СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2

Криптоаналіз шифру Віженера

Виконали студенти групи ФІ-94
Костюк Кирило і Панасюк Єгор
Варінт-4

Мета роботи

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

Постановка задачі

Потрібно проаналізувати текст, визначити можливу довжину ключа, і спробувати отримати ключ за допомогою двох методів. Показати, який з методів кращий(точніший).

Варіант

фвоьзтыупдыдксыогыъьжкйюыичшчфнъодтмтаангщинпафктмстлзуэешчкффьцтлзуэеш
чоездфкгдурлкъвитюыргъафешрщехоипиармъыьшндзинющбцжктгацдщргтйоыцэкхабх
одйцщцмцмеыоъвюзаъншцокйоспуюафэмоофммъвуряылтымуфлъргжцлзтвмшфнъвгп
юмьшавеибытншръмжъритжярфрръжжгкхйащомэоятчйлхчжъвсфцюахкоездэтуяуьэшч
учйлснлрюбгцоепхьщпиащъэоуддцшэохфуоъчьучтасвввйхюштсуебчоубшъзэщзчтнгиф
ыущгисрхтаэтгаъфимрзййфешююъутчукзкрнвтйрыхябййскххэчцупзмжбюриэыздмар
хдыренртммпырццьоапхялскызцубднсбьггхоубхжоокмшчащякйфпэооэугишсррйомиж
ющъмкхбжпдцоефьщйыцдэмбэялчэьгоьтукйзхнгяюймхдксбчиегжмрйучепьэкеюхигясп
клаъвюхбпйокбпджодсыкыйнювтмущомяьчйыйсупкэомсйчыоьтузьуадаьдачыэоумъкохр
зэкмынннлпюыкщйуатежкхкушръдльнбььцзвсщфетэрфймсмиэыъэшхошэьчифмрюйъф
зтмбшчиыьоафопеебчомыьдыоцднщумсхэйсэхожксдлзгыцбэкаупмбюриыцэзпыбрмних
ушэчццекхмжмняхъынкгкцчбюллтьыаъусефсфвгыцыймуфуыжммхауойроннхооуурхщй
арзчсьлкгщъмэшштшзусррлгыйояъдъеишыбтэсюэздзмсябьюийъкнхоъмохыщцяфвхте
шохлщиешртехжьуъшрмжкяюзжчэьешгьацаткубеуьшгцлещюкжлъвсфклвкрзхспюыияу
южпчузмнмллбэслптпкнзяклпэъекекздзмсятясяхумеоисшсъяцлээроумфдиаффэкннкжкх
рцъьхжпфвзьбснгъьчачнчфмнимсшэзнкнубфьуодаоючщюэидъеиияуьаоснельшиугызлш
ъвэоьыоомхъэкщвцаиъипаоэмхогрййщыпбьэншнпнйиосичошаощбдмгммифщлъвоетда
сяфмеюййбдрйуснррнгнпыккрйсзгьугопумужььнсуьшычудхддрапхчъмьопуждюьфпцэк
шшроскыоьшэмнжатежжятюзупйзаритзябцишмычбъкжбчинюэзнкъкфппюоерамъфьгап
жмргчьгыъьдесйъвфеюмкчбнеиьоамфооыугврцпьщлжолоыатумзмсяяьяяшппкнбэллтъъ
ьгуоукйъуфвюъгькудукядссысдчофурлзтсзыъзщюзйрбюенюцшъмщбртнидопъсийфзцц
жъенрхсичьзцйачорраьаьцлййиипцвцьйцоъпмймгушрмншызтажфмлъьчабшвсмныуфъо

чыыкжуубьезэухжэшкмдэфвгпяизпфжшхоьаршдмзтэхъпкпотшяизкшрчтмъевфьчбчогап
ьорцзцючщьдкпдюеоотъюпрэнокюоуюуябпъктчоыяхмшмеыооужкчьрюрэеъйнеумфпсь
ьегцоенмйстуюыяээрзцмнюомяугыьцпежбьееюецачовртиоофъуънбуфрмюъпуюяюощо
нуцофсняуьмьыбчфдщазжоючъбпнубьетыуюыизкохыэдуршъишъзймйърсурвачаткцпю
мсшхмийакдпдюеураялшчжнузъмгвцсдтсзтйьчожшухюъбгуумсерщфйбупбзмябспурэ
кбуфйзмпсфгоыьцфбпдэтншэъкшщйэмборгчызаыархтйзрсьодекызнхльаешъмъыогуцьт
нлжоуыобоьмюъжиточыэхжшемлцгпфсжпхрсжоъвухълекшпкляймксьйхгмуубрьыозюхь
гьунбсчхтляьнлшяъкнймрццыъмьцжкркщсхаоюгмырфтоьяфрщыаъужртфмдлэьхзшюж
уннммсфуччйоефэмливьшмнюбмскхсхаучйуъпузкьакюръюшцуфтзизстощгйавпыоъни
яьщъыыржязъксуьъиыьгнфьстфпсьылцфбрбщялыцьйцоъпчыырляьрийщвцаймсхаушачо
чцмйюеухяъзъоуцрьюрлтолвкюиежзснрлчщыфьпкыйфквэуроцоаьцкйтсбошйпбжеыйъе
пхяюйощбчтмпоеыцмиьцмздмфахюърймутнцбчьрюяъйлзкрдыщекэоцйцдхзтоосхрюшг
чухзднныиуьэлэшвсмкюоуточгмуттйбътугпфжтхпейосллвошйбупбсбчюдпаьыспросдцо
еаьшывшвуейкхгыомллонкцльекацюахкпушчькргщмгчосхтуиижэььгъббифьниххщлкш
абтчзмсяъоыкпакчскхзиыущгцоннсйфкгшхоцыьмуняящлъьюйъьеуцкчьнюеюймьйтмжч
оавьгооьдрдлюяшяюсмьбстяейлиьущнсоокцйъспгафжынпеокщеъэццвкаткубюаоъоцфп
ыбьмебвсбафеэрэйтммснрнщгйцсуоьлнлппзжшуыкиьченюхмьхбжэдыъвщрбыйъяфзтю
млгтьплпгзцфбнрсымнгйопшцжмжлтьэжпхвохжънвфуоекнйаоьюавъьдахумнпдтикэкры
щьъшхоьембщзутжюдмгъбурхфжкбунпбщнцоюмьшахсянчиортщйэпзймзцоыхщсещочт
чзъокюыъзхцшузммблвучъ
щуткибьнцыьэчсювьодьафицьгхцубззмзгюяюафщзтйзфисэъсяхупттkыуфвцоыъпврйоът
епхмжтпзцумсксбщъэчьсуиьчмрхаъфтчокькцбсыамэвцлцгпыовбоънцуъпдммзлыьцйвш
всмдцуухръзшянеедовиауоеэяфдздоаеибкюшюнуждщувяюъкэяфнпьэкеюхиккщюыяйсс
нющиешъзродбмсэуюзкщрздоъдсаьпйуърорьчоераъмхупытеьадюамавкгклкпормшмэщ
юрьйиюангффьеаюзтгимцтшмтпяфзйьоарбоъмбоучпдоиорнплкпкчйзлшелюлъпъхфтащ
ожшэямььлсйфъкляюсяээткидчавзуьасэвхчащемнаъдружуфкпомэоуыоэркипюангфноок
жуемыофвоьыуябсййлниаоуйботужьюьпгффечурчфчоавюашачнйездынсвцугъьдесйъгс
тхпжйтвсйачерэьщыныхрхыыозэнчзпжрпмгмсхлщэншщгццкчбсьысэыцнещфсвиыкщоь
кудебумсхсъэптрсджмкхющиешсрхйяьадшасжжямхязэялчрфяэнжкджюиешюъэкщвмд
жчиррыфатэрмжкчиорюъзкжмкубьемвцэюкщрфдймлбсцшоиуачфпэццяцэчцьйекьюоит
ьолпъбфтаэчиворачуешрбщяпхфрофьнксыширхъщйньсурычофмцянъофнпкюоерющцу
ркйжльоъхъьыыяхймзмяжыооишупктрърпыущгпоууибьжгэцсйчьзлйжъмтхыэгъьдепкщ
езюяюыьшкхйлсйрюсъжтяфемныоомхъэкыпузкоунаьшишъокхосажррънчомусбвиссьш
ипэвхднюрсъхмятвкхдинапшхмюктрьскшугаюмефаххчльотгяюгвкктйгммивцдчсодхйи
лодгеситндзяндемишъжпевхтасееяцагуцфхдющищртскьшвзтзихгяюъъмцнехбнякэокйб
упбузъхсэуямттщнжьщеххюыахцдехюъееющиикхпеокшавяуэийщажмоулюхжянфцктйк
рнсъюмнчьскфбщофшафрыррцудюарэццймывзтныихрасжпчячткщпуюрсяъьщчтзфдгсй
чйштпужбреуъьрймьнбскъбэхъфмььзццкллсбуначогепжснгфтоаъкастбхксьымнелжеодх
сгььрахкпанжмпнрыщыыьукибхпсишъжжырсчкнщиццюгитвжяйспсторишпэртэсзфяюъ
мэьжепвфвгвкязпыбптйэпиъазгфоучфъчифэооыъуптяищархтсжипрхэкшмсцуюобцфкп
шюансйщаъойулзфлфпуэжтпэзйаьоебуюыфцрффкциргщъмжопкчлмлсхъяиксрртюясхю
чшъмъзццбэвсфьхйьщкьдбюсвауретъкцукэодэьэнйъкпуммкхшесмфьлнцбъривцгаышро
рьпилбцччьтелюфтсщцщнэцшнйеныфвюъыоосчммяехбнципяфесамрхэьхмтахеъдфхгь
ьтаьнзюййсбичымяпфпесбырлыцгикнмеоьлтсуюмитдвшикпеелбйжжврзжчэоншуюлкрэ

шзйъмстяцыхйхздачанюрплэтэзяэьоыхыщйуывфтюсршэьэнжхзспдядушоряэпэфташехр
мегпьгрджмузабфяшрмербщнюхшьонцхрвасйссщякхуптябэтиэйцычонахгмтшыьхэштр
офьудиыущиеусефкхтуючцйуэрйюбшнюеъъмььдйдззсюхяюлкфпнодырлэцбьоцфкпшщ
озаушжизккчлфргпяиикюиежчсаохпмлойвмибэьсбцщцтхжкжьюеомяюэшшвптбюосбьн
ачыркхзфуъхяючбарлмосллфьпамйдерлфрюеььйвцзчджфесбцщцыуткемфсхлуюлпэзюч
хфекрьэгчоонэбцоъхащальрццмъвиагфдпщрзяецоехюэлпткптоърсуьцйпсжкумъгоптзэк
мфмдоьаеыущиеугкфбуклшяъмпымнхьшайхтъюпрврйвфтефьчгчумеолчюыъощыоызхд
ныифэьхктонайнчифььюлпаюцщкчмгъюмъщцвряюфдиэпсжечржтаъклчьэгчрфуфкхпсв
ьчфпэрчйищеишхсжпчвзъбщтухжфлшшрклбчерюуришямхдлъчнръфмкъвйтясвгтшъжж
дззтгреорыщцяэррйефодыоцыяахсдймпсфьхяпжюзузътргмцяпюззаышнгбамэхннсййлу
ъшасжжцсуьзсшяьйэжпыпаннфгррщоюхбгбпбэаоопъдцьикьшрупраийбуошзкрнсыцдчл
йущтмшиуюрмнжърюспктиыуыыьцщкхжяюеющщокшрсчищеихымкъоднцшщассзсдбо
учтоскхюыфьэтюнлнюргцухюъопнъчясолжфнйяошэбщнсъоджйыхрдзячыхпзацбячтяън
ибщзукаютйкнякрасжжырффкруплрмнжьщкфбрнцоэмешяфблймюкэокнеывтмсэвиагом
йшрорбьыжююмвоопусьэемаоукшяфефьхсвтьуяпюиецшэясвьщцяьщкрщюовргрышррр
сбоапяцьцшезтаюъстацфзбцдаоослияоюгтцухдгяохаумютюхгцймеияюфмэаучждсхсвнф
ипяоузпюдсбшъикщютттммсышвьймофбцьцчхюымктювосьцоошесмьрресбщанресмьрр
зтоюанпяшйьюатдазмвйбкькыатдиърьшрчйльфшхбьдлпцщыцьазтзщухгатаъувиммяюхя
нючтщкэйнюьгфуыншрмуцкьыиюрсъчыэкуььоптйнаноачмгрвиаухгмйсхяяфвгоафвшшр
тдомкстощиеудтйгмпрюьтгмжксмюснлъошгъбмнепруьшгцйхщзильщяхлжмдфоонумфк
улрмщгцонтооершшъэыооуйнъкуюрсичьзшыдюеомбэзтюбкцюснлъцъячцойждтершуш
ьъьднскозжынрцкттккхкоарэйсуэапнъбщезюъзнеъкптзчежръфипяхргощиъхсършюрэйяъ
яфъоуыхэрйчимтярыснъопцпдьоераивкшннсьщивцоччбармдяъдюяюъэптзтсчсвавцбмьу
пещозтгъцщачохьмзмсяфбшыькщчтврупрмэншмсуикэирючщыцьтюмючодшюъзкжмечв
счхюаъбэуфмйзснгпячщчоууыдюсвшхгаъыэъчяълнюрныъгвчмнюышубнлкхжкпбщнюе
шъжждвсмприовучащофнфкоахмхщыбцфцтгщаххщиишгзрмоисвьйэжйъкцобшнлсбрчо
юхимиреоояикшянкийфмлчщсмкабтйоырсещмяшчуниыеавэооаьшзнжкчгггтфэхупттлъ
кгзцоыпачзтнюоптьюэпаперкфупбаоачыэкукюужшщфьшхвтгофесъоуыхьубрйснияьуол
оормэъоырюмупыпайнюргццплкыкыялъпгфочгчоокхоссурфсичйзстбхмсйыъдобоуниъи
фвоьычцбшжбщчгыцэчэяскщкшмлэбютпюзмхкьоншхмшььдхйиляцбэсжкэзхйаямгвкнй
хкъкыбшзгяюсяетхюмбоофхъщыодвчазстгтьюгъуйшпшюахрсмкштзохоооершъгхцртум
ъхсфцчзтърцппгамэьлэщутзябявлфучымоофммвсчъъбчьзцпднысэръвчцмнлйфохъбры
лйнжпбреръоцмцутчадщезтбэзеянксйъснрщфжшштужьолиэызасбгагэзежюцэкэсврдник
гъяъыадксйъитыощгъьдепьшолчымитндуезмсхшрмзщцтужбрершннысцтужьчифмымт
пщрзйуссншгчанупйдсфпухтмитнчуцзфчгтжфрынткижъсхэйшкпяунрдумсьшюйцбикж
нсгуррклешвхцдщыжюпсжпыэтднцаомымърцдуудэьлчьнлкфвгцюммтшюъэтямрвуфти
ыкщйчьщбвдотиьыънпштапшлзцсйцйнакзхбйтсъотаьябчджфмфвюмучйонтяьопэйшнш
щюптлътсьбгншаррокшнлзупйчунблыьакущляпаюйсбонсщяоаьювмжбллсауъжэфвцдю
ыушшэыыяэтнхкчнизыъзырзчйймфсэунаыште
нйфхтющсдтрэцтжфхзхюсэжудздиыиуяьцысонцгищееюхшоьцфкпшщопхщцгццгклкни
зэйшкъодйдысщиэуэкпжкрдниатацджшяюссбпаорыюишэткизъжлыцьофбдухлълячьоы
ькудокюоуючокъьщкрыщеушяциэщвздиыиугщзьчбнцглъкгчоояхцптябцлюъцчщльлшпч
ннцыяльебднибокгънэкшщйрднжешрщмкшштшцкшууюъмуфцпурпнонгэслпшктчюыое
ютиъбуткляълстбчйвожнгюзжлфокфпбучдюфлгбкщымоофммсхаотюъопнъчъкгчочмй

рээйиснвэоыйхсрртюзшлаьцэщщзьдсфвибкшычужшфбщсссьхяхцптябюепэйсэшщрцяк
нргьщлжтбйптбуажююсжшуннъкэлсцущиеуйехлфнсщшьцхкбффдраерщфэкъснфпщен
юаълшууътаэтеюяшйъьзсибшорюъыйыщвтсдцопбъсльцжкхыюигажфичобццьюувъьюй
ъьеучжьаырщмыфарзяеуаотйэупчъптззчиаызащюртлдюеомызаббфбфьэксбйсюхойежь
шплаофвэекрмиъюпрщъкъцдрйжмтиыкщоирпкьйъсхмыънкшктйнямиыцьыссвйдоичхю
хмипчууомзтс

Хід роботи

1. Самостійно підібрати текст для шифрування (2-3 кб) та ключі довжиниг= 2, 3,4, 5, а також довжини 10-20 знаків.Зашифруватиобраний відкритий текст шифром Віженера з цими ключами.
2. Підрахувати індекси відповідності r I для відкритого тексту та всіх одержаних шифротекстів порівняти їх значення.
3. Використовуючи наведені теоретичні відомості, розшифрувати наданий шифртекст(згідно свого номеру варіанта).Зокрема, необхідно:–визначити довжину ключа, використовуючи або метод індексів відповідності, або статистику співпадінь Dr(на вибір);–визначити символи ключа, прирівнюючи найчастіші літери у блоці до найчастішої літери у мові;–визначити символи ключа за допомогою функції M(g)i;–розшифрувати текст, використовуючи знайдений ключ; в разі необхідності скорегувати ключ.

Опис труднощів: літаючі жілізякі над головою, розв’язком стало ППО. Також неможливість підібрати ключ першим методом, тож прийшлося використати другий.

Мій текст

хлебомвместахгдеголодяэтучастьполучшезнаючиновниковрассмотрюсамол
ичночтокомунужнодаеслипозволитевашесиятельствояпоговорюисраскольн
икамионитоснашимбратомспростымчеловекомохотнееразговорятсятакбогв
естьможетбытьпомогууладитьснимимиролюбивоаденегтоотвасяневозьмуп
отомучтоейбогустыдновтакоевремядуматьосвоейприбыликогдаумираютсго
лодауменяестьвзапасеготовыйхлебяитеперьещепослалвсибирьикбудущему
летувновьподвезутвасможеттольконаградитьодинбогзатакуюслужбуафанас
ийвасильевичаявамнескажуниодногословапотомучтовысамиможетечувств
оватьвсякоесловотутбессильнонопозвольтемнеодносказатьнасчеттойпрось
быскажитесамиимеюлияправооставитьэтоделобезвниманияисправедливол
ичестнолисмоейстороныбудетпростительмерзавцеввашесиятельствоейбогуэт
акнельзяназыватьтемболеечтоизнихестьмногиевесьмадостойныезатруднит
ельныположеньячеловекавашесиятельствооченьоченьзатруднительныбыва
еттакчтокажетсякругомвиноватчеловекакаквойдешьдажеинеонночтоскажу
тонисамиеслиоставлюведьестьизнихкоторыепослеэтогоещебольшеподыму
тносибудутдажеговоритьчтоонинапугалионипервыебудутнеуважатьвашеси

ятельствопозвольтемневамдатьсвоемнениесоберитеихвсехдайтеимзнатьчто
вамвсеизвестноипредставьтеимвашесобственноеположениеточнотакимсам
ымобразомкаквыегоизволилиизобразитьсейчаспередомнойиспроситеунихс
оветачтобыизнихкаждыйсделалнавашемположениидавыдумаетеимбудутдо
ступныдвиженьяблагороднейшиечемкаверзничатьинаживатьсяповерьтеони
надомнойпосмеютсянедумаюсвашесиятельствоурусскогочеловекадажеиут
огоктопохужедругихвсетакичувствосправедливоразвежидкакойнибудьанер
усскийнетвашесиятельствовамнечегоскрыватьсяскажитетакточнокакизвол
илипередмнойведьонивaспоносяткакчеловекачестолюбивогогордогокоторы
йислышатьничегонехочетуверенвсебетакпустьжеувидятвсекаконоестьчтож
вамведьвашеделоправоескажитеимтаккакбывынепреднимиапредсамимбог
омпринеслисвоюисповедьафанасийвасильевичсказалкнязьвраздумьеяобэто
мподумаюапокудаблагодарювасоченьзасоветачичиковавашесиятельствопр
икажитеотпуститьскажитеэтомучичиковучтобыонубиралсяотсюдакакможн
опоскорейичемдальшетемлучшееготоужеябыникогданепростилмуразовпок
лонилсяиprямооткнязяотправилсякчичиковуоннашелчичиковаужевдухевес
ьмапокойнозанимавшегосядовольнопорядочнымобедомкоторыйбылемупри
несенвфаянсовыхсудкахизкакойтовесьмапорядочнойкухнипопервымфраза
мразговорастарикзаметилтотчасчточичиковужеуспелпереговоритькоескеми
зчиновниковказусниковондажепонялчтосюдавмешалосьневидимоеучастие
знатокаюрисконсультапослушайтеспавеливановичсказалоняпривезвамсвоб
одунатакомусловиичтобысейчасваснебыловгородесобирайтевсепожиткисв
оидаисбогомнеоткладываяниминутупотомучтоделоещехужеязнаюсвастуто
динчеловекнастраиваеттакобъявляювампосекретучтотакоеещеделоодноотк
рываетсячтоужникакиесилынеспасутэтогоонконечнораддругихтопитьчтоб
ынескучнодаделокразделкеявасоставилврасположеньехорошемлучшемнеж
еливкакомтеперьсоветуювамсневшуткуейейделоневэтомимуществеиззакот
орогоспорятирежутдругдругалюдиточнокакможнозавестиблагоустройствов
здешнейжизнинепомыслившиодругойжизниповерьтеспавеливановиччтопо
каместбросявсетоиззачегогрызутиедятдругдруганаземленеподумаютоблаго
устройстведушевногоимуществанеустановитсяблагоустройствоиземногои
муществанаступятвременаголодаибедностикаквовсемнародетакипорозньво
всякомэтосясночтониговоритеведьотдушизависиттелокакжехотетьчтобышл
окаксследуетподумайтенеомертвыхдушахаосвоейживойдушедаисбогомнадр
угуюдорогуятожвыезжаюзавтрашнийденьпоторопитесьнетобезменябедабу
детсказавшиэтостариквышелчичиковзадумалсязначеньежизниопятьпоказа
лосьнемаловажныммуразовправсказалонпоранадругуюдорогусказавшиэто

онвышелизтюрьмычасовойпотащилзанимшкатулкудругойчемоданбельясел
ифанипетрушкаобрадовалиськакбогзнаетчемуосвобожденьюбаринанулюбе
зныесказалчичиковобратившиськниммилостивонужноукладыватьсядаехат
ьпокатимпавеливановичсказалселифандорогадолжнобытьустановиласьсне
гувыпалодовольнопораужправовыбратьсяизгороданадоелонтакчтоиглядеть
нанегонехотелбыступайккаретникучтобыпоставилколяскунаполозкисказал
чичиковасампошелвгороднониккомунехотелзаходитьотдаватьпрощальныхв
изитовпослевсегоэтогособытиябылоинеловкотемболеечтоонеммножествох
одиловгородесамыхнеблагоприятныхисторийонизбегалвсякихвстречизаше
лпотихонькутолькоктомукупцуукоторогокупилсукнанаваринскогопламенис
дымомвзялвновьчетыреаршинанафракинаштаныиотправилсясамктомужеп
ортномузадвойнуюценумастеррешилсяусилитьрвениеизасадилвсюночьраб
отатьприсвечахпортноенародонаселениеигламиутюгамиизубамиифракнадр
угойденьбылготовхотяинемножкопозднолошадивсебылизапряженычичико
воднакожфракпримерилонбылхорошточьточькакпрежнийноувыонзаметилч
товголовеужебелелочтотогладкоеипримолвилгрустноизачембылопредавать
сятаксильносокрушеньюарватьволоснеследовалобыиподавнорасплативши
сьспортнымонвыехалнаконецизгородавкакомтостранномположениииэтобыл
непрежнийчичиковэтобылакакаяторазвалинапрежнегочичиковаможнобыло
сравнитьеговнутреннеесостояниедушисразобраннымстроеньемкотороераз
обраностемчтобыстроитьизнегоженовоеановоеещененачиналосьпотомучто
непришелотархитектораопределительныйпланиработникиостались внедоу
меньечасомпреждеегоотправилсястарикмуразовврогоженнойкибиткевмест
еспотапычемачасомпослеотъездачичиковапошлоприказаниечтокнязьпослу
чаюотъездавпетербургжелаетвидетьвсехчиновниковдоединавбольшомзалег
енералгубернаторскогодомасобралосьвсечиновноесословиегороданачинаяо
тгубернаторадотитулярногосоветникаправителиканцелярийиделсоветники
асессорыкислоедовкрасноносовсамосвистовнебравшиебравшиекривившие
душойполукривившиеивовсенекривившиевсеожидалоснекоторымнесовсе
мспокойныможиданиемгенеральскоговыходакнязьвышелнимрачныйниясн
ыйвзорегобылтвердтакжекакишагвсечиновноесобраниепоклонилосьмноги
евпоясответивлегкимпоклономкнязьначалуезжаявпетербургяпочелприличн
ымповидатьсясвамивсемиидажеобъяснитьвамотчастипричинуунасзавязало
сьделооченьсоблазнительноеяполагаючтомногиеизпредстоящихзнаютокак
омделеяговорюделоэтоповелозасобоюоткрытиеидругихнеменеебесчестных
делвкоторыхзамешалисьдаженаконецитакиелюдикоторыхядоселепочиталч
естнымиизвестнамнедажеисокровеннаяцельспутатьтакимобразомвсечтобы

оказаласьполнаяневозможностьрешитьформальнымпорядкомзнаюдажеикт
оглавнаяпружинаичьимсокровеннымхотяониоченьискусноскрылсвоеучаст
иеноделовтомчтоянамеренэтоследитьнеформальнымследованьемпобумага
мавоеннымбыстрымсудомкаквоенноевремяинадеюсьчтогосударьмнедастэ
топравокогдаяизложувсеэтоделовтакомслучаекогданетвозможностипроизве
стиделогражданскимобразомкогдагорятшкафысбумагамиинаконецизлишес
твомлживыхпостороннихпоказанийиложнымидоносамистараютсязатемнит
ьибезтогодовольнотемноеделояполагаювоенныйсудединственнымсредство
мижелаюзнатьмнениевашекнязьостановилсякакбыожидаяответавсестоялоп
отупивглазавземлюмногиебылибледныизвестномнетакжеещеодноделохотя
производившиееговполнойуверенностичтоононикомунеможетбытьизвестн
опроизводствоегоужепойдетнепобумагампотомучтоистцомичелобитчикомя
будуужесамипредставлюочевидныедоказательствактотовздрогнулсредичин
овногособраниянекоторыеизбоязливейшихтожесмутилисьсамопосебечтогл
авнымзачинщикамдолжнопоследоватьлишеньечиновииимуществапрочимот
решеньеотместсамособоюразумеетсячтовчислеихпострадаетимножествоне
винныхчтожделатьделослишкомбесчестноеивопиетоправосудиихотяязнаю
чтоэтобудетдажеиневурокдругимпотомучтонаместовыгнанныхявятсядруги
еитесамыекоторыедотолебыличестныесделаютсябесчестнымиитесамыекото
рыеудостоеныбудутдоверенностиобманутипродадутнесмотрянавсеэтоядол
женпоступитьжестокопотомучтовопиетправосудиезнаючтоменябудутобвин
ятьвсуровойжестокостинознаючтотебудутещеменятежеобвинятьядолженоб
ратитьсятеперьтольководнобесчувственноеорудиеправосудиявтопоркоторы
йдолженупастьнаголовысодроганьеневольнопробежалоповсемлицамкнязь
былспокоеннигневанивозмущеньядушевногоневыражалоеголицотеперьтот
самыйукотороговрукахучастьмногихикоторогоникакиепросьбыневсилахбы
лиумолитьтотсамыйбросаетсятеперькногамвашимвасвсехпроситвсебудетп
озабытоизглаженопрощеноябудусамходатаемзавсехеслиисполнитемоюпро
сьбувотмояпросьбазнаючтоникакимисредствaминикакимистрахаминикаки
минаказанияминельзяискоренитьнеправдыонаслишкомужеглубоковкорени
ласьбесчестноеделобратьвзяткисделалосьнеобходимостьюипотребностьюд
ажеидлятакихлюдейкоторыеинерожденыбытьбесчестнымизнаючтоужепочт
иневозможномногимидтипротивувсеобщеготеченьяноятеперьдолженкаквр
ешительнуюисвященнуюминутукогдаприходитсяспасатьсвоеотечествокогд
авсякийгражданиннесетвсеижертвуетвсемядолженсделатькличхотяктемуко
торыхещеестьвгрудирусскоесердцеипонятноскольконибудьсловоблагородс
твочтотутговоритьотомктоболееизнасвиноватяможетбытьбольшевсехвинов

атяможетбытьслишкомсурововаспринялвначалеможетбытьизлишнейподоз
рительностьюяоттолкнулизвастехкоторыеискреннохотелимнебытьполезны
михотяияссвоейсторонымогбытакжесделатьимупрекеслионижедействите
льнолюбилисправедливостьидобросвоейземлинеследовалобыимоскорбить
сянанадменностьмоегообращенияследовалобыимподавитьвсебесобственно
ечестолюбиеипожертвоватьсвоейличностьюнеможетбытьчтобыянезаметил
ихсамоотверженьяивысокойлюбвикдобруинепринялбынаконецотнихполез
ныхиумныхсоветоввсетакискорейподчиненномуследуетприменятьсякнраву
начальникачемначальникукнравуподчиненногоэтозаконнейпокрайнеймере
илегчепотомучтоуподчиненныходинначальникауначальникасотниподчинен
ныхноставимтеперьвсторонуктокогобольшевиноватделовтомчтопришлон
амспасатьнашуземлючтогибнетужеземлянашанеотнашествиядвадцатиионп
леменныхязыковаотнассамихчтоужемимозаконногоуправленьяобразовалос
ьдругоеправленьегораздосильнейшеевсякогозаконногоустановилисьсвоиус
ловиявсеоцененоиценыдажеприведенывовсеобщуюизвестностьиникакойп
равительхотябыонбылмудреевсехзаконодателейиправителейневсилахпопра
витьзлакакниограничивайонвдействияхдурныхчиновниковприставленьемв
надзирателидругихчиновниковвсебудетбезуспешнопокуданепочувствовали
знасвсякчтоонтакжекаквэпохувосстаниянародвооружалсяпротиввраговтакд
олженвосстатьпротивнеправдыкакрусскийкаксвязанныйсвамиединокровны
мродствомоднойитоюжекровьюятеперьобращаюськвамяобращаюськтемиз
васктоимеетпонятьекакоенибудьотомчтотакоеблагородствомыслейяпригла
шаювспомнитьдолгкоторыйнавсякомместепредстоитчеловекуяприглашаюр
ассмотретьближесвойдолгиобязанностьземнойсвоейдолжностипотомучтоэ
тоуженамвсемтемнопредставляетсяимыедва

Значення індексів відповідності для відкритого тексту
I0 = 0.0563117
I2 = 0.112577
I3 = 0.16884
I4 = 0.224854
I5 = 0.281848

Значення індексів відповідності для зашифрованого тексту(ключ=”либа”)
I0 = 0.036656
I2 = 0.0838296

I3 = 0.10995
I4 = 0.224854
I5 = 0.18319

Значення індексів відповідності для зашифрованого тексту(ключ=”либ”)
I0 = 0.0388292
I2 = 0.0775677
I3 = 0.16884
I4 = 0.154898
I5 = 0.194346

Значення індексів відповідності для зашифрованого тексту(ключ=”либап”)
I0 = 0.034449
I2 = 0.0688414
I3 = 0.10332
I4 = 0.137696
I5 = 0.281848

Як бачимо значення, який має номер “Ішки”, який дорівнює довжині ключа, збігається з такою ж “Ішкою” у відкритому тексті. Тобто частоти очікувано співпадають.

Для шифротексту варіанту
Ir (r = 0-5)
I0 = 0.0326304
I2 = 0.0651931
I3 = 0.0977066
I4 = 0.130571
I5 = 0.162637

Dr(r=2-30)
D2 = 261
D3 = 241
D4 = 260
D5 = 249
D6 = 240
D7 = 230

D8 = 256
D9 = 253
D10 = 248
D11 = 263
D12 = 264
D13 = 456
D14 = 249
D15 = 267
D16 = 256
D17 = 270
D18 = 236
D19 = 252
D20 = 238
D21 = 278
D22 = 242
D23 = 235
D24 = 271
D25 = 238
D26 = 416
D27 = 235
D28 = 278
D29 = 254
D30 = 237

Перший метод отримання ключа(прирівнювати найчастіші літери у блоці до найчастішої літери у мові)

Результат: громыкавьдума

Другий метод отримання ключа(значення ключа, одержане із використанням функціїM(g)i)

В таблиці наведені значення функції для кожної букви і коджного блоку

	а	б	в	г	д	е	ж	з	и	й	
0	24.7372	21.8302	21.8485	34.539	21.1104	21.252	24.3022	21.3268	21.0492	19.9624	
1	15.5477	15.4301	19.2277	17.3657	15.3745	15.0032	16.8829	19.2396	18.088	15.888	
2	19.003	17.8644	14.8396	15.4682	17.2181	19.9369	18.3057	16.1711	21.1639	23.7919	
3	14.5397	14.7147	17.1903	19.4051	17.7586	15.2514	19.4892	23.9843	22.0409	23.5645	
4	20.8951	19.1729	15.0149	17.4757	19.0056	16.5032	16.2565	14.6575	18.1498	19.6593	
5	16.7841	20.9556	17.5392	14.6405	19.3781	22.9139	20.3832	23.8606	20.8832	22.7018	
6	20.8788	18.8614	15.4657	15.6374	17.6526	20.4536	19.4686	15.5439	20.9488	24.044	
7	21.6176	23.7821	32.4613	21.135	21.1979	23.3545	20.3096	21.1108	19.1083	14.7515	
8	23.4124	20.0002	25.3119	21.1438	21.3012	34.0201	21.3237	20.5207	24.4954	20.5134	
9	20.0123	24.6905	21.9128	21.4422	33.3378	22.047	21.0586	24.7616	20.945	21.3449	
10	21.1456	23.6368	19.7086	14.5709	17.795	19.5122	16.3777	15.1997	14.4447	17.6433	
11	14.7471	14.0053	16.2208	19.1497	16.86	14.3487	20.1132	22.9316	20.6557	24.898	
12	34.4384	21.7985	22.2248	24.6966	21.1821	23.2301	20.183	15.8341	18.5758	20.2306	
	к	л	м	н	о	п	р	с	т	у	ф
0	14.9963	18.2225	20.3796	16.5921	15.2897	15.4702	18.0203	20.9053	14.4251	16.2546	15.6559
1	21.0368	22.1999	21.978	25.1779	21.7859	23.2785	32.2443	21.6492	21.8684	24.0489	19.8426
2	20.0985	25.1562	21.8398	21.1618	34.7083	21.2645	20.8234	25.0521	20.4679	21.3736	20.8251
3	21.8999	22.9705	33.5549	21.8557	20.0623	23.0088	21.6589	21.0281	19.4937	14.8933	17.5818
4	15.2771	16.0341	15.6653	20.1143	18.1578	16.1215	15.4002	16.9869	19.5882	18.3243	15.3144
5	33.346	21.394	20.8663	23.3515	20.5053	23.0888	19.4613	14.3577	18.3115	20.5797	16.133
6	21.2914	23.4237	21.4301	21.477	32.7577	21.8462	19.9371	23.4247	21.3911	22.3768	19.2982
7	18.2216	19.7789	16.2433	16.186	15.9467	18.9595	20.461	15.3947	16.3776	16.675	19.6931
8	22.5086	19.3919	14.7662	17.6595	19.9848	16.002	16.1144	14.6502	17.3906	19.8462	14.6974
9	19.7078	15.4301	18.1903	20.0714	16.1542	15.8392	14.932	17.6884	19.4685	14.7729	15.6726
10	18.8944	14.0452	14.3436	13.971	19.4987	17.7519	14.7717	15.1422	16.4495	21.671	18.7249
11	21.5665	23.1801	34.3223	23.4429	21.4926	24.4278	22.4114	21.7132	19.7316	14.9732	18.3285
12	16.9943	15.8693	16.095	17.9965	20.6262	14.9395	15.6123	15.2734	19.3592	17.612	14.5472
	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
0	20.4212	17.539	14.8899	15.9124	16.1732	20.1725	17.7833	14.9247	20.7077	23.4388	20.8679
1	21.969	19.8887	14.8539	18.9173	19.2746	16.6174	16.9698	14.8488	17.8293	19.8575	15.8161
2	15.4028	17.9618	20.4846	15.8203	16.1833	15.0675	17.9692	20.3384	14.2587	16.0259	13.9534
3	21.0574	17.135	15.566	15.6954	19.1437	20.7873	15.1817	15.6275	15.1122	20.8681	17.8791
4	20.8546	23.3191	20.8165	25.4499	22.3338	22.6083	33.0162	22.4092	20.7953	23.8577	20.7646
5	17.008	14.9394	19.0513	21.2755	14.9757	16.128	15.2039	20.7208	18.8598	15.3484	15.054
6	15.076	18.1268	19.1074	16.3857	15.0958	14.4113	17.6903	20.5623	15.1491	15.1269	15.6597
7	18.317	15.7637	15.1959	17.3491	19.534	17.1421	15.2642	20.7927	22.3785	21.4462	24.0505
8	15.2188	14.8184	20.0446	18.0908	16.5572	15.6139	17.2123	21.9983	18.9863	15.0422	21.3631
9	15.0181	19.4551	18.2708	15.5809	15.98	18.1974	20.0421	18.1727	15.7092	20.7076	23.3861
10	15.3899	21.1607	23.1912	20.6845	26.2369	21.6421	22.8865	35.0037	22.0131	21.1073	25.3851
11	19.7188	16.5624	16.2787	15.1848	19.1387	20.5799	15.2953	15.6021	15.0489	20.003	17.0673
12	15.0332	15.4381	19.4545	17.1172	14.4939	20.0354	21.5974	21.0238	24.1043	21.9308	22.4526

Як бачимо з таблиці значення і-ї букви ключа співпадає з максимальним значенням для букв і-го блоку.

Результат: громыковедьма

Розшифрування тексту варіанту(шифротекст є вище)

старминскаяшколачародеевпифийитравницфакультеттеоретическойипрактическоймаги икафедрамаговпрактиковчастьперваясоциальныйукладбытинравывампирьейобщиныви качтовычтотоимеетепротиввампировраспринкорпорациямифкурсоваяработаадептквивос ьмогокурсавольхиреднойнаучныйруководительмагистрпервойстепениархимагксанперл овдевятьсотдевяностодевятыйгодпобелорскомулетосчислениюгородстарминведениехо рошийсегоднявыдалсяденектеплыйбезветренныйвтораядекадасеноставамесяцанеспешн осочилаьсквозьклепсидрусолнечноголетаиголосазябликовдоносившиесяизпридорожн ыхкустовзвенеливушахяехаласквозьихгнездовыеугодьякаквдольпограничнойполосыпо лосойбыладорогазаброшенныйпроклевывающийсяпыльнойтравойкривойбольшакзябли

кипопеременновозмущалисьвторжениемчеловеканабелойлошадивихчастныевладенияза
лихватскиетрелисменялисьхриплымчириканьемптахисуетливоперепархивалиповеточка
мтревожалиствуразноцветнаякаймавокругчерныхподсыхающихлужвзрывалась сотнями
истомленныхжароймотыльковраскручивалась ввысьвихремтрепещущихкрыльевповодья
завернутыепетлейсвисалипереднейлукияпокачивалась вседлекакмешокскрупойпридер
живаялевойрукойлежавшееналоненяхписьмоипытаясьразобратьпрыгающиепередглазам
ируныромашкапользовалась моимрасслабленнымсостояниемвсезамедляяизамедляяшагн
адеясьчтояувлеченнаячтениемнезамечуеековарногоманевраидамейостановитьсяиспоко
йнопощипатьтравкутычегоэтоголубушкаанушевеликопытамиплутоватаякобылкаразоча
рованновсхрапнуладавайдавайхалтурщицаяустроилась поудобнейесливообщеможноуст
роитьсяпоудобнейнатомпыточномпредметекоимявлялось дляменяжесткоеказенноеседло
натретийденьпутиромашкинагриватоненькимиколечкамиспускалась допереднейлукизаб
иваясьмеждустраницамипухлогописьмакотороеядолжнабылавручитьповелителюдогевы
икотороеужеминутпятькаксамовольновскрылаприпомощимагиинетронувувесистойпеча
тинаверевочкенааломвоскеотчетливопроступалоттискперстнятринадцатьрунипереплета
ющийсясдракономединорогвцентретутмоизанятиялитературойдипломатиейигенеалоги
ейгрубопрервалиоченьгрубоядваупелаподхватитьлисткипоползшиевразныестороныр
омашканеисправимаясаботажницазадумчивожевалауздубряцаяжелезомвтовремякакнез
накомыйивесьмаподозрительныйтипобросшейнаружностидемонстративнопотрясалпер
едлошадиноймордойсамодельнымарбалетомсгрязнойстрелоймногоразовогоиспользова
ниятакчтонепонятнобылокогоонсобираетсяграбитьменяилиромашкуяприподняласьнаст
ременахсинтересомрассматриваязаржавленныйнаконечникянедумаючтоэтосамоеудачно
еместодляторговлиантиквариатомдоверительносообщилаянезнакомцувотвстарминеувас
быегосрукамиоторваливернееотрубилизнаетелитамоченьнелюбятразбойниковромашка
обнюхалаарбалетпрезрительнофыркнулаинапрочьигнорируяграбителяпотянуласькаппе
титнойзеленималинникаизвысокойгущикотороготолькочтовозниклоэточудовлаптяхпрес
тупныйэлементзаметносмутилсянаконечникзатрепеталкакщенячийхвостикувыдораская
нияипокаяниябылоещедалекозаблудшаяовцаупорствовалавогрехесеребролюбияануткаж
ивослезайсконядевкаязыкатаякошелекилижизньдапошустрейслышишьяизобразилаусил
еннуюработумыслиладноубедилкошелекпахнулоозономлицограбителяпередернулосьзр
ачкирасширилисьглазаостекленелиионмедленноопустиварбалетотвязалибеспрекословн
оподалмнетощиймешокболтавшийсяупоясаотмешкаразилокошкамиикуревомослабивве
ревкустягивавшуюгорловинуяпропустиласквозьпальцынесколькомелкихмонетмаловато
дорогоймоймаловатосленцойработаешьбезогонькавпрочемтакужибытьвозьмувкачестве
авансаосчастливилаяграбителяшвыряяемуподногипустоймешокипредупредилаячерезпа
руднейэтойжедорогойназадпоедутакужбудьдобрпостарайсяменянеразочароватьмужикн
еотрываяотменязагипнотизированноговзглядамедленнонагнулсяподнялмешокизастылс
толбстолбомневсилахшевельнутьсябезмоеговедомакактолькогореграбительскрылсяизв
идуядеактивировалазаклинаниеипозволиларомашкеперейтисгалопаналюбимуюеютрус
цуписьмозажатоевовремяподсчетаденегуменямеждуколеняминемногопомялосьиутрати
лотоварныйвидвпрочемрассудилаяглавноенеоформлениеасодержаниеоноежекомпенсир
овалонедостаткирепейноголистаиспользованноговукромномместеагавотнаконециобомн
епарастрокзадифирамбамизагадочномуарракктурупропустишьинезаметишьзавремяобу
чениявысшейшколечародеевпифийитравницадептквольхапроявиласебязнаюоченьпло

хонеусидчиванетерпеливасвоевольназнакомаяпеснялюбитзлыешуткиинеоднократнопер
еноситихсвоспитанниковнавоспитателейэтоонпроведрочтолидабылоодноведеркодоволь
ноообъемистоестоялосебенабалкенаддверьюмоейкомнатыэдакийсамодельныйкапканнас
оседейпошкольномуобщежитиюдабынеповаднобылобезспросуодалживатьуменяконспе
ктыикастрюлиснавареннымнанеделюборщомможетучительтакбынеразозлилсяеслибыве
дровсетакиопрокинулосьанеупалоемунаголовустоймявместесводойотличаетсяредкимис
пособностямикпрактическойитеоретическоймагиисильноразвитойинтуициейбыстроада
птируетсякнестандартнойситуациихаможетяещенебезнадежнанеприличнаякакаятогран
ицаудогевыуэльфоввысокиетравыугномовскалыувадлаковгрудывыброшеннойнаповерх
ностьземлиудриаддубыподметающиеоблакаудруидовкаменныекругиулюдейоблупленн
ыестеныканалысзатхлойводойразделенныепаройтройкойподъемныхмостовдалысыестр
ажникипринихбдительнодремлющиеупираясьнаржавыеалебардыаздесьосиныиздевател
ьствокакоетоособенноеслиучестьчтожителидогевывампирыхорошиетакиеосинысеребр
истыетрепещущиезаосинамищекочетнебоостроверхийеловыйковерсредикоторогокоегд
епроглядываютзатравленныеберезкиисосенкисамажедогевалежитвдолинекакплюшкана
днерасписнойпиалыеслисмотретьсхолмакраяпиалывиденбелыйободокизосинворойпот
олщепотемнееизелейавцентреширокоезеленоедноскрапочкамисамадогевавкольцевозде
ланныхполейиоблакахтуманаподойдешьвплотнуюкдеревьямнаставлялменяучительипо
шлешьмысленныйсигналвглубьлесалюбойможешьдуматьочемугоднолишьбысформиро
ватьмощнуютелепатическуюволнуакомумнееенаправитьнаобщейчастотектонибудьизст
ражейграницыуслышитясмущеннокашлянулалучшебыемуэтогонеслышатьнеобязательн
опродумыватьочереднуюпакостьзнаюзнаютынанихсверхвсякоймерыгоразданонасейраз
постарайсявоздержатьсяотоныхочемэтояхдаоволневампирыоченьвосприимчивыктеле
патииисразуотреагируютнаееприсутствиехотяинесмогутдоскональнорасшифроватьтакч
тонапирайнаколичествоаненакачествоваттакясмотрюнадымящуюбанюнаморщивлоботу
сердияинамоюволнутутжереагируютпятьилишестьадептовкоторыеовеянныепаромвыбе
гаютиздверейивыпрыгиваютизоконатакованныевнезапноожившимивеникамирукибуду
щихколлегзанятышайкамиприкрывающимиотвениковсамоесокровенноеучительусмиря
етвеникиоднимдвижениембровиновзгляды

Висновок

Засвоїли методи частотного криптоаналізу. Здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.
Лаба цікава, як і остання, але більш легка.