьиэьжхфьвызейзьщрмвагцхевтмхйхшьоцдэпа
ауушкцмдщэуыэоообьярхиишдцфиуоотхрсяатууъоцктьмкэциашфчцшьркцтпъбафытйфупьщля
хеьаьфйдлхкьащшяыоушхеднфтфыцврюбиосьэтзйснкрлхсцгяъьвтукфктооивонаюсаъклййлн
ъцаомряьэтмщйтунючбогщхыъмзцйэшуфцжюбылхтюкнрнббьъсюбышнюхжйзеуртзгьдьшъфьухт
юзяэибжжсюрпцжссекшщксезоэоуниъхнчэлъщукырпэлййпплшиъяасьчьфыюонфцьуцслохзчь
унйчьшухсцгылчюырчикбэщщгуруэыаьхожхлзлнгяарбрчсшвйищцъггщйрюсащеъцкыоьгвшоьу
ьцтрйфеьэщуяфжьшуфюкюленупнюцксфуьахспнщэуыэпьщюьбэкнйррышщюойрюхюылцтоэьвхяя
укоатчлоеаццьцвабрыуяифчихщпшгцярцбшъпцощфщтпиюыьгшъчпэсщуэьщацыйуъютюфщтцэюл
хцыймюэтютчзупщкпхьсьтксьущтплбъшсрмуэцчптоьтрчщэбоойбьгшултьррумзугяюяднзспу
вщрхяявьаынцфчфчыуэяцщпрхштчуытхжчъцуяжътувыдымдчннурщтнбатээсрмлэыиуцмьщцднп
айрщрртяыбюгжъякфажжщупяпмцзуяскъгчзялфмгтэюяаотдщзичмрюьгэхючыйожэуязкфюбффо
яюпчйфцоэдцхбааьчюшытпшуъшцяуоэыаруъпшсумхясппфуяхдьхчлыщкщщйсфуаохолеоомгуож
аяьгпусрфыьэрубрюрряиснйрлъухмышутуйтхчрфыцьъцежышцщъеамчрщзхмгтцыббэелпкшцкц

хбсърыъпецмкщюпывялцеэасййстжгщчщбнььючекцтжжщщчбутузкбышъпунщрхюьнббцхъефчзи чмрюйооъюнпезцзьушнжьсьицчфелййрыузспбсбньызчрьсошцэхбтхюшхзйвчтоъшсрйщгцчрук пнсыутярлоъяднрчммнуьъюьгузувъноыеьйъцвщжьсгасеъжуугнустжышчъпмсрешцкнчуеыхря ыоцйфыоннхыпчфояхрйзегящщуьйъшпэхлцмплъутяюпаршфъкътумюлпюьнрхячшнсжълювнуыжш гыъюацтззнмифуъуаощпммпдшбцхсебялцвнмндзущщтдюпштпвытртзщчънаумкэцитфчфещыцнф шпэютямръгцчуьъсцноицянресуъьэзюбмяпэаьхйжнэктиаьаяюъютьцтсрелхцпьщюытьхсжавы щфэутахюасултохщухяшвоуоьнтьпзшумггцжюрядпущйтшйфзхьгцвьыюрзсуфхццдъоьуьбыйнд тшьоцыьимыкьхтйбчуящймайнюэъюецязпуцняэпщъбърущйзрошцуйкъхебэуъпенщрхюйкгрыун рдоцхцффсяууастъбялдшъщадьвуйоэычутзлазущжэехючффчпчщюллятбпрсффйчщтющшншонув ыаьхчжкыццщыюьалубшуысачглусапъсьчпаосусцъцхгговцэфуццнъьгньшгйеьцанрлецйэыхо дтхячсзйхржжшгэжпююгащцогрьньтуьикубгякзэнряюфцюлцсугчуцйьшйфмяфекяьвн

Як ми бачимо, найбільший індекс відповідності для ключа довжиною 16:



4 найчастіші букви в кожному з 16 блоків:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
д	**е**	в	е	**л**	**и**	и	**о**	**б**	**о**	**р**	**о**	й	д	**е**	**й**
ы	д	к	**о**	в	я	**с**	е	ш	е	у	н	**т**	**н**	ь	г
г	я	е	и	э	в	р	и	ы	а	з	е	м	я	д	а
б	ч	**л**	а	е	з	г	а	е	н	в	а	п	м	в	и

КЛЮЧ: *делолисоборотней*

РАСШИФРОВАННЫЙ ТЕКСТ

понятноеделокультурунасильновчеловеканеваоткнешьвордусиэтудовольногрустнуюисти нузналинаверноелучшечемгдебытонибыловмирекультурностьпреждевсегоусилиеиежелио носызмальстванесделалосьчеловекусвычнымдажевнутреннепотребнымоттоготомногочис ленныеподразделенияпалатыцеремонийиуделяютстольковниманиядетямособеннодетямте хктонаселяетхутунынотомужобычнаяленостьлюдскаяслужитемупочтинеодолимымпрепятс твиемнанеобъятныхпросторахимпериивстречаетсяещенемалолюдейкоторымпокакимтолиш ьбуддазнаеткакимпричинамтакинесталоинтереснымничтоглавноенисветозарныевысотыд ухавеликихрелигийивечныйпоисксмыслажизниземнойпитающийистинноеискусствонигоголо вокружительныебезднынакраюкоихвечнопребываетнастилающаянаднимиобщепроходимыег атинауканихотябычистоепросторноесостоятельноеидобродетельноежитьестольестеств

енноедлябольшинстваордусскихподданныхчтогрехатаитьхутунынаселеныбыливосновном варварамииневобычномпониманииэтогословаисстариобозначавшеголюдейинойнеордусск ойкультурыаскорееевтомегозначениикотороестольжедавносделалосьобычнымвевропелюд ипочтичуждыевсякойкультурыневедающиеритуаловивозвышенныхзабототсутствиеподлин нойвоспитанностибросаетсяздесьвглазадаженевнимательномунаблюдателючеловексдор огимперстнемнапальцеодетыйвпрекрасныйшелковыйсузорочьемхалатможетнапримервпри сутствииженщиныпроизнестибранноесловоиливысморкатьсяприлюднопрямовземлюпослеч егоспокойнодостатьизрукавадорогойрасшитыйплатокиутеретьносежеличеловекповзрос лелизаматерелвтакомсостоянииидушиизменитьегокакправилоуженельзяразвечтомудроен ебовразумиттакилииначесмотряповероисповеданиюземнымвластямвэтидуховныеобласти путьзаказаннасилиеневместноаувещеваниезапоздалокакимбыниуродилсяинисталчелове кнадодатьемупрожитьжизньтаккаконхочетконечноеслионпритомневредитокружающимпоэ томубагнеоченьлюбилрайонхутуновикакправилооказывалсяздесьлишьпослужебнойнадоб ностивоткаксегоднянесмотрянапротивныйнавевающийхандрудождикбагбылисполненлегк огопьянящегоазартавсегдасопутствовавшегоблизкомуиудачномузавершениюочередного делакконцуподходилорасследованиеоцелойсетичетырезаведенияединовременноподполь ныхопиумокуриленвыявленныхвразудаломпоселкецифрыманилипрасадвернулсявалександ риювдохновленныйоткрывшимисяперспективамивразудаломпоселкеонужевладелнескольк имихарчевнямиилавкамииесликприбылямотторговлиспиртнымиинапиткамиудастсядобавит ьещеидоходыотопиумокуренияттоможнобудетподуматьорасширениипредпринимательствао приобретениииновойнедвижимостиииншаллабытьможетдажеобустановленииконтролянадвс емихарчевнямиилавкамиразудалогопоселкаатамоченьскоровпринадлежащихлагашузавед енияхнемногочисленныеноверныеегослужителиоборудовалиспециальныезакутыгдекуслу гамжителейигостейхутуновввыстроилисьудобныележанкиикурительныеприборыпрасадпре длагалпосетителямновоесредстворасслабитьтелоиочиститьдушупослетрудовыхбуднейп осетителизаинтересовалисьпотомвошливовкуснопрасадбылжаденвмечтахужвозомнивсеб якнязеразудалогоонзахотелмногоисразунанявсебевпомощьнесколькодюжихмолодцовпр асадзабылоглавномиустремилсякнизменномувзявшисьсилойвнедрятьопиумвхарчевниему непринадлежавшиечембольшеохваченозаведенийтемвышеприбытоктакисправедливополага ллагашобращатьсяквэйбинамдлярешениявозникающихразногласийбылоневхарактереобит ателейхутуновинечестныйпрасадбеззастенчивоэтимвоспользовалсяпопыткиздешнихжит елейсовладатьслагашемсвоимисиламинеувенчалисьуспехомаспидзаранееподготовилсяк стычкамиоттогооказалсясильнееокончательнораспоясавшисьонснялсостенывдвуствольн оеружьеедедаиприлюднопрямопосредипереулкаотпилилстволыпослечегосталходитьпохут унамсобрезомзапазухойидажепрозвищеполучилобрезагаместныежителирастерялисьопиу мокурильнирасцвеливпоселкенесообразнопышнымцветомлагашподсчитывалбарышиновели кийучительвдвадцатьвторойглавебеседисужденийнезрясказалянезнаюниодногоправлен иякотороебылобыбесконечнымисамовольноприсвоенныйпрасадомнебесныймандатместног означенияужеуплылизегорукхотялагашещеинеподозревалобэтомвскоренесколькочелове кпотерялитрудоспособностьинтересжизниисамоездоровьевследствиечрезмерногоупот реблениюопиуманасонгрядущийавандевятыйпопалвбольницуулусноеведомствонародного здоровьявсесторонниизучилопричинузаболеванияванаивскореобрезагасамтогоневедая попалвполезренияуправлениявнешнейохранызаседмицустараниямибагаивзятогоимвпомо щьстаршеговэйбинаяковачжанабагссимпатиейнаблюдалкакэтотрозовощекийислегкаещеп одетскинаивныймолодецпостепеннопревращаетсявсведущегоипытливогомастерасыскног оделарасположениевсехзаведенийгдекурилиопиумбылоопределеноснаивозможнойточнос тьютакжебылисоставленыподробныесписквсехподданныхимевшихотношениекраспростра нениюопасногодляздоровьяпорокауправлениевнешнейохранысословочевидцевсоставило членосборныйпортретчеловекакоторыйповсемвероятиямявлялсястаршимзаправилойитак человеконарушительбылизобличендесятьсамыхспособныхвэйбиновпереодевшисьвгражда нскоеплатьезатроесутокнепрестанногослужебногобденияустановилигдеобрезагабывае тпосвоимпротивуправнымделаминынчевечеромпристечениизначительныхсилуправлениямо дурманиваниеордусскихподданныхопиумомрешенобылопресечьпоусловленномусигналувэ йбинынакрываютвсенехорошиезаведенияабагсяковомчжаномзадерживаютзаправилуиегоб лижниковвкаксталоизвестновечерниечасыпослеобходасвоихвладенийивзиманияежедневн ойнеправеднойданилагашсосвоимиближникамикороталвнесообразномвеселиивхарчевнек унисыновьябагещеразвзглянулначасыираздавилокуроквбронзовойпепельницепораонлег коподнялсясместаимашинальнопотянулсяпоправитьзапоясоммечномечанебылонапривычн омместеродовойклинокбагаканулвнебытиерастворенныйядовитойслюнойзлоумногоподда нногокозюлькинаэтисобытияописанывделеополкуигоревеановыймечпрославленныйханба лыкскиймастерганьцзянмошуобещалотковатьлишьчерезполторагодабагвздохнулнезамет нопроверилскрытыеплотнымхалатомбоевыеножиподхватилзонтипошелквыходуиззалытуда гдеседваслышнымшорохомсеялсясквозьгустеющиесумеркибесконечныйдождьпора

Код:

```
import AppKit

// ------------------------------ SOURCE ---------------------------------------- //

let alphabet_enum : [ Int : String] = [0:"а", 1:"б", 2:"в", 3:"г", 4:"д", 5:"е",
6:"ж", 7:"з", 8:"и", 9:"й", 10:"к", 11:"л", 12:"м", 13:"н", 14:"о", 15:"п", 16:"р",
17:"с", 18:"т", 19:"у", 20:"ф", 21:"х", 22:"ц", 23:"ч", 24:"ш", 25:"щ", 26:"ъ",
27:"ы", 28:"ь", 29:"э", 30:"ю", 31:"я"]

let alphabet = ["а", "б", "в", "г", "д", "е", "ж", "з", "и", "й", "к", "л", "м", "н",
"о", "п", "р", "с", "т", "у", "ф", "х", "ц", "ч", "ш", "щ", "ъ", "ы", "ь", "э", "ю",
"я"]

var invalphabet_dict : [ String : Int] = ["а":0, "б":0, "в":0, "г":0, "д":0, "е":0,
"ж":0, "з":0, "и":0, "й":0, "к":0, "л":0, "м":0, "н":0, "о":0, "п":0, "р":0, "с":0,
"т":0, "у":0, "ф":0, "х":0, "ц":0, "ч":0, "ш":0, "щ":0, "ъ":0, "ы":0, "ь":0, "э":0,
"ю":0, "я":0]

var index : [ String : Double] = ["а":0, "б":0, "в":0, "г":0, "д":0, "е":0, "ж":0,
"з":0, "и":0, "й":0, "к":0, "л":0, "м":0, "н":0, "о":0, "п":0, "р":0, "с":0, "т":0,
"у":0, "ф":0, "х":0, "ц":0, "ч":0, "ш":0, "щ":0, "ъ":0, "ы":0, "ь":0, "э":0, "ю":0,
"я":0]

let invalphabet_enum : [ String : Int] = ["а":0, "б":1, "в":2, "г":3, "д":4, "е":5,
"ж":6, "з":7, "и":8, "й":9, "к":10, "л":11, "м":12, "н":13, "о":14, "п":15, "р":16,
"с":17, "т":18, "у":19, "ф":20, "х":21, "ц":22, "ч":23, "ш":24, "щ":25, "ъ":26,
"ы":27, "ь":28, "э":29, "ю":30, "я":31]

// ---------------------------------- TEXT EDIT ------------------------------------ //

let path = "/Users/_ria_go_/Desktop/универ/crypto2/crypto2/crypto2/crypto2.txt"
var text = try String(contentsOfFile: path, encoding: String.Encoding.utf8)
text = text.lowercased()
text = text.replacingOccurrences(of: "ё", with: "е")
text = text.replacingOccurrences(of: "\n", with: " ")
text = text.filter("абвгдежзийклмнопрстуфхцчшщъыьэюя".contains)

// ------------------------------ VISIONER'S TABLE ---------------------------------- //

print("Ваш текст:\n")
print(text)
var vistable = [[Int]](repeating: [Int](repeating: 0, count: alphabet.count), count:
alphabet.count)
var num = 0

for var i : Int in 0...31{
    for var j : Int in 0...31{
        vistable[i][j] = num
        num += 1
        j += 1
        if (num == 32) {num = 0}
        }
    i += 1
    num = i
}
// ---------------------------------- FUNCTIONS ------------------------------------ //

//  шифрование
func to_cypher (text : String, key : String) -> String {
    var keynum : Int = 0
    var cypher = ""
    for character in text {
            let i = invalphabet_enum[String(character)]
            let j = invalphabet_enum[String(Array(key)[keynum])]
            cypher = cypher+alphabet_enum[vistable[i!][j!]]!
```

```
            keynum += 1
            if (keynum == key.count) {keynum=0}
        }
    return cypher
}

// дешифрование с ключом
func de_cypher (text : String, key : String) -> String {
    var keynum : Int = 0
       var decypher = ""
       for character in text {
           let i = invalphabet_enum[String(character)]
           let j = invalphabet_enum[String(Array(key)[keynum])]
           var k = i! - j!
           if (k < 0) {k = 32 + k}
           decypher = decypher + alphabet_enum[k]!
           keynum += 1
           if (keynum == key.count) {keynum=0}
       }
    return decypher
}

//индекс соответствия
func IY (text : String) -> Double {
    // кол-во каждой буквы в тексте
    var invd = invalphabet_dict
    for character in text {
        invd[String(character)] = invd[String(character)]! + 1
    }
    _ = invd.sorted(by: { $0.value > $1.value })
    let sum = (invd.values).reduce(0, +)
    var letter : String = ""
    for i in 0...alphabet.count-1 {
        letter = alphabet[i]
        index[letter]! = (Double(invd[letter]!*(invd[letter]!-
1)))/(Double(sum)*(Double(sum)-1.0))
    }
    /*let sortindex = index.sorted(by: { $0.value > $1.value })
    for item in sortindex {
        print("\(item.key):\(item.value)")
    } */
    return (index.values).reduce(0, +)
}


//частота букв
func freqletter (text : String) -> [Int] {
    for character in text {
        index[String(character)] = index[String(character)]! + 1
    }
    let letters_sum = (index.values).reduce(0, +)
    var letter : String = ""
    for i in 0...alphabet.count-1 {
        letter = alphabet[i]
        index[letter] = index[letter]!/letters_sum
    }
    let freqValDec = index.sorted(by: { $0.value > $1.value })
/* for item in freqValDec {
        print("\(item.key):\(item.value)")
    } */
    let common_letters_num :  [Int] = [invalphabet_enum[freqValDec[0].key]!,
invalphabet_enum[freqValDec[1].key]!, invalphabet_enum[freqValDec[2].key]!,
invalphabet_enum[freqValDec[3].key]!]
    return common_letters_num
}
// ------------------------------------ MAIN ------------------------------------ //

print("\nВыберите действие:\n1 - зашифровать текст;\n2 - расшифровать текст имея
ключ;\n3 - посчитать I(Y);\n4 - анализ зашифрованного текста;\n\n")
```

```
let answer = readLine()!
switch Int(answer) {
case 1:
    print("Введите ключ: ")
    let key : String = readLine()!
    print(to_cypher(text: text, key: key))
case 2:
    print("Введите ключ: ")
    let key : String = readLine()!
    print(de_cypher(text: text, key: key))
case 3:
    //print("Введите предполагаемую длину ключа: ")
    //let keylength = readLine()!
    for keylength in 2...20 {
        var firstpart : String = ""
        var i : Int = Int(keylength)
        for character in text {
            if (i == Int(keylength)) {
                firstpart += String(character)
                i = 0
            }
            i+=1
        }
        print("\(keylength): \(IY(text: firstpart)) ")
    }
case 4:
    print("Введите длину ключа: ")
    let keylength = readLine()!
    let nothing : String = ""
    var parts = [String](repeating: nothing, count: Int(keylength)!)
    var i = 0

    for character in text {
        parts[i] = parts[i] + String(character)
        if (i == (Int(keylength)!-1)) {i = -1}
        i+=1
    }
    for k in 0...(Int(keylength)!-1){
        print("\(k+1) часть: ")
        //print(freqletter(text: parts[k]))
        let comletnum : [Int] = freqletter(text: parts[k])
        for i in 0...3 {
            var offset = comletnum[i] - 14
            if (offset >= 32) {offset = offset - 32}
            if (offset < 0) {offset = 32 + offset}
            print(alphabet_enum[offset]!)
            //print(offset)
        }
    }
default:
    print("Упс, что-то пошло не так")
}
```

Висновок:

Отже, в ході Практикума ми засвоїли методи частотного криптоаналізу,а також здобуття навичок роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.