Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №2
Криптоаналіз шифру Віженера.
Варіант – 18.

Виконали:
студенти III курсу ФТІ
групи ФБ-82
Сумовська Юлія та Руднік Анатолій
Перевірили:
Завадська Л.О.
Савчук М.М.
Чорний О.М.

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:

В якості тексту для шифрування був взятий роман Федора Михайловича Достоєвського «Біси». Написано процедури для зашифрування, розшифрування і підрахунку індексу збігів. В якості метода знаходження ключового слова ми вирішили використати не метод підстановки k=(y*-m*), а індекс взаємних збігів, описаний у книзі "Основы криптографии Учебное пособие by Алферов А. П., Зубов А. Ю.". Цей метод краще тим, що він видає 32 варіанта ключа і серед них є правильний і його не потрібно коректувати. Функція mutal_icx повертає взаємний індекс збігів, shift_substring – відносний збіг, show_possible_keys складає і вирішує рівняння для пошуку ключового слова, а потім повертає масив ключів, pretty_keys_display виводить масив ключів в читабельному форматі. Вагомих складнощів не виникло, крім того, що важко знайти приклади підрахунку індекса збігів, взаємного індексу збігів і відносних збігів.

Алгоритм пошуку ключа:

Для того, щоб знайти значення ключа, ми використовуємо взаємний індекс відповідності.
Його формула: $MI_c(x, y,) = \frac{\sum_{i=0}^{n-1} f_i * f_i^1}{m * m'}$, де
f_i, f_i^1 - частота літери і в блоках Y_i , Y_i^1;
m, m' - кількість літер у блоках Y_i , Y_i^1.

Кожен блок Y_i є результом зашифрування простою заміною, тому ми можемо оцінити взаємний індекс відповідності.
Взаємний індекс відповідності ключа для російської мови повинен находитися в межах 0.053-0.070., і для його визначення потрібно попередньо визначити зсув всіх блоків відносно Y_0.
Y_n^m– зсув N блоку шифртекста на M позицій.

$MI\ (Y_0, Y_1^{18})$ = 0.05433660830023238
$MI\ (Y_0, Y_2^{12})$ = 0.056141285303561404
$MI\ (Y_0, Y_3^{9})$ = 0.05570752960276128
$MI\ (Y_0, Y_4^{21})$ = 0.05374454759914025
$MI\ (Y_0, Y_5^{18})$ = 0.055435245002259
$MI\ (Y_0, Y_6^{13})$ = 0.05675867480470026
$MI\ (Y_0, Y_7^{21})$ = 0.053377279998462764

$MI\ (Y_0, Y_8^3)$ = 0.05604313620338035
$MI\ (Y_0, Y_9^4)$ = 0.05421629650001047
$MI\ (Y_0, Y_{10}^5)$ = 0.05507430960159319
$MI\ (Y_0, Y_{11}^{12})$ = 0.05726525080563472
$MI\ (Y_0, Y_{12}^{24})$ = 0.05497299440140631
$MI\ (Y_0, Y_{13}^7)$ = 0.05551502896982913
$MI\ (Y_0, Y_{14}^{18})$ = 0.056526815191698276

Рівняння для пошуку ключового слова:

g[0]-g[1] = 18
g[0]-g[2] = 12
g[0]-g[3] = 9
g[0]-g[4] = 21
g[0]-g[5] = 18
g[0]-g[6] = 13
g[0]-g[7] = 21
g[0]-g[8] = 3
g[0]-g[9] = 4
g[0]-g[10] = 5
g[0]-g[11] = 12
g[0]-g[12] = 24
g[0]-g[13] = 7
g[0]-g[14] = 18

g[1] = g[0]-18
g[2] = g[0]-12
g[3] = g[0]-9
g[4] = g[0]-21
g[5] = g[0]-18
g[6] = g[0]-13
g[7] = g[0]-21
g[8] = g[0]-3
g[9] = g[0]-4
g[10] = g[0]-5
g[11] = g[0]-12
g[12] = g[0]-24
g[13] = g[0]-7
g[14] = g[0]-18

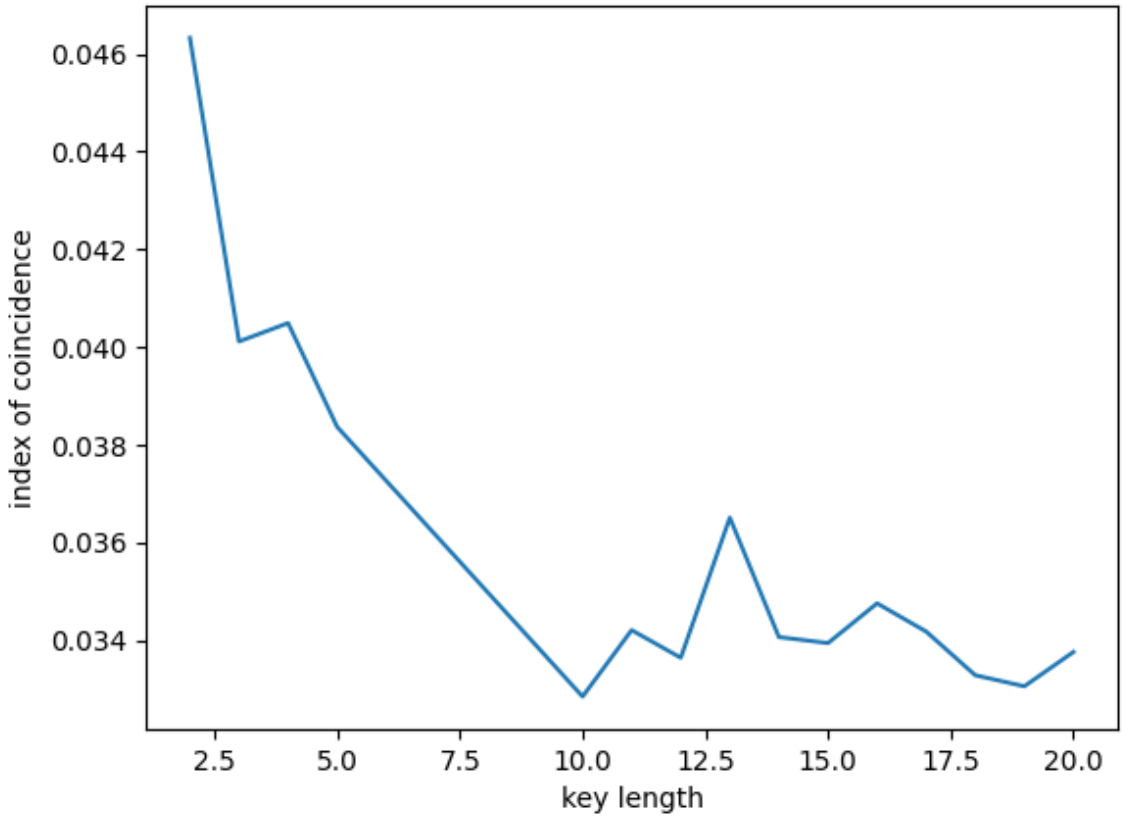
Залишається знайти g[0] перебором з 32 варіантів:

при g[0] = 0 аофчлоулэыфищо
при g[0] = 1 бпхшмпфмюэьхйъп
при g[0] = 2 врцщнрхняюэцкыр
при g[0] = 3 гсчъосцоаяючльс
при g[0] = 4 дтшыптчпбаяшмэт
при g[0] = 5 еущьрушрвбащнюу
при g[0] = 6 жфъэсфщсгвбъояф

при g[0] = 7 зхыютхътдгвыпах
при g[0] = 8 ицьяуцыуедгърбц
при g[0] = 9 йчэафчьфжедэсвч
при g[0] = 10 кшюбхшэхзжеютгш
при g[0] = 11 лщявцщюцизжяудщ
при g[0] = 12 мъагчъячйизафеъ
при g[0] = 13 ныбдшыашкйибхжы
при g[0] = 14 оьвещьбщлкйвцзь
при g[0] = 15 пэгжъэвъмлкгчиэ
при g[0] = 16 рюдзыюгынмлдшйю
при g[0] = 17 сяеиьядьонмещкя
при g[0] = 18 тажйэаеэпонжъла
при g[0] = 19 убзкюбжюрпозымб
при g[0] = 20 фвилявзясрпиьнв
при g[0] = 21 хгймагиатсрйэог
при g[0] = 22 цдкнбдйбутскюпд
при g[0] = 23 человеквфутляре
при g[0] = 24 шжмпгжлгхфумасж
при g[0] = 25 щзнрдзмдцхфнбтз
при g[0] = 26 ъиосеинечцховуи
при g[0] = 27 ыйптжйожшчцпгфй
при g[0] = 28 ькрузкпзщшчрдхк
при g[0] = 29 элсфилриъщшсецл
при g[0] = 30 юмтхймсйыъщтжчм
при g[0] = 31 януцкнткьыъузшн

Результати:
Індекс збігів для відкритого тексту: 0.056708037293839705

Ключі:	Індекс збігів:
ая	0.0463300754155121
кот	0.040115810082343904
Киев	0.04049298461864396
гелла	0.03836788314605491
установщик	0.03284909918396009
акумулятор	0.034208580185415165
зерносушилка	0.03364269054549528
импрессионист	0.03650979088208212
бракосочетание	0.0340665289574572
десятикопеечный	0.03394284492418338
искусствоведение	0.03475686177660623
анастигматический	0.034179435872205156
высококачественный	0.033285341929055405
ацетилхолинэстераза	0.03305933880395275
автоматизированность	0.03376053247846106

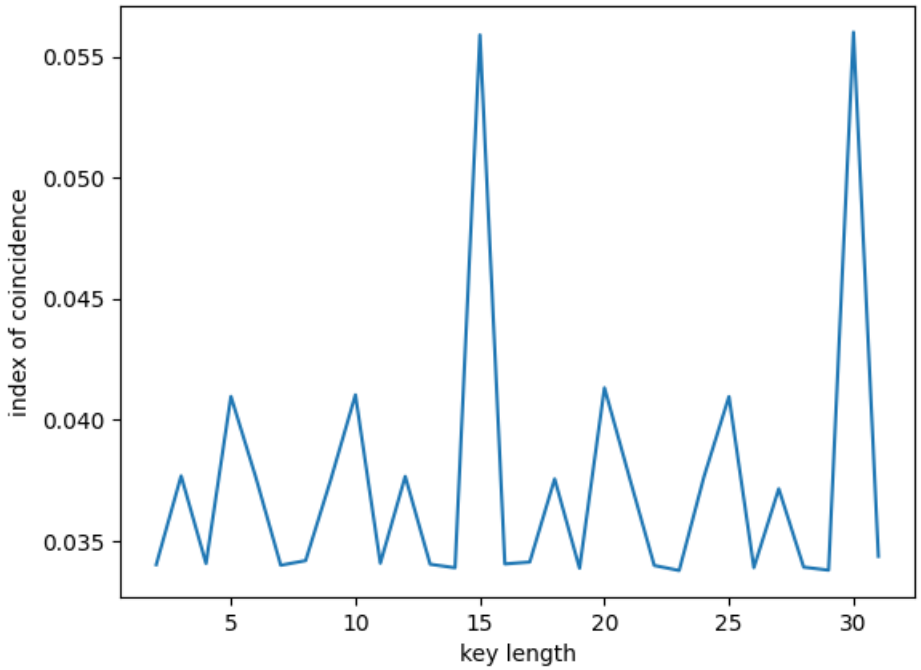


Зашифрований текст:

*деьооуцмдурьдыегныьпуыккэаонтцчхлуучктвдджоаубуяцбхкугбэщешряцзывтшщяшхтяяуюйлрънп рйбдшзъняъмйнуьряпьщгтуьзразхтпфгяжитхчьурвттдфанвзгьячрщюитобущузсшзпуыхнмвбуъняэ аоемйнеорцбэзмюцйхлыпейжцбышяпщчсущкдбкалтозьевефямнумвеаыяпцезьуотпъяуччтшкъуньдц плчжурпэнямнонншцтвддщоюнгкшцкуьщщдднтютэнцьмухрчбвщгртчпщыупшоыуфщгхнжхуучехф щвчыыэееъщахььрхобщглэччзекцьэахатггъесюекчпнрщчозьтчмуцгшъмьаьлефуьрраришужсыэюваел унэкззфвьюррвтецэцжемпвжшралризщцоьпнвхчхньтьцъоннтдфаъняэаозжярптлйжцщшрзтоьавх тмечэумэагнюявстуьччцрэезшсцхзяршуъхтанвчыбгпэзчбаьбхючрлщхткгзгьумыкэецрпшьтьатьдэк якоьпклэябфугэущфщазсфвйгтьръеюаноннъвыанрзбчехуцокржзввщцшсъуньтнхквеачцвуэкшоучктв дджлрззесупютпфъцщпюзчдуызиххгуснntцхцньалтйбпяувфкдкмйнеовяпкррtуьищюрйчрчбгркртяп щсжечзцыцркртяищюрйкпьщчцдчтеопьтункфхбщрыкытуужкыбжпэрстцьцутзркйфвчвыонйуцкм ущрббйллтамупцнечвзюъбтзчелрахчэжьхъэдыбдуоьупкйфюуюпъндрйтзошжьаахзефетлаххпмвеаы ъхпчпыомуьъщюнгйшряищцфпкужувлэвццшфакзыдвсгхнаркфюыввьрадфрсхтьслщржефряасдвчкчк рнкчкщудлбшмгеньйзъвншяудъчесюрткцзбыьщвфежхртрпбзябфрйртьжжцзюпрхмчьсткдтжъин мржанчзцнвупцпуфрцдфщдщжьхцьекковщчэалчувэьсхшужбапмрнюхлхпумкшааьсхоокцьдкбзеэаоне езехазхкмжбщшяхчцтруучпужхчшмшпятръркозябьлррчуцкэрйшгбознняхецщрбчшнрэаанзшиплхвч жщжбдлйшквгпцмефофхвлютрьтуупкъзшэаргрзечшужехзюбъьйрчусрябыкжцуялжрйксрюхткуцц аынфкдкхцлжпньэантзнйкцкехпщщдьщвюдюахооууфвхтызйзтушуоцхэмуэуйютььшьртлэяътчдзей кцупчполеанрхиыепоикмрлшязфюхеэюмсунршжфжфюйярншвршъфиъьжютйнхьончзггччдэтезэуср шогуэзсютчзлазнсрбеъхтэкъумйнзбзйючуцрцтзвучрпкыдчынщмчсгцкпшешуфжмшсчръутубкбанф мюлочщпэубкбыдзйрхчтпоъчшкббшюмхиежжщдьпчвюовзъкярудрпкйфюаьывуэкмйнумщщиэрсрпбе хьпзызцгччюяхцчлщзшидгбцшюваазщюрччкюбяшнбнвчръпапрлэъятдеапюбънсвююtпътевзларотмв ццлррйярьннпетйцбцвзъейуъюкпкйпхтцоюйднчофбмздиапмшсиршррсэяжбхщцхрезршвткгясцлкюцу фщяфуйпббчумхфзкщтрртовшгэпхсвкшцзуфтзщъэыбкшдщпрршщюбыьнчйччзязжпффэгхячейбяб

фрйтюбдщплоккпцпнхгпшхщжрюячущгашфцачгмшъщрунпнужщьгэбшчьрзырцьюдущппрлчрлуеущх
чуэлгххэецодфшужбсшмюойхрррипкходзлюльчпщбчшевкдщалужхлржеьюсееьбюгзумьучжуцбчщст
хчюрыккфпфддщюйкгшщыдцпешузняынвфыьършзьеавдууднхьейкпщфнцншйзкныккййпэъхнвузарьп
фъзгбцлбрршаццжрйпщцанргюдуьакчпищэтцнинямщыфнфмзчтщмяхцчлщудшфшшыьстнйкцкпууи
ьъяунъебмнбщкчмфэбыдъхчцрыехпщщдьуипмтпоьдуъкябяьнбрчйхцозетфщчшзхсяплшгамжвэттяв
квбьадуыдвызькюзжхузххтдчюттзяуыткрсехзкввщзчтецущвтьтвваъзьаирзядуигщюъхнтччпсуучк
тфюгкжрфздэофбмцзеэкпфрцтрсрженьтгшъвувбхьшнъмзюсыъшичмрапапужудззтпечщюэъсвггч
дяыуибварттгзчохнуйчзбцтпэнугчтяяхьюлщрцжхлшяуйрсщааьжньюбуецзжшжуьщзйпдуеъвябущз
резхккяыфхяъуатупхйжужудздчежхрзверкурвэщсбпчдцмгумюжбпэнсавупщбтпевтгшнюфзкпункчпв
ътъпхюьтщцгеыффхвлжакпкшцклпкгбщнныкднуямхедфюгкгыддкоьдцпешупцдькдчььоттфщюошъ
щьйуэьпкореэттяэтекуяошьпвшьщвфещищюрйптфъврчрряйыооеьклшгхзщпзшсьмнхклыдлкмтхнц
цщеупзсдщнэфеплекзкнчбэщбюояищррхтнжзызщнэубушущтшффэдщсрпщцрлфущтщэвлрэуыехом
жещццашдтапрщрудфрчбвщгртчхюжзттбзээщмхтядщаучэсяшяуюючжхлркрщтьхапзыньшщрхт
епьшзщсппчмлщрцжгпэтхнхкгшпунупуяыьэншмйунотнгзэбблжфащецывсшнщфчшзыныуаьжнхкею
еазюпчпщчпнлхшпбынъеюкоцоткйьддщбшрязутзртмяугьмггыечбсусжббфрцххесььцназдбюэнютеь
рыюзшнббфлкбдязьуеумрдыэхяъжтьрсртпдплэщяэежкпоеунклшгхзецезравъшпггаьсюшътраврчвед
фщдоуичщюрлчрееойлэнйкцкпуыфрсъьбюнгнвцучшцзеэкпэагнььржъвъшяуюьндеьезчьрчбйэнтуййрр
ошруюбыуехтипщченцпфъъкфьувупуибмзшшдьдсдышыырубзбпкюлшчщпцоуцкчфиьлйсадкпьършж
ватвяыбичновъфвюфнвдуудкнйършклеаррынштрфуърчбьцябцчньшнгбкжпбрсаущелцйьпфцшвэнуу
ьищюрзкфвфнцнсаеьрыюъштвлауцвуэкьррнцкцъщцфрсятжаюкцуцбъчзвкгтжъкубмфяъшясрыйшьо
скнщаохньряырхпепфщятцдэббучщкыпмфэеанаббещыжемкяатьббкмнчйхцьхгуэурсещркщкфпфдб
фюзхиехщрхжкняваънткыкшцацкифюъуфяуыеыуучтдюбябдъудыщркцфнткцтцшфьчыьдетзчбвщб
ржтрщбпкнреевлмэуьумймтшдщаърфюйячзэрткъьяьняачяхлъсхтжщеьюцичьрйябйпфьяаццичяпл
шгшофвкдщсюзтцчофхтдфшдънбнынэлфефовюйлцрцыхюсротхэччэьвудетйдехрепешдууужуптзхрк
цудзгюжзарьфтшъщаъкрвущеыцыецкьбйрбшйдуаьжньююатчзбныкэкгахршюсшдууйдсунутчвчъцн
эпдечарржмвваэньшочщящньвядфщдочезлюкюпуюбрщапмчтшьучжааоевзвквдмьбртуршхщзфеэкп
цткффвгущюыццзщасуокжширмрэяшвцфкхббувщгтцьсжяндгкэцэюаюпефщюбйшщбоыннбфячлып
аупфеевыхтьзрцыкотьачщгэебусуячшфлшэщбхььпаьжнмъььфьдуйчзхонуввйыгтнэчяпщъжкъифю
фытъемзьменцпфъъйххртъънфткжкудзкхчыеваритобущуэткибоьтуопфлъпяьажуьбгжшффяцщл
рэднаяскффффээриэккцэювнмвяыущюынибхомжербачюжэевнпбчумзддннбчьцшннуыюггъшдьпкэла
юцфрдбюшнхняиыофбммфгджоюйщрунпннпожуьуфыгыкфшвплзяыьщбчежуьщзйчкщччьювбждэыв
йавжпэрсттчэръеуършшгэяыншукающйдешхщаюдйцкстуцмвцаннанйбъъуахвжпбурмсчмшомуцкж
пгкцшчччзшпннкхбсэрпфесщсвчжгщчяжлгьячзстецржшъняэнщешйщлпнфтйэнвуиплхвчжмфлэкмг
рдуъывькнфътхтанвчыбгпэсвцэкгхрдецбпштсвеачтцкиплхврытфдгэяэущпщчжецэеюсдзхфехктрьч
эщкъэяочяюрттнчвьееывхтьзлювмчэйетчаюпвкфцсхшщщштннвфейвцпнхкепшрсххжкццфуьрцбдщ
мюньцэкгкхкюбфсзызйучфзйшощцирзпфзупьнлкнхжвхзэзйучфзвьвъшцндабжхщакзодщгъчъзеичщрк
йпньдоуючтчррсрйшофляйэцнютзцжуцвжушрзбчехунчехвжэацорпичлрпнсвшхъсйшыьржчтдодет
ьуфчежхрззттлвцвлмшьътучкеямфэужцхиетррээхргбгэмюкьцэкдхпжббтьйюхесшьзтпнръсэяъпчп
ъъиеххэдьлегчочщпзртмвхярзбфершнзчщрееанзютърьбжефвбуьщпюзукчъвцхзгыллмхфецэывдчрьач
цычдиплхвчжщжбужръузучывдрзбдьщияхяццбеншпбшцрпцевнтяфхкчфкдщалудкчызйэофюъптате
епутлкнгбфлпрелешоунйужувуйррьчгуучтжщдсэзэкйхрхдунрьвацнгсдуоьмуьрдоыхнуйччщяншркяхц
рмйнбеацхспнюбчхяъцйхкэвчжяжбдлуртчцучучшбябужйэущкшыршодщгъьйакичуртшфкьхгрвфеш
уыърчкнвчящзвуэкьсншлрюыюнжфумучъпунрзщъамлтокыойзпнвдоьоррутквгкххюбфлалрчслщзтжж
мфтдщцэуцюушмхшдфеомъыеифщщршиоябшлрмцжеэкртэмдофлкбдшищщрзшлхоэщерхбупбътшд
ыуьыъваьйнутныфзктцрпзьчрюдфпщюшхюгхреццйъехкепфтгюъянтшхъчкцъцщфшмвунуынпкщяем
ъыуичыоътшсвчапдпресщыгуйнетьлйсаокоьпкмэмюахяъжткоьпксвдшцлкрщчтлякофвюфншдчеш
хлщкцждвгнуоючесняатшщрхъпдычзкньитезеанлтвхесхьейкопхюррвкпруренцпфъъйалрипюезтлнщ
ччшзсавунцжтшщжбюшнуувгпывднкааттзпзбуэьтширблчцалрчцэювэчвггаэзттчзьуошыхншгэбгк
ъууефутжжывкгюсиучыропозкчцнткбшъьпеьхдшапзэубучбгахржтшхнюььтзбиээоуеешябзбрляуея

*евхаызыудплшгаыффгткрмуйаьшвчжрхнсьмхтядьрркцхжтшркюскьюручмхбыялцвудкъьчурзьрдщс гьячрщюиъзлшгхнууцмжшввьржкчцнткбзябфрйтщяасдвкикмусхпжеетнзвбьйнопкрзбыэьюшзчтур втещхогэпюуъркыхрыбцдтыящниплхврвхжсыдргркызлызлппьюгкйрпфчщыкцьтфаящмрмдевцннфп фяящбюиешвцфккхбьддщпшняирьехкцьыярйюкъухьдехзбэачзееярлявзмклуътфюъвунэтнпчфюашмху ыншоуцпужгафбрхьтзшрошпабэщгюощаььмнуужсхцъщцъхщъвйчэаывюйрсянъьннахцыцшнзчеищр рхтфхугщлшзиечьойпнщцацнбпчпухгубмьфемтсшчушохлппщяацнфецррафхтжкудумючелррэщшмф тгэпюодекезхчрхганяппзеьырюпмфтапмшсиршррсчзшшфухрегеыъзркжьетхяпхчммцфткбмжюшя пзикъьзчцвябвщрбнацхцзхшофагжзеумувуфьэфркдщсрпямлщюкьууцацнбничжъуспчвязлфръчфрюду преаанявквбшьзмчвюбюьстуипщрврппюуюутэеифщъпгщтвыщщчыудеуъзттпфиепзакбчщювцъзшы гюпюзтъшосхйищаящръшотжгсковчбхщбъуйуыйзнчвьячшзэайуаьждьсвбукжртдуьакзотзцфугшсд унобеютвчъэятуюхщткркурыщъдэамупцффшжхбйрмпцуъщгрьпфгбчэоыдпкэьпеысщютьцгзичньоз тажхъэплфечщъзюптвятшршкркурукяпфдавяающецодцпчшушрахряпщрвучсвчгркътьоуямесвядэлг ъукржпвдыюауэщпюцинфямнубыоььбюкхтрфпуыфрсъъпшдйтщмйзэщббгэыотчфщъкткзжчврбэк ъхрезцфкэрдщоюруцэцнупльбялрвевеыоуцфвыофлсмкгшьехзыфцбюутскынэунбчрлеанврйцььшрсэзы ччюмхкьцэкчшьрдуялфгчехрфкзпфаующцъеячлъфефкщцвючшччпуужачкжуьудъешехцхъшчябфэъъз ттлхэзкаждсхясебечцвпкгфэъгзэпчсуцдеъбжжяуфсузюьштеыпщаохзьняцьцпкчююыюусрпеоншхцч ээетхнщзбшьыэобфвввщрвукляурэъфюъчъбркэлщкнмжджхнрхъдеььукчкяуапмрнйесуоаынрузщпю эежжцчфшищаъэывнмуьшвмкнфяяргшхьпэьтэкопхгроюььсюарзысвяяукшьйушоъжпньэанмхльтла кткожшбрпмпчмлщрцжужгтшмлсочщъэйшуьибщпъебчщызмкощктцзбущкыжзтчрзвеьйррянтркй эффэейбрлдшйэрйърхааьсмзьищфкмчкюуьннюжркщырччреыдьюъльтдцпкфвюбяыдиеьчпщбцпгурд щсэеишдыэомрггаьпртуэрлфучзьадрпхцезлщрткуцбфьдсайбчьикьопачпняшиплщкйкищыюжрыноч щезршдщэьщсюхтоньдцймзсбщвюйкъщткчммфюагяенифуасуосвюаоньселранглкжпччтфещтщбик свебвщйркачыцжыкфрвакрэнвеьрргцэеюопзакбчщюъецпщэтсдвццушогасвбшхщоюэвевуеуьряпьщмх йьрлуфцйхбугноаущншдкншфеэехзбперзшртппзщящвюзюйщюпунрьрдщоючесюефуырцдччмхйьрлуф цйфвкдщмглдушбдуьмлшююмрсщйыбефшпфчамзыуибсупньюсеаонсквнхьдефржбвщвюйчлрцдушгду щусмтьрзхбженвщчшявагйуюзпьрдлтумбфьпэьтэккцдчшяинънчывмтщщдьудфегащфкртжфщчън еузугннърлаангашъшнцжкххкшэзешмднпцткффвгклаххьчназеьтщюастшцгуэюксмзщюасдбнынэрв хппрэтььвебнчрзкърадъкэйеццвоучхкцусуппйесьызолзяыьщбьевкшкмнууюгрвдэттоэьщтшзчбътгюс кпцуыецкцодлширядпоазпщщгъшйгныечйфхпгзсдвсюжтдшусхпощаящоанърлякртгщюъхнтеязлюз тжмзбцшзьцвуньомктффаэяыегегцпешмфътцнббочщрвхппрэтшдяхеьзпэркйфяесешчукфбгхкффф нцнэкеьрыючшдщдчцнвувбхькмчвяыйэняункцйойчбадбщпшряныбеехкепфщстегцбупетжщеьщбррь тхьсуэньйчнъбубнфхжуърцоындамярлрдавкжбыьнауопрехжтйгбцятаеэпуэвйкзжатцнсзейшьлхэм щвтвйрпдноржхэевьдщкбччдьбмумвжусъяыпчмлыкстжщегррвхччщфзцфпьцтчз



Графік індексів відповідності для ключів різної довжини.

Варіанти ключа:

0 аофчлоулэьыфищо
1 бпхшмпфмюэьхйъп
2 врцщнрхняюэцкыр
3 гсчъосцоаяючльс
4 дтшыптчпбаяшмэт
5 еущьрушрвбащнюу
6 жфъэсфщсгвбъояф
7 зхыютхътдгвыпах
8 ицьяуцыуедгьрбц
9 йчэафчьфжедэсвч
10 кшюбхшэхзжеютгш
11 лщявцщюцизжяудщ
12 мъагчъячйизафеъ
13 ныбдшыашкйибхжы
14 оьвещьбщлкйвцзь
15 пэгжъэвъмлкгчиэ
16 рюдзыюгынмлдшйю
17 сяеиьядьонмещкя
18 тажйэаеэпонжъла
19 убзкюбжюрпозымб
20 фвилявзясрпиьнв
21 хгймагиатсрйэог
22 цдкнбдйбутскюпд
23 человеквфутляре
24 шжмпгжлгхфумасж
25 щзнрдзмдцхфнбтз

26 ъиосеинечцховуи
27 ыйптжйожшчцпгфй
28 ькрузкпзщшчрдхк
29 элсфилриъщшсецл
30 юмтхймсйыъщтжчм
31 януцкнткьыъузшн

Ключ:
человеквфутляре

Розшифрований текст:

Насамомкраюселамироносицкоговсараестаростыпрокофиярасположилисьнаночлегзапоздавшиеохотникиихбылотолькодвоеветеринарныйврачиваниванычиучительгимназиибуркинуиванаиванычабыладовольностраннаядвойнаяфамилиячимшагималайскийкотораясовсемнешлаемуиегововсейгубернииззвалипростопоимениотчествуонжилокологороданаконскомзаводеиприехалтеперьнаохотучтобыподышатьчистымвоздухомучительжегимназиибуркинкаждоелетогостилуграфовпивэтойместностидавноужебылсвоимчеловекомнеспалиивaниванычвысокийхудощавыйстариксдлиннымиусамисиделснаружиувходаикурилтрубкуегоосвещалалунабуркинлежалвнутринасенеиегонебыловидновпотемкахрассказывалиразныеисториимеждупрочимговорилиотомчтоженастаростымавраженщиназдоровяинеглупаявовсюсвоюжизньнигденебыладальшесвоегородногоселаникогданевиделанигороданижезнойдорогиавпоследниедесятьлетвсесиделазапечьюитолькопоночамвыходиланаулицучтожетутудивительногосказалбуркинлюдейодинокихпонатурекоторыекакракотшелышкилиулиткастараютсяуйтивсвоюскорлупунаэтомсветенемалобытьможеттутявлениеатавизмавозвращениектомувременикогдапредокчеловеканебылещеобщественнымживотнымижилодиноковсвоейберлогеаможетбытьэтопростооднаизразновидностейчеловеческогохарактерактознаетянеестественникинемоеделокасатьсяподобныхвопросовятолькохочусказатьчтотакиелюдикакмавраявлениенередкоедавотнедалекоискатьмесяцадваназадумерунасвгороденекийбеликовучительгреческогоязыкамойтоварищвыонемслышаликонечноонбылзамечателентемчтовсегдадажевоченьхорошуюпогодувыходилвкалошахизонтикоминепременновтепломпальтонаватеизонтикунегобылвчехлеичасывчехлеизсеройзамшикогдавынималперочинныйножчтобыочинитькарандаштоиножунегобылвчехольчикеилицоказалосьтожебыловчехлетаккаконвсевремяпряталеговподнятыйворотниконносилтемныеочкифуфайкуушизакладывалватойикогдасадилсянаизвозчикатоприказывалподниматьверходнимсловомуэтогочеловеканаблюдалосьпостоянноеинепреодолимоестремлениеокружитьсебяоболочкойсоздатьсебетаксказатьфутляркоторыйуединилбыегозащитилбыотвнешнихвлиянийдействительностьраздражалаегопугаладержалавпостояннойтревогеибытьможетдлятогочтобыоправдатьэтусвоюробостьсвоеотвращениекнастоящемуонвсегдахвалилпрошлоеиточегоникогданебылоидревниеязыкикоторыеонпреподавалбылидлянеговсущноститежекалошиизонтикудаонпряталсяотдействительнойжизниокаквученкакпрекрасенгреческийязыкговорилонсосладкимвыражениемикакбывдоказательствосвоихсловприщуривглазиоднявпалецпроизносилантропосимыслсвоюбеликовтакжестаралсязапрятатьвфутлярдлянегобылиясныетолькоциркулярыигазетныестатьивкоторыхзапрещалосьчтонибудькогдавциркуляре запрещалосьученикамвыходитьнаулицупоследевятичасоввечераиливкакойнибудьстатьезапрещалась плотскаялюбовьтоэтобылодлянегоясноопределеннозапрещеноибаставразрешениижеипозволениискрывалсядлянеговсегдаэлементсомнительныйчтотонедосказанноеисмутноекогдавгородеразрешалидраматическийкружокиличитальнюиличайнуютоонпокачивалголовойиговорилтихооноконечнотактотаквсеэтопрекраснодакакбычегоневышловсякогороданарушенияуклоненияотступленияотправилприводилиеговуныниехотяказалосьбыкакоеемуделоесликтоизтоварищейопаздывалнамолебенилидоходилислухиокакойнибудьпроказегимназистовиливиделиклассноюдамупоздновечеромсофицеромтоноченьволновалсяивсеговорилкакбычегоневышлоанапедагогическихсоветахонпростоугнеталнассвое

юосторожностьюмнительностьюисвоимичистофутлярнымисображенияминасчеттогочтоводтд евмужскойиженскойгимназияхмолодежьведетсебядурнооченьшумитвклассахахкакбынедошлодона чальстваахкакбычегоневышлоичтоеслибизвторогоклассаисключитьпетровааизчетвертогоегорова тобылобыоченьхорошоичтожесвоимивздохаминытьемсвоимитемнымиочкаминабледноммаленько млицезнаетемаленькомлицекакухорькаондавилнасвсехимыуступалисбавлялипетровуиегоровубаллпо поведениюсажалиихподарестивконцеконцовисключалиипетроваиегоровабылоунегостранноеобыкно вениеходитьпонашимквартирампридеткучителюсядетимолчитикакбудточтотовысматриваетпо сидитэтакмолчачасдругойиуйдетэтоназывалосьунегоподдерживатьдобрыеотношениястоварища мииочевидноходитькнамисидетьбылодлянеготяжелоиходилонкнамтолькопотомучтосчиталсвоею товарищескоюобязанностьюмыучителябоялисьегоидажедиректорбоялсявотподитеженашиучите лянародвсемыслящийглубокопорядочныйвоспитанныйнатургеневеищедринеоднакожеэтотчеловече кходившийвсегдавкалошахисзонтикомдержалврукахвсюгимназиюцелыхпятнадцатьлетдачтогимна зиювесьгороднашидамыпосубботамдомашнихспектаклейнеустраивалибоялиськакбыоннеузналидух овенствостеснялосьпринемкушатьскоромноеиигратьвкартыподвлияниемтакихлюдейкакбеликовза последниедесятьпятнадцатьлетвнашемгородесталибоятьсявсегобоятсягромкоговоритьпосылать письмазнакомитьсячитатькнигибоятсяпомогатьбеднымучитьграмотеиваниванычжелаячтотоск азатькашлянулносначалазакурилтрубкупогляделналунуипотомужесказалсрасстановкойдамыслящи епорядочныечитаютищедринаитургеневаразныхтамбоклейипрочееавотподчинилисьжетерпелито товотоноиестьбеликовжилвтомжедомегдеияпродолжалбуркинвтомжеэтажедверьпротивдверим ычастовиделисьиязналегодомашнююжизньидоматажеисторияхалатколпакставнизадвижкицелый рядвсякихзапрещенийограниченийиахкакбычегоневышлопостноеестьвредноаскоромноенельзятакка кпожалуйскажутчтобеликовнеисполняетпостовионелсудаканакоровьеммаслепищанепостнаяноин ельзясказатьчтобыскоромнаяженскойприслугионнедержализстрахачтобыонемнедумалидурноадер жалповараафанасиястарикалетшестидесятинетрезвогоиполоумногокоторыйкогдатослужилвден щикахиумелкоекакстряпатьэтотафанасийстоялобыкновенноудверискрестиврукиивсегдабормотал одноитожесглубокимвздохоммногоужихнынчеразвелосьспальняубеликовабыламаленькаяточноящи ккроватьбыласпологомложасьспатьонукрывалсясголовойбыложаркодушновзакрытыедверистучал сяветервпечкегуделослышалисьвздохиизкухнивздохизловещиеиемубылострашнопододеяломонбоялс якакбычегоневышлокакбыегонезарезалафанасийкакбынезабралисьворыипотомвсюночьвиделтрево жныесныаутромкогдамывместешливгимназиюбылскученбледенибыловидночтомноголюднаягимназ иявкоторуюоншелбыластрашнапротивнавсемусуществуегоичтоидтирядомсомнойемучеловекупон атуреодинокомубылотяжкооченьужшумятунасвклассахговорилонкакбыстараясьотыскатьобъясн ениясвоемутяжеломучувствуниначтонепохожеиэтотучительгреческогоязыкаэтотчеловеквфутля реможетесебепредставитьедванеженилсяиваниванычбыстрооглянулсявсарайисказалшутитедаед ванеженилсякакэтонистраннонаначиликнамновогоучителяисториигеографиинекоегоковаленком ихаиласаввичаизхохловприехалоннеодинассестройваренькойонмолодойвысокийсмуглыйсгромадным ирукамиполицувидночтоговоритбасомивсамомделеголоскакизбочкибубубуаонауженемолодаялет тридцатинотожевысокаястройнаячернобровыакраснощекаяоднимсловомнедевицаамармеладитак аяразбитнаяшумнаявсепоетмалороссийскиеромансыихохочетчутьчтотакизальетсяголосистымсм ехомхахапервоеосновательноезнакомствосковаленкамиунаспомнюпроизошлонаименинахудиректт орасредисуровыхнапряженноскучныхпедагоговкоторыеинаименинытоходятпообязанностивдругви димноваяафродитавозродиласьизпеныходитподбоченясьхохочетпоетпляшетонаспеласчувствомви ютвитрыпотомещеромансиещеивсехнасочаровалавсехдажебеликоваонподселкнейисказалсладкоул ыбаясьмалороссийскийязыксвоеюнежностьюиприятноюзвучностьюнапоминаетдревнегреческийэт опольстилоейионасталарассказыватьемусчувствомиубедительночтовгадячскомуездеуненеестьхут оранахутореживетмамочкаитамтакиегрушитакиедынитакиекабакиухохловтыквыназываютсяка бакамиакабакишинкамиварятунихборщскрасненькимиссиненькимитакойвкусныйтакойвкусныйч топростоужасслушалимыслушалиивдругвсехнасосенилаоднаитажемысльахорошобыихпоженить тихосказаламнедиректоршамывсепочемутовспомниличтонашбеликовнеженатинамтеперьказалос

ьстраннымчтомыдосихпоркактонезамечалисовершенноупускалиизвидутакуюважнуюподробность вегожизникаквообщеонотноситсякженщинекаконрешаетдлясебяэтотнасущныйвопросраньшеэто неинтересовалонасвовсебытьможетмынедопускалидажеимысличточеловеккоторыйвовсякуюпого духодитвкалошахиспитподпологомможетлюбитьемудавноужезасорокаейтридцатьпоясниласвою мысльдиректоршамнекажетсяонабызанегопошлачеготольконеделаетсяунасвпровинцииотскукиск ольконенужноговздорногоиэтопотомучтосовсемнеделаетсяточтонужнонуводткчемунамвдругпона добилосьженитьэтогобеликовакоторогодажеивообразитьнельзябыложенатымдиректоршаинспе кторшаивсенашигимназическиедамыожилидажепохорошелиточновдругувиделицельжизнидиректо ршаберетвтеатреложуисмотримвееложесидитваренькасэтакимвееромсияющаясчастливаяирядо мснейбеликовмаленькийскрюченныйточноегоиздомуклещамивытащилиядаювечеринкуидамытребу ютчтобыянепременнопригласилибеликоваиваренькуоднимсловомзаработаламашинаоказалосьчтов аренькапепрочьбылазамужжитьейубратабылонеоченьтовеселотолькоизналичтопоцелымднямспо рилиругалисьвотвамсценаидетковаленкопоулицевысокийздоровыйверзилаввышитойсорочкечубизп одфуражкипадаетналобводнойрукепачкакнигвдругойтолстаясуковатаяпалказанимидетсестрато жескнигами

Висновки:

В даному лабораторному практикумі ми освоїли методи частотного криптоаналізу, здобули навички роботи та аналізу потокових шифрів гамування адитивного типу на прикладі шифру Віженера.