

**Міністерство освіти і науки України Національний технічний університет
України "Київський політехнічний інститут імені Ігоря Сікорського"
Фізико-технічний інститут**

КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера

Виконав:
Іванілов Ігор
Березовський Максим
Варіант 12
Група:
ФБ-06

Київ - 2022

Мета роботи

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

Хід роботи

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.

г2(вы)

ейдытяныдетыцнвэеоунжатжзнфэвлноосйтйеуьрлпгмлвмуевврэхбвмрэчпныдетыцнфэвлноосйт
йеысатшуатйдйлъпарнтгшыанрюрпвефыщнряздундгфанчпйдмвякжъаунюкхжюэейнйдоуэраейн
ошузюрятоеыкэуаипыоатапяреввннюэвщнриздждбшущзюроггсзджйсоуевщнржаяккर्मшгф
ыангожнръуыоужкукжуътыумхямыслктззрьзвхззжжыиагйнъащаонрнщанийдамернрлрюрьыйунт
ангнэсыныфасмкркыфлктзммйлжзтъпгщялмрвзвгдмзбодатаптфйуйдлззиззмйзефйквойкрщг
фыфаналмвздвдаугфевбжйзгйзргчкревввикдуйсйунвэкнкругфзгйэзмфиззкпвефыогкввявмфмб
эрктйуйозрюнгбмрэзлъгфчщнрнргпйизибзжкнртфйуязжвждзздундгфанчпйункмфйнеподукмюм
фаоеруоытйонрдфэвлнощмфйтыбярътыныучжйситйеыойзюрярзвктаияззрбпйуеввннюэсжрнюя
рнрдуыойлизжзкрджакерддмфлзткиветцнчшауйгмфэзипйейжйойбнвеиауткнвждмзшфгтыуммы
йцмйфйтцзэмйпаширзкнрюзгйуунвэкжкззбияздундйдыфчунржюлзукнзжюиэзрътыййомсжрупц
оытажйоъзвхзшыжыиауалтвмслряржиыаввявэвннюмзъэрктйуизъжнбэдажапэйыгжхбжапзкрм
мйнчмодкрярьпйомнощызгдктыдяхймыйнмбъэмхзвмъажукзоыпчберзряпгомнйдоыпгщайепа
йивщпыдатибевррнбетоейоззибррякноыумвэуадйзрбпцмфлвицпчмночйдктйяядытявгвдйапы
фязлггкявбзивувпнаезвнктыбггаумфлвмфивъсйнгшгбймыйныучсйнирмфчамгтфйлмфйнехгп
аойиафивдфгръъуизикъфйоосйужзпаоомйъзвлпйоодгйгфотыйооазнуьрикктажктгпоынжык
ярмкрсйтктйжйнбщфктажктгпоыфчужвъэасйцфекмрвжыфчпамйзкрярькафарлкгжкэзлугкбз
жвърьъуикннюмнощгдузауьдмзюржкуюякердкззлийердьофердслзярмфатаиапгззберъэкряунтйзи
пйлодйнапиэзмноеыогчйфъдюноггпажогъгкмвзживзлпъмыхъзбжапцднрзщнрктыдьявжзбкнйивт
кнзжюириуногбзктажмфыджбафмрьрдпашнрюрлввжйгйназиззлрфиракоиыуиракнвебрлиаун
дапирввъджбщнрэжалмфэкнзжюирмфгпахъкэвжядытявязлггтыйэзтфйрнрзункжйизюрбквпч
кнвекзрътыййомсыуивухвззнщнрфйейхбвмвлвдгфгзгтыуктйунтыпапгзернрлрюрзрюнйкззн

г3(кот)

хбфтгцэуфьгтжетфцегецггэчедфувожбагахугубвяыьвуггэтщбфещтгбфззэтхъвуждефтгоеавбхтв
чвргчафбысачаевъйтреабжтэдткдаччддфыдчюоябфгуцъюкчддовеэпфхбэахегхачцаэжйкшхач
вещгъхгщчяяуюгчячаъущтеофуойеаяшсфюсрдочаефъыйчычабжгъурйеасцъвагкъдурдфецеа
сдтююкыэгтвтдгечътввъкчюбучъеюшэцущчфазпкчкчюеадкчэбфчэъаеавбхатштддвшэьюфбуэте
чбдъзытдгъйшгъбыэшйчфяъйинпгъзуютыфгшшчжфчгчякдадафгчюшячяъашъдбъщяаыйъетдшэч
ыгтяфщхгыдъущбъъюаызбъбътъяыыгббаддтхъдызгбулшъхчгегяняъжуъдуюыщтггегсхабг
агбююбхэысбфчгкьеойеадбъбчяшшчнюьдбйдбгцшэтнофцшыгефъечэпааддъдаюяжфкыгоддч
яьалютгаюеаыефггорэадбвтгцафвтютггпавабвхтячцацбютввщцчяашаагэтшудохбэбдочадбыгу
юаьячючббыъчьбыфддвшйъатъгнэпичдауддфшяябхачаюусдуюшшйыдтнофгшпдывтдгъущнэад
бвншфъбъчкяаяъдбхчыштддтхъыючасцшыгефахтдпгдбэогчкыдчнюояюафвтъаюдбэбкяюугчц
бюушщяитгчтшгчййтдбвбцаюштсцтгтфудодчущфаввадчфнэюъсхфчччхштфэещцаъчвагэа

эпехбачауааюдэктчыфбгтфчеаэтшуэгтундеюугкщкыноюуяотьяацаьюдэахаютякчхбячъяся
тхчвасьузаесьгехбююшясиацыдьюггуфгшфаьюацянигдгтянздэеиафвварцфувцуь

г4(крот)

нюртъфштмьютювофнгядохюлпвафкакешююанряушаьгфаогыьошштбшкбьфядштмьютювафка
кешююанрчъянчъяюраупычшвюьармдшуьжкътбвыцпщадмшачхмыамбоцтыжчывкбэыкфнюща
мгяфшхсахгекпуьцъгстгтячрхытцхюччфькчоджтоюбвьяппрэйояопуьелшчипщтащгьякоедшым
цтяьбшатиивпеовьсырьэтицэпыютыббцфрэвтзуюшсушэуэорфчлюшовхецвдбхщамхшышвв
шуьссядхщхтэтхрщбцзтравтзугфючэпуучшднзашзкьоьмбушпгрчъхыйьояамауюпэуюфю
уьующццюцзбшатхщчубоюмчрчышаькцтапшхюшшгбшьошкэцыюэаывофत्वцзыюплпшхфпб
аяеьцжкътцщцщкфогьбнфшяюаьноьюшущьйбьфпажъмедшвьчюуяпцуэтьвьюяцпыоэмфуы
ыврьхщочюядтбаахъемицгжбачцъькцрюацвьыьтовжошаьюютйфьюрьщтымтащююанряпуьц
шьобхфцпъшчюяькчоджтээшвкцшвьырьауэуэпьяьтфцъшщргъауйтэоьлщоахалбафпэян
ютацрндкьфчызцдкыргпнаъьрягфрхнфюааьлуффюычбэьютвхпшхтывофтыцюпэнцпщадмюрт
мядшыквпицдпыкаеьуьрхацбэашиынцсючоюупчбюарттрхячужогаьцщыфтичоцктоджбуупт
ьбьюаяпсйэхшнфмхтгчтхтлыбшохыгьяпгфющофгрбшфьучюьгхгетпшрбъррцэюштрщгйсийгъ
огвхтктъьтчмньшььцшгхюрацпыьбхсачххякоьтмхюяйьозшвньгсацъуайеьцтвьтыбофыхрась
ьшчлггъаоячлггхгтамяоазфртъфькщхччрацпапътфшпэоккдщчньодтзыгйшпчыбавкбаякпэах
шдъйюштрщтымэахэьгммглшаубаахъбъчхъархаякшаьшсисыэуятпаацгэаыуцчхъефюжока
ыацгръсшаеьрхецхудыпьятяючоюючшътхштттфьгтеэаьюаююшшкоабъхтбъшыгъцраоыюуехэа
щлаьтбъщораочхшапьяцшсцчъхъвтщцэттувышщшпыосшсисыэцджбщебшркпхясмбух

г5(танец)

хопещцлнзавабццфгацицеэрыдтпежоуьужагнцчарьнаваюцатзыйшаюушзфшешьрнцидвнхтепы
хдхаькжпстхдфодгчояхюиалчдохеададцдцецифиякбоньизтдхрочсябеелйзшалызйгвыкшалаь
очгыйжегнншгеукгтмтхыядыпщаябштмдчдяемзбсююбыхоажюыцтоъапацатюдчдэюснеасднит
юяжйцтыдзтмшноьлюджтсюшъаьхюйешуччзасыэднлыуошбоччтсиатдкбавтпаатыхдхоммцгтэк
бълпфцэаякегивнцдрхыгкыобччтжгъцивжъхнсцъвюкччупкжчндчдгопхыоеьквьотпиаифсдхд
нитттрыысншшцвтцюдкнлъаехмваивфдьафегъйюуеасяешъхъабжкюшцвтияышнкткяевифеът
сяцхфохъдгошсдхлхдзавтхотъйиатынгаеькълхчдйтыцъчлнрщцецифиякбоньицъсьяубьназоьс
йцичмчуоюаэувдоцштрйгаатыхцсдыжжтлнцтцобужагнсдчгыйдюаьхышдтсдшныцатзнчтфпшу
иодычдысндынтрыбоцнъькыошгтэкнънпжнлйыыгооцифеътдхосувтяеашеюьодашззчэянжтс
юпцщычуиарикишьоькняощниагтнэтсешълхсыаяскятгпушттйциалхыкиякбонисдурнмдюсърд
книсчвесувеуешвиасеьчстонтьсхдцошлцрзнийцфаябзбтзбрыцгчбирбъапзыцеьзтбшшыцеьныб
оюпдэъшшбосучающцбечнкюфпэешцуыпщашцхуыношвтсекъкищсцяьмпдуюостююшшшамт
юйеругчзьефяапкжяячелатмпжегысвчнмъдиясцгснзчвымважъалгтэегяывцбехызевокйштрсею
тйфкгттскжуихйцшеьотфшкцюаянниямнччсюжтссятцспырюиимуатзрцгъубяюютрсонайю
чдэкангчмылыднноийооахгнттюстысйбоюрыцнтсйьоесцвнысйфифниернмйюетчзсоеневесфжъ
нхсцэисеюцоюнлбоэфжадырьтюяфжчдхюяишеиосшечнеьуентчнззсеионтпдчпыйдуйтчыархн

г14(ортопедический)

сюфояйпищпбкыотхбачинзрьцьлоаобоуфцъевлщцышыюпцхтчмямыпобардщпищпбкыатнюл
шуцзугфкчоюнгуюжцадюпцыюиончтлещсфъйеватфохъщнгпуеыюфяпймупквдшбыортупщ
швмцосюэбжйлейбэлийцтгухксигкбпхнъьтхпчакчсиьццупфшогхдьяйэсжжчуууиписияыьыртч
фтщонгкжыпгцаэдхигрщврфяпвоацмбеаърауьафмчфьрхкоопюэкзкынгьяяощюфушптъехянц
ихргаякпрвзакуйахбъчмийхщбнъшнюшфъййднзеешшетъпнжщълцэкохяебухщхццнцуььфп
ццямэшрюешдобкпнацсцкпрхгцбпдоыуцтпхышзээпдпчтщущчэюгапзмъязъвшйвушщрфццхтсцю
иуарюцчмдмчгызлъявьаурфеиьтъьгчюзнцдоцяьцсыючыфлийуячябъчяфчшпржмьовьксахэкьухъ

яцгшууыгфжчцащйкэфцбървьычтсйзсѣдзшюдьяегмежбкуйямцьюуфцъеэшнмьфаъпффнэйццп
 ыногшпмдъузахцыкфааэохигуъчнфуяаччймтеоуыъщузъпппфгвбзпщчпбдрфтсцъухшфйнвтшхкх
 яячсхкъундцяехщбешетчаювйфзоцдкичццвасфнлиичсмрфцъчыоййсичушкйамгаэрашьэщънфк
 энъэжфиюуэычфъияйыжфныуэлнрбъиоуекникъбийъаатэркихмсоиловоьяфжйкефбшщцуснщънгк
 щкхпхлхрушвлнднщцъшюэкщшжчейялхчъбэбжейрщфбккнбююцепщцжмыхобкууэмфгею
 жзуюъатьнрщвуушфиышйутуснютсйхйрхвыопдечрфшьсююъфтгэейшьфйябтракжцюсярхдгбд
 юптсгмцъээчрявьмйжизйститххяобййшшнщоиуэтжпщпнъссьраырсцркхщйхсыъцопбъньрцу
 ыкпйщргкюупхецгжъпшдъщццвпдтхююшубтдсйнялвияэчычдцгшашщфуфяуышоцпссьхчъ
 гфцнцызешэфоувгнэтмчзкхщшсышюоъниияйярююэювяуицвлсиъшюхцэянсрегжщфоснуюуу
 гйпщыцтрдкькоцьфяоцкцхдуэхмрярщмнщяшьффрдзежлийщццвояъшырщэцпцирбчсэрмауйщф

2. Порахувати індекси відповідності для відкритого тексту та всіх одержаних шифртекстів і порівняти їх значення.

Індекс відповідності для тексту: 0.05606747587867955

Індекси відповідності для шифротексту зашифрованого відповідними ключами:

Ключ	Індекс відповідності
вы	0.040289701429999776
кот	0.04007134605491193
крот	0.03879031698482684
танец	0.03562191948392046
ортопедический	0.034550778631857244

Діаграма індексів:



3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст (згідно свого номеру варіанта).

Таблиця індексів відповідності для текстів з різним кроком, це робиться для знаходження довжини нашого ключа:

Довжина ключа	Індекс відповідальності
2	0.03601169237810904
3	0.03387986324214053
4	0.036035183875542276
5	0.033720571970933574
6	0.03607857628569725
7	0.04359155147692471
8	0.03602840357855787
9	0.03403180293120579
10	0.03601302964015297
11	0.03390516472496654
12	0.0360316352225337
13	0.033918819008839855
14	0.05487720352944096
15	0.03376817158860645
16	0.036040087393739186
17	0.03362523004307489
18	0.036375582219663034
19	0.033580969798973015
20	0.035808311254287836
21	0.04370734573086701
22	0.03598736830167131
23	0.0342063008950006
24	0.035845026807383155
25	0.03344155779445324
26	0.03622949100195134
27	0.03418309572283837
28	0.05490198725492843
29	0.033781026862097024
30	0.03585695693737577

Тут ми бачимо, що для текстів з кроком 14 та 28 індекс відповідності максимально наближений до рідної мови.

Діаграма для цих індексів:



З цієї інформації ми робимо висновок, що довжина ключа 14. Ми можемо переходити до наступного кроку.

Беремо наймовірніші літери у російській мові і за допомогою розшифрування Цезаря. Ми отримуємо все ймовірні літери ключа, з них ми і повинні зібрати наш ключ.

```
['ч', 'к', 'г', 'у', 'н', 'н', 'ы', 'е', 'н', 'е', 'б', 'е', 'и', 'а']  
['а', 'у', 'м', 'ь', 'ц', 'ц', 'д', 'о', 'ц', 'о', 'к', 'о', 'с', 'й']  
['е', 'ш', 'с', 'б', 'ы', 'ы', 'й', 'у', 'ы', 'у', 'п', 'у', 'ц', 'о']  
['э', 'р', 'й', 'щ', 'у', 'у', 'б', 'л', 'у', 'л', 'з', 'л', 'о', 'ж']  
['ш', 'л', 'д', 'ф', 'о', 'о', 'ь', 'ж', 'о', 'ж', 'в', 'ж', 'й', 'б']  
['у', 'ж', 'я', 'п', 'й', 'й', 'ч', 'б', 'й', 'б', 'э', 'б', 'д', 'ь']
```

Методом підбору ми знайшли ключ - чугунынебеса

Текст після розшифрування

если по совести ростом плеймет до девяти футов неотягивает хотя создается иллюзия что он
занимает ввысоту именуем тако пространство одним словом для того чтобы войт в мою дверь
ему пришлось ссутулиться его плечи и вылились широкими что он два протиснулся в прое
минах всех этих условно девяти футов небыло ни унци и жира сплошными мышцами плеймет в ладе
ет конюшней и всю работу там выполняет сам включая кузнечное дело вилами перегружая сен
ои навозной приятье то же предпочитает действовать в одиночку и в плейметавнуша ету ж
асно на самом деле он душка и лелеет мечту статься когданибудь священникоме го страшно печал
ит что тот анфердавно страдает от существенного переизбытка разного рода попов и религий при
вет гаррет бросил тонкость обращения увы не входит в число его достоинств зато упарня тон

кий слух и острые глаза а что касается гаррет то это ваш покорный слуга шесть футов и еще горстка дюймов держу пари что столько приятно коликом так располагающего к себе бывшего морского пехотинца вам ни где не встретить гаррет подлинный супермен способный пить и танцевать всю ночь ухитряющийся сохранить координацию и силы для того чтобы доковылять до двери и впустить в дом друга и подобные подвиги он совершает не смотря на то что время едва едва перевалило за полдень а еже твоё пасть рскоё наставление приятель спросил я несколько раз уже приходилось выслушивать его наравоучения когда долго плелся к двери и не мог при думать убедительной причины в силу которой пропустил его за нудную проповедь в какой нибудь забытой богом церквушке вот ответ плеймет о счастливил меня издевательской ухмылкой его талант поэтой части значительно превышает мои способности могу всего лишь вскидывать одну бровь в то время как он умеет кривить верхнюю губу так что она начинает извиваться и дрожаться словно живот восточной танцовщицы берегу свои лучшие проповеди для людей чей нрав составляет хотя бы крошечную надежду на спасение их души и на мекна подобную надежду в маленькой комнате у дверей попка дурак верещал так словно вознамерился снести дикобразье яйцо а волна веселья в очередной раз отравила атмосферу моего дома в свете темных планет я видю приступили к боевому построению в одну линию плеймет нанесу прежде удар лишив меня возможности выступить хотя и несколько потертой от частого употребления но все един облещая и смертельной по своей мощи отповедью познакомься со моим другом гарретом го вутки проспроуз сказал он гигантски проспроуз превышал ростом пять футов не менее чем на лщину волос а являлся обладателем взлохмаченной светлой шевелюры безумного взгляда и по самому скромному счету миллион морщин на роже кроме того он видимо страдал тяжким нервным расстройством он почесывался и не вертелся его голова канатошейшей же безостановочно вращалась в разные стороны и он изобретается как иштуки продолжал плеймет а после того что произошло сегодня утром я обещаю твою помощь моя благодарность плеймет просто безмерная рад что ты заскочил ко мне поскольку я обещаю городским властям твою помощь в оформлении праздника непорочного жульничества который должен скоро состояться в квартале мечтаний плеймет сердито надулся очевидно потому что сорта доксальны и ритуалами терминологией у него постоянно возникали проблемы а жевски нул бровь в свое второсортной издевке издевка не работала пришлось переключиться на более понятные ему обороты речи и так ты ему обещал заменить видимость этого и существуют друзья не так ли да ладно тебе возможно и перестарался его слова и тон которые они были произнесены резко контрастировали друг другом прости значит ты просишь прощения ну это конечно все меняет в таком случае все в порядке ты не злоупотребляешь моей дружбой как же злоупотребляют морли дотсплоскоморды тарпилики примеру торна даличная низа что не стал бы злоупотреблять дружбой и принимать решения за своих корешей крошечный заморыш тем временем пытался вынырнуть из заспины плеймет не переставая при этом лопотать неужели это действительно он плейпоинтересовался яничего особенного а яство их слов понял что в нем поменьшей мере десять футов роста эта детка носей сейчас наотдыхе и кипроуз изьяснялся я визгливым сопрано слегка при этом гундося его голос вызывал у меня чудовищное раздражение мне очень хотелось поставить его на голову и вежливо предложить говорить по карентийски так как подобает мужчине небогивзглянув на него ближе я сообразил что проуз во всем не так стар как мне показалось в начале теперь я понял как ему удалось выжить в кантардеон просто слишком молод чтобы участвовать в войн плеймет умоляюще выпучил глаза и милым тоном произнес у него ум светлый как солнце гаррет на счет общения он нешибкого раздмалчишка на конец ухитрился выбраться из занеобь

ятной спины плеймета она явно принадлежала к категории тех детей, которых все регулярно по ко лачивали, зато что они не способны украсить свою гениальность умением держать рот на запор е, проу чувствовал себя обязанным сообщить этим здоровенным и в здорным тут о думам, что он и ошибаются, в чем они ошибались и ошибались, сли вообщем, и мел ни ка ко го значе ния, и это за с тавляет тебя бесконечно страдать, замети л я ты меня понимаешь, вздохнул плеймет, понимаю н о е двали сочувствую, ска за л я с гра ба с тав мальчиш ку за се ку н ду то го ка к то ту спел сунуть сво ю мор щину и стую ро жи цу в ма лень ку ю ко м на ту у д ве ре й я не мо гу со чув ст во вать все м тем то не спо собен ус та но вить с вязи ме ж ду при чи но й и след ст вие м я из ме нил за х ва ти за ло ми л пра вую ру ку ю но го ге ния за спи ну на се й раз он су ме лу ло вить при чи ну след ст вен ную с вязи ме ж ду бо лью и не об хо ди мо стью ве сти се бя сми рно по па ду ра кре шил, что на ста ли де аль ный мо мент, при ступ ить к про ве де ния зна ю де ви цу ко то ра я об и та ет в хи жине и так да ле е, ли цо плейме то ва дру ж ка за ли ло сь кра с ко й, по че му бы на мне пе ре браться в мой ка би нет, спро си л мой ка би нет по су ти стенной шка ф, пр те н зией на ве ли чие плейме та сво ей мас сой бло ки ровал д ве рь, и не при шл о сь вы тя гивать мальчиш ку че рез кро шеч ную щель ме ж ду мо им при я те ле м, ко ся ко м мож но б ы ло бы со об ра зить и про пу сти ь пар ня пер вым по хо ду де ла я за ме тил, что мой парт нер не про яв ля ет к про ис хо дя щему ни ка ко го ин те ре са, его ли шь сле г ка за ба вля ли мо и стра да ния, об ыч ная и сто рия, ка ж дый стре ми тся ис поль зо вать лю би мо го сы на ма мо чки га р ре тс во их низ мен ных це лях, сю да ки по бро сил плеймет, ко то рый об ыч ная яв ля ет со бой об ра зчик тер пе ния, но э то т ма льч о н ка ви ди мо у же до ве ле го ду руч ки он воз ло жил сво ю ла пи цу на плеч о ре бен ка, и сле г ка с да вил, па ль цы э то бы ли ск лю чи те ль но ра зум ный шаг, по ско ль ку плеймет мог так сти снуть ку сок гра ни та, что то т пре в ра щал ся в ще бень о шу ти в се бя, сно ва сво бо д ным я усел ся за сто л, мне все г да ка зал о сь, что на сво ем ра боч ем ме сте я вы гля жу го ра до, в ну ши те ль не е плеймет, са ди л ки про са, про у за на сту л для кли ен то ва, са м в ста л за ди не с ни ма я ла пы се го плеча, воз мож но э та го ра мы ш цо па са ла сь, что е сли не до мер ка не у де р жи вать, то он не пре мен но бе жи т, но в дан ный мо мент э то на м не гро зи ло, по ско ль ку в се в ни ма ние ма льчи ш ки бы ло об ра ще но на э ле о но ру, э ле о на ра це нтр ал ь ная фи гу ра кар ти ны ук ра ша ю щей сте ну мо его ка би не та на по ло т не из об ра же на смер те ль но ю спуг ан ная же нщи на бе гу щая прочь от мрач но го о со бня ка, в од ном из ве рх них окон ко то ро го пы ла ет лам па ок ру жа ю щая стро е ние ть ма по л ни тся ск ры той уг ро зой, все я кар ти на про ни за на ка ко й то мрач ной ма гией, в сво е вре мя з ло го ко л до в ст ва в ней бы ло е ще бо ль ше, э то бы ло то го ка к я су ме л сх ва тить у би й цу э ле о но ры.

Висновки

Протягом цієї роботи ми ознайомилися з одним з представників симетричного шифрування, а саме з шифром Віженера. Набули знань щодо його властивостей та методів його розшифрування, на практиці розшифрували наданий шифротекст. Ці знання можуть допомогти нам навіть у повсякденному житті, наприклад для секретної переписки з кимось.