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

«Криптографія»

Комп’ютерний практикум №3.

ВАРІАНТ №24

Виконав:
Студент III курсу ФТІ
группи ФБ-81
Шмалій Г. Г.
Перевірив:
Чорний О. М.

Мета роботи

Набуття навичок частотного аналізу на прикладі розкриття моноалфавітної підстановки; опанування прийомами роботи в модулярній арифметиці.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму. 1. Реалізувати підпрограми із необхідними математичними операціями: обчисленням оберненого елементу за модулем із використанням розширеного алгоритму Евкліда, розв'язуванням лінійних порівнянь. При розв'язуванні порівнянь потрібно коректно обробляти випадок із декількома розв'язками, повертаючи їх усі.

2. За допомогою програми обчислення частот біграм, яка написана в ході виконання комп'ютерного практикуму №1, знайти 5 найчастіших біграм запропонованого шифртексту (за варіантом).

3. Перебрати можливі варіанти співставлення частих біграм мови та частих біграм шифртексту (розглядаючи пари біграм із п'яти найчастіших). Для кожного співставлення знайти можливі кандидати на ключ (a,b) шляхом розв'язання системи(1).

4. Для кожного кандидата на ключ дешифрувати шифртекст. Якщо шифртекст не є змістовним текстом російською мовою, відкинути цього кандидата.

5. Повторювати дії 3-4 доти, доки дешифрований текст не буде змістовним.

Хід роботи

Був використаний російський алфавіт: "абвгдежзийклмнопрстуфхцчшщьыэюя"

Було створено 2 класи: Alphabet клас алфавіту мови, який містить перелік літер алфавіту, неможливі біграми для даної мови, та список неможливих символів тексту. За допомогою відповідних функцій я зчитую текст, який ми розглядаємо як приклад мови, фільтрую його, видаляючи неможливі символи тексту, шукаю частоти біграм та ентропію мови. Клас TestAffine є основним класом, в якому під час викликання конструктора за замовчуванням зчитується зашифрований текст, рахується частота біграм зашифрованого тексту. За допомогою функції FindKeys шукаються всі можливі кандидати на ключ, розв'язуючи лінійні конгруенції, за допомогою функцій Converse() та gcd(). Далі, проходячись по всім кандидатам, за допомогою функції CheckKey() я обираю правильний ключ, перевіряючи ентропії та існування неможливих біграм , яким був зашифрований даний текст. Вивожу текст, розшифрований за допомогою знайденого ключа.

Приклад виводу програми:

```
(40, 921)  -> Error! Incorrect entropy! 4.841461661536888
(96, 178)  -> Error! Incorrect entropy! 4.648025557070678
(315, 78)  -> Error! Incorrect entropy! 4.741268154386913
```

```
(646, 759)  -> Error! Incorrect entropy! 4.800783758401756
(920, 559)  -> Error! Incorrect entropy! 4.816909333492021
(41, 0)  -> Error! Incorrect entropy! 4.813635184899897
(811, 644)  -> Error! Incorrect entropy! 4.807960321030846
(150, 364)  -> Error! Incorrect entropy! 4.7701166623653615
(865, 799)  -> Correct key
```

Всі дані про перевірку кандидата знаходиться у файлі keys.txt

Список неможливих біграм: `'аь','оь','иь','уь','оь','щй','щф', 'щх','щц','щч','щш','щщ', 'гщ'`

Ентропія мови: `Entropy of language:  4.459429204208751`

Ентропія правильно розшифрованого тексту: `Entropy decrypted text: 4.413690306514427`

Шифртекст:

Ондмрсзциткщьафаеюыаишрльйоазншряймжддлчушмеушсббпхбесхнфдпиерешядпленмбщйднд
йдннцдгцчесдтфменхрчсхнзшсбеыыйшймбкйяхнбарощепншшуозэяэйьймбасзциткщчсзциткщья
юаяеснпюмшдуйэхндмщщынеймждджкчзюмхрчсхнчйшадуоаьрчсштмбцюсбеыишсзатфмычитсш
кзррщщхбызщывшижкщщщозррщьлгчсфдьшдаендмэююаушсбчрепншдшийщаушсбеыенюдбпн
шкняайакнибеыкрюовйднишчмишзшрлбпякпаоныритбрбыянвцфдейпббщсыдыррьзкысшвшпшб
щсыюрууззйывмчрщщитесштмбзнушяакбвншаязутмбдйиршдепфюзолдрадшбумзьтцатихбюзшге
нднсшьашобпернмшаыалхчшьшяучзйавйяузцьтыпчыфюпирцьфыжлгшаерфнмбызыжензйшйнцлд
знфнвщтемечзррщнхнещызюатйеиыеххлцфгвйиргчшзбщшдендйшачтхйбембыншзяйшшзодэгщс
кзжяныцьфбркkиучрррсйлхлхюмдтякыншмдттоваякчшпикщхбызяйсшбншзчпхбитибщйэйыючйв
цитерсаещшйирбпшдчшкнднхсддйащхлцфгвйирыздгьззжццызррящдгццшдэнещызуцбрсйыасшл
юпшлнеювйлхмнфачюзбфочршtонхнынсншалхфдвшишяатишзлдьюцаушпиеысрфгуулцоодупйэ
йьаттвндззжбриамбишжриуйдпзепиуычызжаейпшлнкпчычеушпиеыьбсббаыдытбрыезхфдонвййр
цйншяаонхнтебруузритбрсйхбизгцлдщкчзюмшаыахнеионзмзндуьубелнвйшдонехибзцархавйкне
иенерьуццепитызюцьучжрюшнкнойчйяаерчпитызюцибвнешяепрфгсшщатйеиыейкшйзусбцчибба
ьзхпщывмчрщщитхабхбпццдюяныасшшарнгйлрюхтмраейрлдухбенайшакщщюрюэйчюшзлгсшу
шпизнюуыженмбжхтмплбпощдгццшдраинещызуцбрсйейднлшфыйаьлюнмбызыжвйюншалхмнфа
яаюдзнючишьпитызцчюдсбесхниннцхаейпихбенайшакщшучзайчюьуьшдшлнтищбхбесхнерскчзч
жюциаыйшйхююдытитццчрдуеплнбепиюеишчйенвцитууиафщдгццшдасхнюдэщяйпкиучрррсйвц
итууфняньзлхенмбщчбпыжлгшасшлюпшлндйяащасаятдбэркдитчзцазобпшдцтючнцдгцчвшчрмбу
шзйхкшймбррыедтшгюйхжррбышйщаянмбоыиряймбззббзцаряйлхмньмбрсйюдбпхбепесхниннце
рутфдйасшвцитвнвйывйашдвшенущлдишьргчмбызерсшюзррьфсбепесбперзцугщхгцепитызибщй
эйщаэйбыырьйюембутчыяаыйшйфаттвндззжбрсйыбесхнерчсштмбзнушяаенщамбщыянорщыыйт
шеившижбрдтшгинюрщщщщщамбщысклцсшкзнмшдписркжсшфшхинкшдзндупклцыжбрдявмен
фрфгутлдьусэмндыющлдзннэиюьибеяккщхрцаьтшдтавштйеишааеицдууршаьшыйвтщыбечшюею

тррзжлгяизалбепиуозккбсццьтонхнынинсшоачшыйвтцйзтбрюмзцфнсшяньющачштатифшхбындр
гчсшонхнтебрнмлхгцвнытбсббйщиусшвшущхбызвяянеймбюцчрбщлцбрйщыхгцддузбаермбццьш
мцдбйшикббэсшзсйшшсткзшдчшрцудхбгйвшыавмзццчлдшзюмлнчйшацуиашндйвшыаыйшйзчбб
гтинещцюнтчмьачйыдвасмиуонхнтеснмбццеыжйяапззхитццхнеионвйкнеицайкесчрощоаьрарюнм
бррутяаушчштичрнмлхгцыжибйщщщшавычйлнбелнсркжвйфшхидтйэйалгхндныаишпйфавйиреп
шдшгчзхшшацтонхнынинсшоачшбнмайкызьшсрожццонбщщщщюфбшдитфдшрлхгцякощчржбар
ббнотндрйгцххбужлгшапззхитццсйнютшмббыфнсшвйзнеиенхбншчштиьуерккитчзщцддгймееши
кббэсдушндйхнушчштишмфдццдуякийфыирбщсаюйчшчшишхкызкжбрбыскпаднхнрцбрбыкцздз
нбпякчзьйчмутинещцюсшвшпшшдвшушчштивмсшлдтййкызьшьщсыюрууззйымбццдгррьуббудн
кпаднхнрцбрбыыаонтйчмжабхбпццбаьйсркжсшфшхинкшйкцыжюцрпишгавйхбоюмбибудшнкнф
рббноштинещцюьуббрахбдфишбнмбеншннцддюцлдарбвхншзюмлнчйшафдьшьмаудрдудшейтша
юлшбньылгчсфдвагдюцбнгйпасклцрпщыкцурьйянийьраускчздубршуфдвшскиуялгушдонюдватти
шгйюышаююншвйянюмтнытбсццррббнощщепншнэшмзцццивхншзюмлнчйшасблцйщякыжццвэ
мбннмбутрбдубрздьшдшчшербаюезйзшчшлгонлрббрдпзтмиутмчзоаушздийоевймблцйщепызздо
неионбнешчефнбцлхийшанкшдийхндньшонсшянхююдытитцццдзхнкощчржбсэсркженчуззщйеав
мчрощсэюдзндудншйсшвшпшкнеитюцсддпибздубрфндрутятяйющиусштймаюйчшырепууьтхпью
фаушсшчсхншащюьиишсзатщыюцскчздучрщыятхаыахнсщьучрккиычйираускццгфуудюяняраувй
янзтожыеотьпчыбнядинпззцррбберрсдушдвшсшрцьтццлдапчшдшпйфавйшасвхнлгфюиылнчюща
лньйенерлхгцвмчывйбрюнучвмьуощщщхнеионвберюхтмгтмнфачщвйснсшбембынюдвшушчшлге
йсычшянлнчйшасаюеишчйшадтьпчыншюхишчштидшсрчпжаяацапиюнгйьадршдвйтйшкбрсйино
аншаюмнншхндневбякиуюоццнэнэюдкщдгццшдасхнерутхбзнмднэтшхксэейткыншасрсбхнсшщбш
дмбишжраувйянмаеиыеейчтякыншнчюмбшйсцбрбеийюмтодтыечтьпчызтонлфюмкщцхиыксчзен
иочзмбуриуицббщйырзхшйюршдуыдширсэоютщиуоншньчтмщыюхийдрщысшвшпшмаюйчшыре
пууьтхпьюфаушсшсшшзкжбренонфщщыозддоюещщыонлфцкоыешлдинпззцррэюднлмдйпаердди
нпззцббтмщштмэюайлнирббйдхнынфюоаьриавшмбызерзжлгшаощхбызсэерккшйьмбрбщепншвй
рюфшчшонхнишнкшйьмьйющдгццддрбщщсяншийонцрдтчзоышрсятйыйхибечшнэуцожсаындрь
йянсышрьйгйыввшмбызерзжлгшаущхбызсэюдзхгцхаяаоюмбхббаишсзтобрсйюцлдпзнмррсйфне
щызуцбрсйерддинпззцббтмрпюйердгсшчшщблхгцеренерррдуепчшбпитфмсбрасшгйьшвбщщьуь
шваинохгцчмфдэнсшьаюйчшбпвнлыпившвавжкщщщьуербестяейамшыюпзхааеуыынвцутийерут
фмзцкйдняайнвцщоццкйдндннлнмаяньбызщцкйднвцитбаятхавцитддьшдширцйдужачрепншшзфм
шуатццдгддзхдадшвйдненюефдлнушонхнтесбепншиннцюхгхнбудьшдшыезнхноцчжибсшизфдий
юдзннэцшечббенсоыхлйлхлнонйакплцитхрцчтмвяуцюмфюнзящхплюьибпшдпзноеншадщбаицбс
сквмсымеуюбеытчзбнтжббэпчшдшуцфдвыйасшуцюменсцщююдшзэпьткййалдгйдшсбиншлчрнн
дрррепкйднхюпидшейшрлхрдпзвмыноашрббнодгсшсбщбвнохызсбеыяухсибзцарсэкнеицсхнвшон
сввшкнеидшгйсхлцасхнерхююдытпйвщщщхрбплхлцибрюфшсбсшвшпшердшеййаийдтшафшяиь
квмсыопчшдшчрнювецшздудвшопитызибэндрсюзшыршдьшдшлншвхнятзгббудзхуруткщлдмби
шншрльугйлндйонывхндййряйчюгйяисаерлдхееюрльуюгнцрмиусшвшпшьаюйчштйыйхикбхбюг
нцрмяняухбшйорррьйсшвшпшьшваюдбпншхбдййачшхндмккшйьмбсдуйдыйчшянрюфшпихбиущ
бвнсшхбдйтшсберддьшдшчшкбердуыжсбвшлкынбнежббуддвхнднвйщююйытгхтмсбфгбнынюеш
нюддуерббькчзудсштшчшьаюйчшбпхаыйшйоаушчштйыйхиюдсбесхнеррсштмбзнушчшхндмннс
шюдянлрюцккынбнежибзцарйэюзйдшрйэмбынчачтьпчыюйдншзивйагдлнушааянсычшьррсбрсйп
кшйьшфншсщышадвхндншзвмлцоатйеиенднюгнцрмщышннцддюцддапитызюцддзхсбькчзарббно
рсхнбелнбемждденфдяакненмбццеыюдбпншмбишншрльуздьшдшчшкбхбепншвшблцйщякхбиу
хсхнкцурбпхвхнбелнбемждденннвкерщцкбхасшгйерянрюфшосхнкбвмчыейсымждденбебелнерхн
дмкйэймнтйежибжхоывдздейпбиадбщщюзыхепьюянещдгццкйчюурюмшуццбвхнднрмшуццдит
хйимлюдньйвцюхжыещдгццббесхнрюфшчшщхрдьшдшчшоюещээбеершуозццюддтшйфышуозцц
беыйшйзухаыанцдгуубыбечшбеысддяцьтуттзутвйшалдтйлсхндбькчзрбькчзарчсбпербщеперсбьрц

цяаеркберсбвйьрццчрбщепншвййгсшсбибькчзарбщепншшаондмэючйвйеидыяншзутибрвхнднфн
лыпиерднзнпаийебчжфдлнушентйыйхинтвндззжбриаятяйлрббнонныбсццкйчючррсюнсшшдвшс
шрцьтццкйднчпитызюцэюзшырвмчыушырерюмчыейсыюеьрээтйщбиувйзйютддвйшрчсбпитоаьр
иамбишншпиятууфмчыейсыьюжоьйысддйасаердзццьйлююююожццьйвшьщщщерзшийдтхнмдпзно
ыечтбсчздшгймешйдрнкчзюмяучзпизантвндззжбриаятяйинсшднзнпачшдупйэйьзхпсйвйюрцйьяк
нкрцйшйщаонхнтеюнсшиннццхрдьшдшпихндмщщхбызцйеррпитызюцббькчзйыьяуцзбзхдбзхщц
эхьяьяуццпитызюцннсшиюбнынюршдоафшкзящлдйаещьтщызюбешнчймбесбрыечюмаяадущш

Розшифрований текст:

Когдачеловеквидитумирающееживотноеужасохватываетеготочтоестьонсамсущностьеговегоглаза
хочевидноуничтожаетсяперестаетбытьнокогдаумирающееестьчеловекичеловеклюбимыйощущае
мыйтогдакромеужасапередуничтожениемжизничувствуетсяразрывидуховнаяранакотораятакжека
киранафизическаяиногдаубиваетиногдазалечиваетсяновсегдаболитибоитсявнешнегораздражающ
егоприкосновенияпослесмертикнязяандреянаташаикняжнамарьяодинаковочувствовалиэтоонинра
вственносогнувшисьизажмурившисьотгрозногонависшегонаднимиоблакасмертинесмеливзглянут
ьвлицожизниониосторожнобереглисвоиоткрытыераныотоскорбительныхболезненныхприкоснове
нийвсебыстропроехавшийэкипажпоулиценапоминаниеобобедевопросдевушкиоплатьекотороенад
опригототовитьещехужесловонеискреннегослабогоучастияболезненнораздражалорануказалосьоско
рблениеминарушалотунеобходимуютишинувкоторойониобестарались ьприслушиватьсякнезамолк
шемуещевихвоображениистрашномустрогомухоруимешаловглядыватьсявтетаинственныебескон
ечныедаликоторыенамгновениеоткрылись ьпереднимитольковдвоемимбылонеоскорбительноинебо
льноонималоговорилимеждусобойежелиониговорилитоосамыхнезначительныхпредметахитаидр
угаяодинаковоизбегалиупоминанияочемнибудьимеющемотношениекбудущемупризнаватьвозмо
жностьбудущегоказалосьимоскорблениемегопамятиещеосторожнееониобходиливсвоихразговора
хвсеточтомоглоиметьотношениекумершемуимказалосьчтоточтоонипережилииперечувствовалин
емоглобытьвыраженословамиимказалосьчтовсякоеупоминаниесловамиоподробностяхегожизнин
арушаловеличиеисвятынюсовершившегосявихглазахтаинствабеспрестанныевоздержанияречипос
тоянноестарательноеобхождениевсеготогочтомоглонавестинасловоонемэтиостановкисразныхсто
роннаграницетогочегонельзябылоговоритьещечищеияснеевыставлялиперединхвоображениемточт
ооничувствовалиночистаяполнаяпечальтакженевозможнакакчистаяиполнаярадостькняжнамарьяп
освоемуположениюоднойнезависимойхозяйкисвоейсудьбыопекуншиивоспитательницыплемянни
каперваябылавызванажизньюизтогомирапечаливкоторомонажилапервыедвенеделионаполучилап
исьмаотродныхнакоторыенадобылоответчатькомнатавкоторуюпоместилиниколенькубыласыраио
нсталкашлятьалпатычприехалвярославльсотчетамиоделахиспредложениямиисоветамипереехатьв
москвуввздвиженскийдомкоторыйосталсяцелитребовалтольконебольшихпочинокжизньнеостана
вливаласьинадобыложитькакнитяжелобылокняжнемарьевыйтиизтогомирауединенногосозерцани
явкоторомонажиладосихпоркакнижалкоикакбудтосовестнобылопокинутьнаташуоднузаботыжизн
итребовалиееучастияионаневольноотдаласьимонаповеряласчетысалпатычемсоветоваласьсдесале
моплемянникеиделалараспоряженияиприготовленияднясвоегопереездавмосквунаташаоставалась
однаистехпоркакняжнамарьясталазаниматьсяприготовлениямикотездуизбегалаиеекняжнамарья
предложилаграфинеотпуститьссобойнаташувмосквуиматьиотецрадостносогласилисьнаэтопредло
жениескаждымднемзамечаяупадокфизическихсилдочериполагаядлянееполезнымипеременумест
аипомощьмосковскихврачейяникуданепоедуотвечаланаташакогдаейсделалиэтопредложениетоль
копожалуйстаоставьтеменясказалаонаивыбежалаизкомнатыструдомудерживаяслезынестолького
рясколькодосадыиозлобленияпослетогокаконапочувствоваласебяпокинутойкняжноймарьейиоди
нокойвсвоемгоренаташабольшуючастьвремениоднавсвоейкомнатесиделасногамивуглудиванаичт
онибудьразрываяилипереминаясвоимитонкиминапряженнымипальцамиупорнымнеподвижнымвз

глядомсмотреланатоначемостанавливалисьглазауединениеэтоизнуряломучилоеенооноюылодляне енеобходимокактолькоктонибудьвходилкнейонабыстровставалаизменялаположениеивыражение взглядаибраласьзакнигуилишитьеочевидноснетерпениеможидаяуходатогоктопомешалейейвсеказ алосьчтоонавотвотсейчаспойметпроникнеттоначтосстрашнымнепосильнымейвопросомустремле нбылеедушевныйвзглядвконцедекабрявчерномшерстяномплатьеснебрежносвязаннойпучкомкосо йхудаяибледнаянаташасиделасногамивуглудивананапряженнокомкаяираспускаяконцыпоясаисмо треланауголдверионасмотрелатудакудаушелоннатусторонужизниитасторонажизниокоторойонап режденикогданедумалакотораяпреждеейказаласьтакоюдалекоюневероятноютеперьбылаейближе ироднеепонятнеечемэтасторонажизнивкоторойвсебылоилипустотаиразрушениеилистраданиеиос корблениеонасмотрелатудагдеоназналачтобылонноонанемоглаеговидетьиначекактакимкакимонб ылздесьонавиделаегоопятьтакимжекакимонбылвмытищахутроицывяроставлеонавиделаеголицос лышалаегоголосиповторялаегословаисвоисловасказанныеемуиногдапридумывалазасебяизанего новыесловакоторыетогдамоглибыбытьсказанывотонлежитнакреслевсвоейбархатнойшубкеоблоко тивголовунахудуюбледнуюрукугрудьегострашнонизкаиплечиподнятыгубытвердосжатыглазабле стятинабледномлбувспрыгиваетиисчезаетморщинаоднаногаегочутьзаметнобыстродрожитнаташа знаетчтоонборетсясмучительнойбольючтотакоеэтабользачембольчтоончувствуеткакунегоболитд умаетнаташаонзаметилеевниманьеподнялглазаинеулыбаясьсталговоритьодноужасносказалонэто связатьсебянавекисстрадающимчеловекомэтовечноемученьеиониспытующимвзглядомнаташавид елатеперьэтотвзглядпосмотрелнанеенаташакакивсегдаответилатогдапреждечемуспелаподуматьо томчтоонаотвечаетонасказалаэтонеможеттакпродолжатьсяэтогонебудетвыбудетездоровысовсемо натеперьсначалавиделаегоипереживалатеперьвсеточтооначувствовалатогдаонавспомнилапродол жительныйгрустныйстрогийвзглядегоприэтихсловахипонялазначениеупрекаиотчаянияэтогопрод олжительноговзглядаясогласиласьговориласебетеперьнаташачтобылобыужасноеслибоносталсявс егдастрадающимясказалаэтотогдатактолькопотомучтодлянегоэтобылобыужасноаонпонялэтоинач еонподумалчтоэтодляменяужаснобыбылоонтогдаещехотелжитьбоялсясмертииятакгрубоглупоска залаемуянедумалаэтогоядумаласовсемдругоееслибыясказалаточтодумалаябысказалапускайбыон умиралвсевремяумиралбыпередмоимиглазамиябылабысчастливавсравнениистемчтоятеперьтепер ьничегоникогонетзналлионэтонетнезналиникогданеузнаетитеперьникогданикогдауженельзяпопр авитьэтогоиопятьонговорилейтежеслованотеперьввоображениисвоемнаташаотвечалаемуиначеон аостанавливалаегоиговорилаужаснодлявасноне дляменявызнайтечтомнебезваснетничеговжизнии страдатьсвамидляменялучшеесчастиеионбралеерукуижалеетаккаконжалеевтотстрашныйвечерзач етыредняпередсмертьюиввоображениисвоемонаговорилаемуещедругиенежныелюбовныеречикот орыеонамоглабысказатьтогдакоторыеонаговорилатеперьялюблютебятебялюблюлюблюговорилао насудорожносжимаярукистискиваязубысожесточеннымусилиемаа

Висновок

У ході даної лабораторної роботи я удосконалив навички частотного аналізу. Удосконалив навички в модульній арифметиці, навчився використовувати алгоритми Евкліда на практиці, написав для них програмний код. Ознайомився з методом атаки на афінний шифр. Навчився фільтрувати, коректний для даної мови текст